House of Lords
House of Commons

Joint Committee on Draft Communications Data Bill

Draft Communications Data Bill

Session 2012–13

Written Evidence

The Joint Committee on the Draft Communications Data Bill

The Joint Committee on the Draft Communications Data Bill was appointed by the House of Commons on 21 June 2012 and by the House of Lords on 28 June 2012 to examine the Draft Communications Data Bill and report to both Houses by 30 November 2012.

Membership

HOUSE OF LORDS

Lord Armstrong of Ilminster GCB CVO (Crossbench)
Rt Hon Lord Blencathra (Chair) (Conservative)
Baroness Cohen of Pimlico (Labour)
Lord Faulks (Conservative)
Rt Hon Lord Jones (Labour)
Lord Strasburger (Liberal Democrat)

HOUSE OF COMMONS

Mr Nicholas Brown MP (Labour, Newcastle upon Tyne East)
Michael Ellis MP (Conservative, Northampton North)
Dr Julian Huppert MP (Liberal Democrat, Cambridge)
Stephen Mosley MP (Conservative, City of Chester)
Craig Whittaker MP (Conservative, Calder Valley)
David Wright MP (Labour, Telford)

Contents

Written evidence

ADM Shine Technologies

These are the collegiate comments from all at ADM Shine Technologies Ltd. Aggregated and moderated by Andrew Dawson-Maddocks {Managing Director and Chief Technical Officer} and Barbara Breeze {Commercial and Finance Director}.

ADM Shine Technologies Ltd is an SME in the Midlands and is home to Specialist Defence Research in Electronic Warfare – EW {Electronic Surveillance Measures and Electronic Counter Measures in the tactical market} and Counter Terrorist {C-IED and related Cyber, advanced robotics and special projects} primarily for the needs of the UK.

Andrew has extensive defence experience and that of national security spanning several decades.

Opening Overall Comment: The Communications Data Bill is well written and explores the complex and contentious issues well. Whilst we have legal experience and qualifications 'in house', we have limited all of our answers to our expertise area and background knowledge into the highly sensitive areas of Special Surveillance, Electronic Surveillance, Lawful Interception {telephone [both fixed and mobile], data networks – inclusive of 'The Internet', and of Satellite Services [including telephone]. These comments will be made at a level that does not warrant government privacy markings and hence may be included if appropriate to the overall enquiry on the said bill.

We made a number of key comments on the consultancy for the Justice and Security Bill Green Paper {CM8194: ISBN 9780101819428}, which we will reference and relate to in our response as some of the same points apply.

We recognise and have the detailed expertise in telecommunications to say that the communications environment (both technically and commercially) is now vastly advanced from the early steps taken by the Home Office and ACPO (late 1990's) for the underpinning relationships for the implementation of RIPA 2000 and liaison support units. The social behaviours and use of these communications mediums has advanced not just with the natural advancement of technology – but in use and the types of communication and in the terminal equipment used to access such (e.g. social media).

It is noted that our law enforcement and intelligence agencies are admired by overseas law enforcement agencies as the investigative capabilities of Great Britain are both good and stringently controlled. That said some politically odd usage of RIPA has occurred, especially local council usage which has the potential to considerably undermine public confidence – irrespective of strict oversight and control.

We continue to maintain the view and agree with the current approach that such release of the above material and techniques in UK or other courts, not only could lead to damage to national security, but also damage to investigative methods and the risks of the full gamut of human life through to technical techniques damage. Control, basis of authorisation, whom authorises, use and oversight are the key issues…

The voluntary code of practice on Retention of Communications Data Order 2003 SI 2003 No 3175 recommends to operators to keep subscriber and telephony records for a year, whilst SMS, e-mail and data 'accounting' records of ISPs for 6 months and the detail of browsing for less than a week (4 days). The volume of data across a day for the UK is considerable even in today's advanced computing abilities. The now compulsory rules are that from Data Retention (EC Directive) Regulations 2009, SI 2009 No 859 which stipulates the Telephony, Internet, e-mail and subscriber records must be retained for a minimum of a year. Complications arise from non-resident operators.

Overall the Bill provides for the advancement socially and technically for the prevention of crime and terrorism. It also aligns to the Security and Justice Bill to implement effective oversight and control. If the UK is to continue to be effective at law and order and keep the security of country, allies and visitors, then it is technologically a prudent way forward, legally wise and so long as usage of such data is restricted once authorised to only the law enforcement government departments then oversight shall be effective and strong.

Our nomenclature is to abbreviate Answer to A. then we quote the question number from the parliamentary question on the 'Have your say on the draft Communications Data Bill' web page that it relates to. If more than one question is posed for a given section then in parenthesise will be roman numerals to depict the order of the question the answer relates to.

Our Answers:

GENERAL QUESTIONS:

A.1 – Yes. The technology and social use of such is highly dynamic and when RIPA was posed both were far less complex than today. 4G, internodal and intermodal communications are going to complicate this further.

A.2 – Yes.

A.3 – They shouldn't, however we are concerned for the Use of such intrusion by teams and areas across government not tightly aligned to the rigours and control as the judiciary for example. Local Government (for example) to be so trained and authorised as a Single Point of Contact (SPoC) to use of this Bill and RIPA will only further exacerbate public disquiet. These extraneous SPoC's should be transferred and amalgamated with the relevant law enforcement units – such as the relevant Constabularies' Economic Crime Unit for say DWPs SPoC's. Perhaps such extraneous SPoC's should have to seek authority for use from either local law enforcement bodies or centrally administered with revisions of procedures and oversight and necessary shift in budgets and resources. Whilst on the fringe and minority perhaps, the public do not respond well to media claims of RIPA being used by local government for minor issues within a local council's catchment area with issues such as minor placement problems i.e. an occupant's rubbish bin.

A.4 – Don't spread it widely in court, treat as sensitive data/evidence otherwise you risk damaging the effectiveness and ability for its use. Or worse still the legal paradox of causing crime through its release. It is crucial that very strict access to this data is undertaken to prevent corrupt sale or use of this by criminal elements.

A.5 – No comment.

A.6 (i) – The two work well as our answer to question 1 postulates it is wise to keep these two separate as the Data Retention Regulations may well need to be refined and differing data types specifically regulated without need to change the overarching legislation of this Bill.

A.6 (ii) – No as technological is rapidly evolving the need for revisions to the Bill would at least every government term in office {=5 years}! Therefore it would be unwise to have it as an overarching combined piece of legislation.

A.7 – No comment.

A.8 (i) – Technologically they shouldn't as much of the data the Bill relates to the approved operator needs to conduct and control their business – save for some elements of data – Therefore No.

A.8 (ii) – Commercially some of the data volumes especially on the internet side are significant. If these became burdensome then the government could elect to have the cost of stowage and retention – then the operator will have limited cost of implementation. This is a mute argument as globally most jurisdictions require IOCA/RIPA capabilities and this Bill is bringing those needs to the 21st century.

COSTS:

A.9 – No comment.

A.10 – No comment.

SCOPE:

A.11 (i) and (ii) – Yes

A.12 (i) – Law Enforcement and Intelligence Agencies only would be our strong view. All the other government departments should seek assistance and raise the necessary cases (which the use to which the bill is then put) could be highly scrutinized and kept safe to the wider public privacy.

A.12 (ii) – Yes but that order must be agreed to by the ICC and that they are so obliged to give the draft order a fair hearing by the Investigatory Powers Tribunal (IPT) as expanded by the proposal for parliamentary oversight of these powerful tools in the Justice and Security Bill. The IPT has a key remit and legal framework to ensure ECHR issues of ensuring the principles of fairness of our justice system along with the implications of rightful use of such tools.

A.13 (i) and (ii) – No comment save for the 'roaming agreements' should obligate third party and overseas operators to be legally conformant with RIPA and this Bill, otherwise such telecommunication services (or licenses), should be withheld.

USE OF COMMUNICATION DATA:

A.14 (i) and (ii) – see our answer to question 3 and 12. We make no further comment.

A.15 – Yes although if the requirement was pursued to its limit of also requiring more and more 'content' data then the challenge and commercial costs for service providers would become very prohibitive and our answer to question 8 (ii) is referred to.

SAFEGUARDS:

A.16 – Current safeguards in RIPA and those authorisation processes will be enhanced by this Bill and definitions already exist in this system which on the whole has proved to have been controlled well, with tight strict controls on access and use {save for our opinions mentioned above}. We do not believe within the scope of our understanding of the procedures, controls and ECHR, along with HRA, that ECHR Article 8 would raise compliancy issues/concerns?

A.17 (i) – Whilst on face value a warrant based system has considerable merits – its current use for 'content' is a strong instrument that should remain – so expanded to include content in the data world – e.g. the actual SMS text or URLs so visited

A.17 (ii) – No we favour the exiting system as defined by IOCA, refined by RIPA and so implemented. This system procedurally should recognise the elements of the Digital Age and the Social Trends of Telecommunications – warrant for 'content' would be a wise doctrine to keep. Record Data (as outlined within this Bill), shall require an authorisation from an authorised and approved point of contact and we recommend if that sits outside of the traditional law enforcement and intelligent agencies then that request so requires authorisation from such.

A.17 (iii) – Yes as defined above.

A.17 (iv) – minimal if the 629 SPoC's were to be refined as outlined here.

A.18 – ICC role is Yes (save that great care that is needed to keep pace of not just the technology but the terminal equipment and social usage), and the IC role perhaps needs greater authority to act for misuse and breaches of the DPA and related acts.

PARLIAMENTARY OVERSIGHT:

A.19 – Yes when combined with those consulted on for the Security and Justice Bill.

ENFORCEMENT:

A.20 – No comment.

A.21 (i) and (ii) – No comment.

TECHNICAL:

A.22 – Yes. Very safely. It can be enciphered in a way that is evidentially sound to a very strong level of protection too as can any electronic feeds of such data.

A.24 – Yes, Yes and technically feasible.

A.25 – If implemented effectively and by using strong data and network protection standards, this will be extremely difficult.

A.26 – if the encipherment of the data and encipherment of the access to such data is done in a way that is evidentially sound and highly protected then No.

August 2012

Nathan Allonby

This submission mainly relates to the provisions for retention of data for postal communications.

Clause 25 of the Bill has provisions apply requirements for data-retention "to public postal operators and public postal services as it applies to telecommunications operators and telecommunications services", i.e. to create a system for logging all mail in a database, similar to that recorded for telecommunications, e.g. details such as addressee, sender's address, date, and any other visible information on the cover. Clause 26 would allow postal operators to recover the cost of this from government. It appears this information would be held in a database and retrieved at the point an individual becomes a suspect in an inquiry.

The Draft Communications Data Bill contains approximately 94 sentences referring to data retention for postal services. Provisions relating to postal services are thus a very important feature of this Bill.

It is believed that this may be a new and unprecedented form of surveillance: - no state has ever logged all post, even in those nations where there was comprehensive censorship of the post.

Crime and the "threat"

Nowhere has the government made any case for retention of postal data - there appears to be not a single word relating to a case for postal data-retention in any of the government supporting documents, i.e. : -

Draft Communications Data Bill impact assessment[1]

Draft Communications Data Bill privacy impact assessment[2]

Communications Data Bill - key background information[3]

Strategic Defence and Security Review (2010)[4]

On this basis, the government has presented no case whatsoever for what may be an unprecedented surveillance measure.

For telecommunications and the internet, the government arguments for increased data retention powers pivot around a new medium of communication creating new types of crime and new modes of criminality. For terrorism also, the government arguments are based around new patterns of criminality arising from new forms of communication. The government case for increased data retention is not merely based upon high levels of terrorist threat, but upon a threat moving to take advantage of a new medium. (Please note: the government arguments for telecoms data retention are not accepted by the writer).

None of the government arguments appear relevant to postal communications data-retention.

A Freedom of Information request was also made to the Home Office about cost, feasibility and the threats to which the Bill was responding [5]. I would draw your attention to the following section of their reply.

http://www.whatdotheyknow.com/request/119629/response/297764/attach/html/3/attachment.pdf.html

"The draft Bill also contains a power for the Secretary of State to place obligations on service providers to retain, collect, generate or process communications data when appropriate. Before imposing obligations the Secretary

---

[1] Draft Communications Data Bill impact assessment (PDF)
[2] Draft Communications Data Bill privacy impact assessment (PDF)
[3] Communications Data Bill - key background information (PDF)

[4] Strategic Defence and Security Review (2010)
[5] Freedom of Information request to the Home Office about the Communications Data Bill.
http://www.whatdotheyknow.com/request/119629/response/297764/attach/html/3/attachment.pdf.html

of State must consult OFCOM and the providers on which the obligations would be placed. However, there are currently no requirements for Royal Mail to retain postal data and there are no plans for that to change.

"In answer to your specific questions, we have not consulted Royal Mail as we do not currently envisage obligations being placed on them. For that reason we do not expect any costs to be incurred. You will be aware that the draft Bill is undergoing pre-legislative scrutiny by a Joint Committee of Parliament, and is also the subject of a separate inquiry by the Intelligence and Security Committee. As you may be aware, the current threat from international terrorism is judged to be substantial – in other words a terrorist attack is a strong possibility."

The FoI response from the Home Office (above) appears to contain the following admissions: -

The government has no plans to introduce data retention for postal services at this time. The absence of plans appears to imply that there is no need for the postal data retention provisions within this Bill, at this time or foresee-ably.

There is no specific problem at present with criminality relating to postal services which would require data-retention.

There is no specific problem with regard to terrorism relating to postal services, other than the general terrorist threat.

The government has made no consultations about requiring postal operators to gather and retain communications data and may have no information about the implications of this.

In summary, there is no evidence of need and no justification for the postal data retention provisions in the Bill.

A Freedom of Information request to Royal Mail Group[6] also confirmed that the government has not contacted or discussed cost or feasibility with Royal Mail, the UK's largest postal operator.

http://www.whatdotheyknow.com/request/119538/response/295611/attach/html/3/Allonby%20120712.pdf.html

That the proposals for postal data-retention have not been subject to costing and enquiries to postal operator is significant because this suggests that the proposals have not been subject to the normal processes of formal review and justification. The issue is not cost or feasibility but rather the absence of normal challenge and critical evaluation.

Having "no plans" to implement the postal data-retention provisions of the Bill may not be the same as having no intention to implement them. It would be interesting to be able to explore the difference between having "no plans" and having "no intention", in relation to the government's replies.

Legislation is never introduced lightly. With 94 references to postal services, the Bill appears to be carefully crafted for an intended purpose. The government appears to be thinking fairly deeply about retaining postal data, and about the detailed implementation of this.

Could an intention be transformed rapidly into "plans", merely be announcing a budget and a definitive date for introduction?

If the current Bill is been passed, when government decides it is time to introduce data-retention for postal services, there will be no requirement to consult MPs, only to consult Ofcom. Consulting Ofcom is not the same as seeking approval from Ofcom. Ofcom may not subject government proposals to the same level of scrutiny as

[6] Freedom of Information request to Royal Mail about the Communications Data Bill. http://www.whatdotheyknow.com/request/119538/response/295611/attach/html/3/Allonby%20120712.pdf.html

MPs - Ofcom has narrowly defined terms of reference; Ofcom may not be able to challenge government on the security case or many other important issues.

Technological Feasibility

The proposals for postal data-retention are probably quite feasible.

Royal Mail has been aiming towards total mechanisation. Machine-sorting and machine-reading of addresses makes it potentially possible for sorting machines to log mail items to a database. Sorting machines have to read the addresses on mail items – data-retention merely requires outputting this data from sorting machines to storage. A situation where all mail is machine-readable and machine-sorted would make it possible to log all mail.

It needs to be clarified how close Royal Mail are to achieving total mechanisation, but it is believed to be close to 100%.

Where addresses on mail items are not directly readable by sorting machines, the mail items are marked with machine-readable barcodes containing the address information.

The US Postal Service has already created a database of First Class Mail, very much along these lines, with similar technology. This was created to provide a tracking service for business mail customers, to confirm delivery of items and reliability of delivery. In relation to data retention, this creates a database of all business mail[7].

Since the USPS and Royal Mail appear to use similar technology, a brief description may be appropriate. USPS requires discount bulk mail customers to mark their mail with a bar code which contains the address and zip-code and the sender's details (in machine-readable format).

The barcode information is read at sorting machines and stored in a database, accessible to customers, so they may confirm the progress and delivery of individual mail-items.

In Britain, similar address barcodes are used by Royal Mail. Bulk mail customers mark mail items with address barcodes, for machine-reading, in addition to the normal script address. Sorting machines can also read some script type-faces, by Optical Character Recognition.

Royal Mail has aimed to reduce the number of items that require marking, and to maximise the proportion of items that are directly machine-readable. Royal Mail customer agreements for bulk mail services require both address and sender's details to be entered in machine-readable format. Royal Mail uses a system of Customer Bar Codes (CBC, recently renamed simply "Barcodes"), similar to US postal service, for bulk mail customers, as part of Royal Mail services named Mailsort and Walksort. These barcodes contain details of both addressee and sender, in machine-readable format, which are read by sorting machines. For other reduced-rate mail services, which do not require customers to use address barcodes, Royal Mail customer agreements specify preferred machine-readable type-faces which have to be used.

As has been mentioned above, for other items, where addresses are not machine-readable (e.g. private post), a barcode is marked on the item. It is understood that machine-reading has been adapted to recognise the majority of hand-written script, and this is used at the stage of applying barcodes to items on reception.

In relation to data-retention, it is not known whether Royal Mail sorting machines currently record the information they read from these barcodes, or whether they are capable of doing so. It is not clear what data is currently recorded and whether there is any mail database comparable to that in USA. It would be extremely helpful, in relation to postal data-collection, if your Committee could clarify the current situation in the UK.

Europe

---

[7] Stephen Barr - Postal Service Sees Simplicity in 31 Digits
Washington Post, 17 Feb 2008

The European Commission has discussed proposals for adding unique electronic identification to all mail items, using RFID chips[8][9].

The stated motive behind this proposal is in relation to the liberalisation and privatisation of postal services, Europe-wide: - in a situation of multiple new mail-operators, to avoid a fragmented service, the Commission wished to pursue a unified mail-tracking system. It is believed that this is a long-term project and at this stage Royal Mail does not appear to have been approached in regard to implementation – however, this does not mean that this can be ignored.

The implications of this proposal are that it would create a Europe-wide database of all mail, that would interoperable, accessible by multiple different operators in different companies, different nations, and potentially by police and security services in different nations also.

In terms of privacy, it would be very difficult to ensure any meaningful level of privacy under this arrangement.

The RFID system would also be able to gather very much more information, which would make the system much more intrusive and damaging, in terms of impact on privacy.

The EU is very committed to the promotion of RFID technology.

Attractions of RFID, compared with visual barcodes, include the following: -

- greater accuracy, with fewer reading errors
- the RFID chip can contain more information, and can be written with extra information
- it would be possible to identify all the items within a bag, without having to view each item visually

RFID is closely linked to an internet technology called the "Internet of Things" that facilitates open communication of information, globally, across different enterprises. RFID is already is use by many supermarket and clothing chains, and is used to manage complex international manufacturing supply-chains.

RFID would make it possible to collect much more information, more easily, making mail-tracking faster, simpler and universal. It would be possible to track not merely mail sent by businesses, but also to track all mail from each post-box, and to track each stamp sold. The privacy implications will be much greater as each mail item will carry a greater amount of data, and will be able to be tracked in much greater detail. It would be possible to track every Valentine card and love-letter - and every plain brown envelope posted to an MP. This would leave no such thing as private mail.

This makes it more important that the current Bill does not leave the door open to uncontrolled and unlimited expansion of data-collection.

At present, no nation yet has firm plans for the introduction of RFID to the general post. Given the level of support from the EU and major nations, and given the falling cost of RFID chips, it is reasonable to expect that RFID identification of post may become universal within a decade. Some nations, such as China, are already applying RFID to a limited range of services, such as express items. Many postal services use RFID to track mail bags and pallets. The international Universal Postal Union and Royal Mail use a form of RFID to test delivery times, on special sample items of post.

The European proposals will be an important context for any UK measures for retention of postal data.

---

[8] No missing mail with RFID tags, says Commission | EurActiv.com
[9] EU wants RFID chips for its postal services - The Inquirer

It would be useful to know how Britain sees its proposals for postal data-retention in relation to European proposals – whether or not Britain's scheme is seen as a pilot for Europe.

Postal Data Retention and Human Rights

Necessity or Availability?

If this legislation for postal data-retention is not being introduced in response to combat a new type of crime, is it instead being introduced due to technological feasibility, i.e., is this being introduced because it has become possible and easy to implement rather than because it is necessary to fight crime?

The government appears to propose that the test of necessity should only be applied when accessing data, on a case-by-case (or person-by-person) basis, rather than as a test of whether whole categories of data should be collected at all, hence that the government should not need to justify the necessity of introducing a new class of retained-data.

If this became the basis on which new privacy-eroding measures were introduced, this would be a dangerous slippery-slope. Given that technological capability is constantly growing, this would lead to continual expansion of government access to personal data and corresponding erosion of privacy and civil liberties.

Retained data might initially be applied to fighting serious crime, but the rapid increase in the capability and reach of computer systems over time would enable an expansion in its use, leading towards the use of retained-data in the enforcement of minor regulations.

Data-retention has itself been made possible by the extremely rapid increase in available computer power, and the rapidly falling cost of storing data – a report by the Brookings Institute has described this as a potential threat to civil liberties [10] - and it is only reasonable that the use of retained-data should also be considered in this context.

Function-creep has been a constant in the growth of the database-state.

Proportionality?
How would the data be used?

Having "no plans" to retain postal data means that (perhaps conveniently) the government does not have to discuss intended uses for that data.

It is quite likely that, rather being used for a small number of relatively serious offences, such as terrorism-related offences, postal data could be used widely, on a large scale, for minor matters. This is likely because postal “mail cover” data may not be considered "private information", hence would largely escape restrictions on proportionality of use (discussed in more detail below).

Use of this data for minor matters would have a pervasive impact on society.

It appears that the proposals are driven by technological feasibility rather than the need to combat a new type of crime – i.e. this is being introduced because this is possible rather than necessary.

On this basis, it appears that this fails the test of necessity.

Given that technological capability is constantly growing, this would lead to continual erosion of privacy and constant expansion of government access to personal data.

---

[10] Recording Everything: Digital Storage as an Enabler of Authoritarian Governments, John Villasenor, Brookings Institute, December 14, 2011
http://www.brookings.edu/~/media/Files/rc/papers/2011/1214_digital_storage_villasenor/1214_digital_storage_villasenor.pdf

This Bill is Human Rights legislation, regulating the use of surveillance. As Justice points out, in their report Freedom from Suspicion [11]

> the general provisions of Article 8 ECHR were never intended to be a substitute for proper regulation of the use of surveillance

In effect, Article 8 required the introduction of further legislation to control surveillance. RIPA was introduced in response to this, and the current Bill replaces provisions in RIPA. The current Bill introduces new surveillance powers, but also introduces corresponding new regulation of surveillance. This Bill is thus human rights legislation.

The Bill also contains provisions to for the government to revise and increase the scope of permitted surveillance powers, in Clause 9(7)

(7) The Secretary of State may by order amend subsection (6) so as to add to or

restrict the permitted purposes.

Given that this is Human Rights legislation, intended to define limits on government surveillance powers, it seems strange that the government should be given the right to change and amend the limits of its powers, by order, without asking Parliament. This does not sound like a regime intended to guarantee fundamental rights. The whole point about human rights is that it should not be easy for governments to change or re-write human rights.

Many of the rights of access to retained data are very broadly written, with no apparent minimum threshold to ensure proportionality, for example, in 9(6)

(6) For the purposes of this section it is necessary to obtain communications data

for a permitted purpose if it is necessary to do so—

...
(d) in the interests of the economic well-being of the United Kingdom,

(e) in the interests of public safety,

(f) for the purpose of protecting public health,

(g) for the purpose of assessing or collecting any tax, duty, levy or other

imposition, contribution or charge payable to a government department,

"Public safety", "public health" and "the economic well-being of the United Kingdom" are vague catch-all terms with no indication of proportionate use; (g) by referring to "any" tax, duty or charge, indicates no minimum limit and no proportionality.

The government has suggested it needs these powers in relation to serious crimes. If this is the intention, then surely this should be written into the law. As a suggested example, 9(6b) which currently reads

---

[11] Freedom from Suspicion: Surveillance Reform for a Digital Age, Justice Report, October 2011 http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf

(b) for the purpose of preventing or detecting crime or of preventing disorder could be changed to "preventing or detecting serious crimes" and could be further enhanced by specifying "expected to be punishable by imprisonment of one year or more."

The concept of proportionality has itself been criticised for being a shifting-sand leaves no clearly defined limits and creates impossible grey areas. The concept of proportionality is based on a principle of utilitarianism, in which all rights are elastic and negotiable. A fierce debate has raged for over 200 years, since the earliest days of the US Supreme Court, over this principle and whether it is suitable to define fundamental rights[12].

In regard to the concept of proportionality, Professor Stavros Tsakyrakis of the University of Athens has argued that , "The European Court of Human Rights is routinely balancing human rights against each other and against conflicting public interests and has elevated proportionality to the status of a basic principle of interpretation of the European Convention on Human Rights. ... proportionality constitutes a misguided quest for precision and objectivity in the resolution of human rights disputes and ... courts should instead focus on the real moral issues underlying such disputes." In relation to similar attempts to balance rights in US law, Supreme Court Justice Scalia made the point that one cannot compare the length of a line with the heaviness of a rock.

The approach of proportionality adopted in the ECHR and HRA seems to be a poor way to define fundamental rights, that will leave rights uncertain and vulnerable to erosion over time.

This leads back to the need for Parliament to include clear definitions within the Bill of the limits to lawful use of retained-data.

Under the concept of proportionality, what limits would be placed on access to retained postal data? What would be considered to be a proportionate use would depend upon whether retained postal data was considered to be private data.

In the US, postal "mail cover" information is not considered to be covered by a "reasonable expectation of privacy", thus does not receive constitutional protection. The same applies to any data shared with a third party, such as telephone numbers dialled and even bank account information[13].

This is obviously significantly different to law in Britain and Europe, but it does illustrate the potential problems defining proportionality in relation to retained-data.

In this regard, however, it appears that US law has failed to recognise the qualitative impact when data is collected systematically and placed in a searchable computer database.

How far would a British government be prepared to go in relation to accessing "third-party data" and applying it to general government purposes?

The British government has recently discussed accessing third party data from supermarket store cards, to advise customers to change their eating habits, as part of a public health programme, within the "Nudge" programme of behaviour modification[14][15]. This is a substantial movement in relation to previous attitudes towards access to personal data. Store-card data is extremely powerful, revealing and potentially sensitive[16].

---

[12] Stavros Tsakyrakis, Proportionality: An Assault on Human Rights?, Jean Monnet Working Paper 09/08
http://centers.law.nyu.edu/jeanmonnet/papers/08/080901.pdf

[13] Reasonable Expectation of Privacy, Electronic Frontier Foundation, https://ssd.eff.org/your-computer/govt/privacy

[14] Chocolate again? Loyalty cards could be used to tailor health advice - Telegraph

[15] Supermarket spies: How the Government plans to use loyalty card data to snoop on the eating habits of 25million shoppers – Daily Mail

[16] Big Brother knows all about my bunion op - and the fish pie I ate after it: How one woman found out about the intimate information held about her, By Claudia Joseph, Daily Mail 14th August 2011

This example is potentially of interest in exploring the potential use of private data for purposes of "public health", e.g. in relation to proportionality and the use of Clause 9 (6f) of the Communications Data Bill.

This indicates the potential dangers in relation to concepts such as proportionality and stretching the use of data to minor matters.

Is collecting more data the best solution?

Exploring alternative paradigms in crime-prevention and policing

Will collecting more personal data really help prevent and reduce crime in our society? Is crime detection, policing and punishment the best way to make a safer, more law-abiding society? Do other nations approach these issues more successfully by alternative paradigms? Can we discuss data-retention without considering alternative approaches, which could be more successful without requiring further encroachment on privacy and civil liberties?

Consider one of the serious crime problems mentioned by the government in the case for this Bill: – drugs.

Drugs are a major issue in crime in Britain. Although only about 10% of Britain's prison population have been sentenced directly for drugs offences, it has been estimated that drugs are the motive behind the majority of acquisitive crime in Britain. The NEW-ADAM research, the (2003) report from the Number 10 Strategy Unit claimed that over half of all property crimes were drug motivated:

> "Heroin and/or crack users cause harm to the health and social functioning of users and society as a whole, but users also commit substantial amounts of crime to fund their drug use (costing £16bn a year)". (p.2)
>
> "Drug use is responsible for the great majority of some types of crime, such as shoplifting and burglary " (inc 85% of shoplifting, 70-80% of burglaries, 54% of robberies)[17]

Survey has found that 60% of criminals are users of hard drugs [18] [19].

Although there is no question that Britain is required, for example by international treaty, to make every possible effort to stop the trade in drugs, the nations that have had the greatest success in reducing narcotics-use have done so by programmes of harm-reduction rather than direct policing. For example, cannabis-use in the Netherlands, which has adopted socially-controlled harm-reduction, is substantially lower than in neighbouring countries, which have adopted more traditional approaches of criminalisation and direct policing[20] .

Direct policing has dismally failed to stop the narcotics trade. There is no sign that new policing measures will be any more successful at stopping the drugs trade. Hard drugs even penetrate Britain's prisons, with widespread availability and prisoners complaining about leaving prison with more serious drug problems than when they entered [21][22][23].

---

[17] Strategy Unit Drugs Report – Phase I, Prime Minister's Strategy Unit (2003) – p.25
[18] Trends in drug use and offending: the results of the NEW-ADAM Programme 1999–2002, Home Office RDS
[19] 60% of criminals take hard drugs, Nick Paton Walsh and Jason Burke, Guardian, Sunday 20 May 2001
[20] Dutch drug policy in a European context http://www.cedro-uva.org/lib/boekhout.dutch.html
[21] Drug abuse rising in overcrowded prisons, study finds Guardian, Friday 13 August 2004
[22] One In Eight Prisoners 'Develop Drug Problem In Jail' PA/The Huffington Post UK | 17/04/2012
[23] Ex-cons speak out over drug abuse in HMP Gloucester This is Gloucester | Friday, August 03, 2012

Is it really justified to introduce measures such as communications data-retention, with a serious adverse impact on civil liberties, in yet another (likely futile) attempt to stop narcotics by direct-policing?

Britain imprisons a higher proportion of its population than most European nations (only Spain is higher) [24].

This is reflects attitudes to civil liberties in different nations - how readily respective governments remove the liberty of citizens by imprisoning them.

The British government uses imprisonment in preference to more effective harm-reduction and crime-reduction strategies.

Let us consider an example of how postal data might be used in practice: - to investigate suspected benefit-fraud. As a typical illustration, consider the case of a woman who might be claiming benefits as a person living alone, having recently separated from her husband, but is suspected to be cohabiting. An investigation based on retained postal data might reveal that she might still be receiving post for an estranged husband, thus would appear to be cohabiting. This woman might have reverted to her maiden name after separation, yet might be receiving post for two different names: - her maiden name and her married name.

In situations such as this, would access to postal data answer the questions or merely raise more doubts? Is it likely that postal data would merely provide a justification to investigate with other, more intrusive forms of surveillance, such as directed surveillance?

This situation illustrates the complexities of real life. Real lives are often not simple and clear-cut. Relationships often do not start or finish neatly. Divorce law recognises that separation can be an on-off business, with many attempts at reconciliation. A married couple may be legally separated, yet still living together in the same home.

Rather than gathering more personal data, in an attempt to determine personal circumstances, would it be simpler and better to redesign systems so that we no longer require to investigate such situations? Rather than gathering more intrusive personal information, why not design a simpler benefits system? Gathering more data about such people and circumstances would not explain or clarify their situation. It is undignified to force people to explain these situations, and often any explanation may be inconclusive or open to doubt.

It is interesting to make comparisons between communications data retention and the ANPR (Automatic Number Plate Recognition) network on Britain's roads.

The analogy between communication data retention and the ANPR network applies because the ANPR system was largely created by retaining privately-generated data, making this available to the police. The introduction of the ANPR system was widely regarded as a major development in mass-surveillance, yet it was never voted on or debated in Parliament. Apparently, this was not regarded as a Human Rights issue, presumably because the movement of vehicles on roads is publicly visible to anyone, rather than being private, in much the same way as "mail cover" information is publicly visible and not regarded as private information under US case law.

The police and Home Office claim the ANPR system has had a major impact in terms of arrests and use by police, but it is interesting to see if this has really been effective in reducing crime and harm on roads, and whether alternative measures would have been more effective with less impact on privacy.

The ANPR network introduced in 2005 as part of Project Laser was based upon retaining data generated within privately-owned systems. The majority of cameras in the ANPR network were privately-owned and had been created for private purposes, not as a national police surveillance network - only a minority of the cameras were police cameras, installed to fill gaps in the network. The privately-owned cameras were in systems such as at petrol-station forecourts (used to prevent motorists driving off without paying) and the TrafficMaster information system (which was used ANPR to obtain live information about traffic speeds on trunk roads). TrafficMaster used ANPR to identify vehicles at different points along a road, and by timing them from point to

---

[24] Prison population statistics, House of Commons Library, SN/SG/4334 24 May 2012

point, determined average traffic speeds. Having timed the vehicles, TrafficMaster then "forgot" the individual numbers, because it was not intended as a surveillance system. However, the police (ACPO) then stepped in and asked TrafficMaster to provide them with the number-plate data from their cameras, which the police retained.

For the ANPR network, the police have cited large numbers of arrests, stolen vehicles recovered, uninsured stopped or seized. However, the real measure of success should be whether the ANPR has led to reduced rates of crime, uninsured vehicles and accidents.

However, despite the use of the ANPR network to detect untaxed and uninsured vehicles on the roads, Britain still has the highest proportion of uninsured vehicles on its roads in Western Europe [25] .

Britain was the first nation to deploy ANPR and comprehensive recording of vehicles on roads; Britain continues to have the greatest commitment to this approach in Europe. If ANPR was the most effective means of tackling the problem of uninsured vehicles, Britain should now have the lowest level of uninsured vehicles. However, Britain has a higher level of uninsured vehicles than most European nations. From this, it appears that the alternative approaches to controlling vehicle safety and vehicle crime adopted by other European nations may have been more effective than policing by ANPR and universal surveillance.

The Home Office believes the answer is to expand the system yet further, by linking fuel sales to the ANPR network, making it impossible to buy fuel without an insured vehicle [26]. It seems that the system will continue to grow, add functions, and become more intrusive.

It is also worth noting that the UK ANPR system also had a European dimension. The ANPR system was intended as part of a larger plan, which included access to car, driver and insurance details. At about the same time the ANPR system was introduced, in 2005, Britain signed the Prum Convention (which had been in negotiation and planning for some time) which created a Europe-wide exchange of vehicle information and vehicle insurance details, and required insurers to provide live electronic information about vehicle insurance. The UK's ANPR system was very much interlocked with Europe's plan for data systems. In relation to communications data retention, and postal data retention, this illustrates how crucially important it is to consider EU plans and the larger EU context.

It has been argued that the ANPR system is actually more useful to police in terms of crime intelligence. However, in relation to crime, it has been argued that the ANPR system generates too many leads, and has distracted police time from targeted policing priorities. The difficulty in prioritising a huge number of ANPR leads was argued to have been a key factor to the tragic case of the “Facebook Killer” in Darlington, where a known sex-offender with live arrest warrants was left free to kill a teenage girl, despite being flagged repeatedly on the ANPR system [27] [28]. Could the police resources absorbed by ANPR have been deployed more effectively, if applied to an alternative approach or crime-control?

Despite the level of arrests generated, the lesson from ANPR is that mass-surveillance and more data is not the route to a safer society. The ANPR system remains controversial: - could we have done more to improve public safety without taking this major step towards a surveillance state?

---

[25] UK still has most uninsured drivers in Western Europe Louise Meeson Insurance Age | 29 Jul 2010

[26] CCTV at petrol stations will automatically stop uninsured cars being filled with fuel, Downing Street officials hope the hi-tech system will crack down on the 1.4million motorists who drive without insurance
By Martin Fricker, Daily Mail 12 Mar 2012

[27] IPCC chief: ANPR is 'a victim of its own success' The commissioner of the Independent Police Complaints Commission (IPCC) has said there are severe difficulties in running automatic number plate recognition systems, Guardian Government Computing, Monday 14 February 2011

[28] IPCC publishes findings from investigation into police response to ANPR intelligence on Peter Chapman 11 February 2011, http://www.ipcc.gov.uk/news/Pages/pr_110211_clevelandchapman.aspx

The role of retained-data in police-work is likely to expand in proportion to the range of data available. However, as we have seen with vehicle data from the ANPR system, a high level of use of such data, or a high rate of arrests based on that data, does not indicate that policing has been made more effective than if the data was not available and police had to rely upon alternative methods.

Unfortunately, once a major investment has been made in a mass-surveillance system, such as ANPR or communications data-retention, there is institutional momentum to continue further in the same direction – the greater the public commitment, the more difficult it becomes to consider alternative approaches. The more controversial and unpopular a decision, the greater the importance of justifying it, and the more difficult it becomes to retreat.

It may be desirable to consider other tests than necessity and proportionality in relation to proposals to collect more personal data. Necessity and proportionality are the tests regarding compliance with the European Convention on Human Rights and the HRA. Necessity and proportionality would be the relevant tests if the intention was to allow access to the maximum amount of data permitted by the ECHR and the HRA. Is this the intention, or would it be desirable to make access to data more restricted?

Rather than merely ask about necessity and proportionality, would it be better also to ask questions such as: - How would this data by used by public bodies? How would this affect methods of working and relationships between the public and institutions? Will this lead to a situation where ordinary people have to remember and justify their lives in impossible detail? How will this affect our society? What price are we prepared to pay for privacy, which is an essential part of personal freedom? Are there better alternatives to retaining personal data?

Despite the potential threat of terrorism, Britain is probably more secure today than at any time in the last 400 years. Recently, the Royal Navy sent all of its warships abroad, and did not require to keep a single ship in domestic waters[29].

During the Olympics, security services considered that there was never any threat from major terrorist organisation [30] (30).

These are not the times in which new security measures are needed.

It is understandable that the Home Office and the police should come to be concerned with potential threats of crime and terrorism and regard these as requiring new policing measures and new powers. The question is whether these concerns are justified, and outweigh the needs for privacy and constitutional protection of liberty.

At present, it appears that more policing may not be the most appropriate solution to the most significant crime-problems in our society, and that non-police measures, based on harm-reduction and social inclusion, have the potential to reduce crime and increase public safety far more than increased policing.

Summary - Outstanding Questions

Ideally, the summary should be a set of firm conclusions or recommendations, however in this case the summary appears to be a set of important questions which the government has failed to answer.

The provisions for postal data-retention are profound and far-reaching - I hope you will not approve this legislation unless satisfactory answers are provided to the following questions.

i) Why has the government included provisions for postal data-retention in the Bill if it has “no plans” to implement them?

ii) What does the government mean when stating it has “no plans” to require data-retention by Royal Mail and other postal operators?

---

[29] UK waters left unprotected by Navy warships in October BBC News - 1 Nov 2011
[30] Unpredictable lone wolves pose biggest Olympic security threat Guardian - 9 March 2012

iii) What specific problems in relation to crime and criminality would require the introduction of postal data-retention? Is there any new form of crime?

iv) What is the government case for postal data-retention? Why is postal data-retention "necessary" (in terms of the HRA)?

v) Why did the government make no mention of the case for postal data-retention in any of its publications about the Bill?

vi) Is the introduction of postal data-retention being driven not by crime but instead by potential ease of implementation? Is this being driven by technological capability rather than by crime?

vii) What next? Where will it end? If government is allowed to encroach on privacy simply because technology has made it possible, given the onward march of technology, can we expect successive incursions to follow, until there is very little personal privacy left?

viii) How is it envisaged that retained postal data would be used? What purposes is it required for?

ix) How much cost and effort would be required for Royal Mail to output address data from sorting machines, to create a database of all mail-items? Are the sorting machines already capable of providing this output, or would they require conversion or replacement?

x) Has Royal Mail already created a database of mail items, for tracking purposes, similar to that created by the US Postal Service?

xi) What EU proposals are there that may be relevant to postal data-retention?

xii) In relation to "proportionality", what would be the appropriate minimum threshold for access to retained data? Should this be reserved only for serious offences, or should the data be allowed to be used for minor matters? Is there a "reasonable expectation of privacy" in regard to retained postal data, or should it be regarded as "publicly visible" information?

xiii) Do the provisions in Section 9(6) have an appropriate minimum threshold, to ensure that they are only used proportionally?

(6) For the purposes of this section it is necessary to obtain communications data

for a permitted purpose if it is necessary to do so—

(a) in the interests of national security,

(b) for the purpose of preventing or detecting crime or of preventing disorder,

(c) for the purpose of preventing or detecting any conduct in respect of

which a penalty may be imposed under section 123 or 129 of the

Financial Services and Markets Act 2000 (civil penalties for market abuse),

(d) in the interests of the economic well-being of the United Kingdom,

(e) in the interests of public safety,

(f) for the purpose of protecting public health,

(g) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,

What wording would limit access to proportionate use, in cases of appropriate seriousness?

xiv) If retained postal data becomes available for use in minor matters, what effect would this have on police and other services?

xv) In a piece of Human Rights legislation, which is required by the ECHR, and is intended to define the limits of government power, to protect personal rights and privacy, is it appropriate to have the provision, in Section 9 (7), for government to expand its powers by order?

(7) The Secretary of State may by order amend subsection (6) so as to add to or restrict the permitted purposes.

Is it appropriate to make it easy for government to change legislation relating to human rights?

xvi) How do the postal data retention measures in the Bill relate to the European Union? Does the Commission or do other EU nations have an interest in adopting postal data retention? Could the retention of postal data in Britain become, in effect, a pilot for postal data-retention throughout Europe?

xvii) What other nations have introduced similar measures for comprehensive postal data-retention? Why does Britain need this if other nations do not?

xviii) Have other nations tackled their crime problems more effectively than Britain, by other methods, without resorting to data-retention and data-surveillance?

xix) Are there alternative paradigms for crime reduction other than increased policing and ever-further encroachments upon civil liberties?

August 2012

AVAAZ

Please accept this letter as a formal submission to the Joint Committee regarding the Draft Communications Data Bill. The submission is a petition, coordinated by the global campaigning group Avaaz.org amongst its UK based constituents.

In the last five months, 93,434 people have signed the petition opposing the current draft of the Communications Data Bill. The text of the petition reads:

"To David Cameron, Nick Clegg and Theresa May:

As concerned citizens we urge you to immediately drop plans for an Internet big brother bill (The draft Communications Data Bill). Our democracy and civil liberties are under threat from the excessive and unnecessary internet surveillance provisions without any judicial oversight in this bill. We hope you will protect our privacy and keep your election promise to 'reverse the rise of the surveillance state'."

I've attached copies of the signers in text format with this letter. Avaaz's online mobilisation effort is part of a broader civil society movement to speak out against the bill, including efforts by 38 Degrees and the Open Rights Group. We believe this movement demonstrates the broad public opposition to the bill, and former police chief Sir Chris Fox has spoken out against the law[31].

If this bill were to become law, it would make accessible a list of all our communications, including email addresses and phone numbers of friends, family and others we connect with and the time, length and location of those interactions. Although the content of communications would only be visible to police with a warrant, the majority of the British public find this law dangerous because it exposes a treasure trove of information about us to the government but contains almost no safeguards, leaving it wide open to abuse. That is why we're submitting this petition to the Joint Committee, in the hopes they will see sense and recommend the bill proceed no further.

Thank you for your attention to this matter, if you have any questions or concerns I would be more than happy to answer them. We look forward to hearing the results of this public consultation.

August 2012

[31] Sir Chris Fox, the former president of the Association of Chief Police Officers (Acpo), said the proposals were "not appropriate in a free country". http://www.telegraph.co.uk/news/uknews/law-and-order/9183641/New-snooping-powers-could-be-illegal-human-rights-watchdog-warns.html

Steve Ball

I have been a user of the Internet since the late 80's and have been providing Internet connectivity for customers since 1996. I have developed communications equipment, which has been used in businesses large and small, including financial, industrial, educational, and government. I have provided Communications Data for customer disciplinary action and Police action.

I am very aware of how much personal information can be determined purely from Communications Data. With vast databases of the Communications Data of the entire population of Britain it will be very tempting to use Data Mining and Predictive Analytics in a kind of Minority Report pre-crime detection system which will likely throw up numerous false positives and distract law enforcement from important goals like tackling gangs, gun and knife crime, drugs related theft and violence which is very unlikely to be solved by officers searching peoples private communications data. As criminals become aware that their mobile phones track them, and that the Police are routinely reading their private communications data, they will simply move their crime offline and either use untraceable mobiles, or not use mobiles at all. Criminals may also use Communications Data to provide themselves with false alibis while committing crime.

Many people will drop their Facebook, Google, Twitter social media accounts if they believe their private data is being routinely scraped, stored, collated and filtered, and may be open to hundreds of thousands of government employees to browse with nothing more than a signature of a designated person.

Both the Conservatives and Liberals went into the last election promising to "Reverse the surveillance state" created under Labour, but clearly had no intention of doing so; Labour's IMP was simply renamed CCDP when the new government was elected. Since the election not only has this proposal for State monitoring of all communications been put forward, but there are also plans for default on censorship of Internet web sites (Claire Perry's anti-porn campaign), and to make the job complete, the Leveson Enquiry is likely to recommend restrictions on investigative reporting by the press, in the light of the phone hacking scandal.

I find this move to a more authoritarian society under a Conservative government extremely worrying, especially since there seems to be significant cross party support.

The Bill does not mention who will be exempt, or have special restrictions on access to their communications data. I suspect that Government ministers, MoD, SIS, Foreign Office, Treasury, the big Banks, and large corporates will demand exemptions from this bill to protect the privacy and security of their business transactions.

The Bill dramatically extends the capabilities enabled under RIPA, and broadens definitions of a telecommunications service and a telecommunications device such that the Secretary of State can demand that any electromagnetic or electrical device that communicates can be forced to have monitoring built into it, for example all of the 'Smart' TVs with built in microphones, cameras, and face recognition software could be forced to log communications data for people in their own homes, very like the devices in Orwell's 1984. Of course our government would not want to do this, but once this legislation is on the statute books, it is there for any future government to extend as it wants “By Order”.

GENERAL:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

The Home Office is vague about exactly what it hopes to achieve, and especially vague about how it hopes to achieve it. The objectives boil down to making it easier for Police to obtain communications data that they are currently unable to obtain, but the government is vague about what communications data it is unable to obtain, and about exactly how it will fill these alleged gaps in capabilities. The bill seems to be an enabling act, allowing the Secretary of State to "By Order" demand CSPs install specified equipment, and can also "By Order" change who has access to the data collected, effectively rewriting the definition of communications data at any time.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?
There have been a number of claims such as stopping paedophiles, terrorists, and even murderers by the use of these powers although I am not convinced that the powers that appear to be enabled by the bill will prevent crimes although they may be useful, in building a case after arrests. The Bill could be very useful in disrupting protests, and reducing the impact of industrial action, investigative journalists, and in tracking down whistle blowers.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?
This Bill appears to give the Police and numerous government departments access to large amounts of not clearly defined data with nothing more than the signature of a 'designated person'. There have been numerous cases of rogue Police officers accessing PNC and RIPA data for example 'pinging' mobile phones of celebrities for tabloid. There is a ready market for surveillance data as Operation Weeting / Elveden found, although their focus seems to be purely on News International rather than other tabloids or Police corruption.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?
Other countries that have introduced Deep Packet Inspection based mass surveillance of the type suggested in the Bill include China, Iran and Kazakhstan. My understanding is that these countries have found DPI based surveillance effective in detecting and crushing protest against the government. The Arab spring took many dictators by surprise, but in countries where the governments censor, control and monitor the Internet they have been able to avoid or crush uprisings before they have been able to attain critical mass. I have not been able to find instances of governments using DPI for crime fighting, although the governments using it to oppress protest may define their use as fighting terrorism, or preventing crime and disorder. It is my concern that our government will use these draconian monitoring powers to spy on peaceful anti war or anti capitalism and other protesters in case protests leads to disorder, or could damage the economic well being of the country. I suspect that investigative journalists will find it very hard to protect their sources and it is likely that this will cause a significant reduction in whistle blower based investigative journalism, which will make government easier, and much less transparent.

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?
From the many vague reports of the goal of this legislation, the government has said that it is unable to obtain communications data from foreign providers such as Facebook, Twitter, Google, Skype (Microsoft), however all of those providers regularly provide the Police with communications data and more when asked for it, although they may require a court order, if they do not believe it is for detecting or investigating serious crimes or terrorism, e.g. communications data for protest groups. I believe that the dangers of hacking communications to scrape the communications data from them is greater than the usefulness of doing so. The social network providers will provide help in fighting serious crimes at a low cost whereas I expect this Bill's proposal will cost dramatically more than the estimated £1.8B once the usual government providers start riding the gravy train.

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?
If there must be more intrusion into the private lives of innocent British citizens then the government must be completely transparent about exactly what will be monitored and why it is necessary rather than using glib terms such as "Its only the who what when and where, not the contents". This definition may be applicable to postal mail or telephone calls, but when applied to complex Internet communications it is totally unclear what will be monitored and logged. For example if I search Google for "snoopers charter" the

web request would be "http://google.co.uk/search?q=snoopers%20charter". Would the database record "google.co.uk" or the full google request which includes the google search I have requested? Data that people enter on Facebook is even more revealing than Google searches, and when combined with phone calls, texts and location data, gives a detailed profile of millions of people complete with tagged mug shots and a complete timeline. What specifically will be scraped from Facebook, Twitter, Skype etc?
The definition of Communications Data does not touch these vital questions. If the details of every search request are logged then this makes the database incredibly intrusive. From peoples Google searches, Facebook posts and profiles, Twitter feeds, texts and mobile phone location data, it is possible to track everyone more effectively than the Stasi ever could.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?
This Bill as I understand it, is a massive attack on civil liberties, and dwarfs the impact of other legislation. The government clearly wants this legislation (considers it essential) or IMP would have been dropped as promised, rather than simply renamed CCDP. I suspect most MPs have no idea how Orwellian these measures potentially are with most people now living their lives online.

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?
The use of DPI to hack secure communications e.g. with banks and other secure websites will put the users of such websites at risk from rogue Police officers and other government or CSP employees who will have access to the databases. It is not at all clear exactly what will be stored for SSL communications (see 6 above). Banking websites rely on the SSL encryption to keep transactions safe, so hacking the SSL encryption with DPI will expose personal financial information, that could be used by criminals for fraud. If communications service providers are required by UK law to open all of their customers communications data to government surveillance with no precise definitions of what will be recorded, then many will chose a freer location for their services to protect their customers, or perhaps restrict what UK customers can do online. Services such as Paypal will likely be unsafe if SSL Communications Data is logged and open to hundreds of thousands of Government employees, with just a signature. Large corporates and Banks are unlikely to accept surveillance of their transactions, and will demand that they are exempt or protected from this legislation.

COSTS:
9. Is the estimated cost of £1.8bn over 10 years realistic?
The government has been deliberately vague about exactly what will be monitored and exactly what equipment will be used to perform this monitoring so it is very difficult to judge exactly what the cost will be, but we can look at the history of big government IT projects and we can see that the initial (low end) estimate for the cost of the "Entitlement Card" project was also £1.8B, and that project too had a vague definition of how its goals would be achieved. As the ID Card project evolved the scale of the project reduced, scrapping most of the biometrics, and simplifying its implementation, yet the estimated costs kept rising. It was eventually scrapped after wasting undisclosed sums of tax payers' money and achieving nothing of any significant value. This is a Defence / Policing project so bidders will be restricted to the usual companies who regularly fleece the tax payer with over priced poorly specified projects that dramatically increase in cost as the projects goals chop and change during the implementation (Aircraft Carriers?).

At a time when even basic services are being cut to the bone it is madness to waste what will likely be many billions of pounds on an invasion of privacy that is very unlikely to prevent much crime. The money would be better spent on conventional policing, and crime prevention such as tackling the problem of drugs, guns, knives, and gangs. For higher level crime we need look no further than the Banks (money laundering for dug gangs and terrorists, manipulating interest rates for personal gain, tax evasion, financial fraud). By actually prosecuting banking criminality rather than simply focusing on crime committed by the poor people, trust in government and the rule of law might be enhanced. I suspect the Banks will demand to be excluded from this legislation to protect their business transactions.

10.The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5 6bn. Is this figure realistic?
This figure has been suggested but there has been no breakdown of exactly where these benefits would come from. If the government is really serious about this bill being a money spinner then it should produce a detailed break down of exactly where this money could come from and provide relevant current figures so that if this project is implemented then the actual figures can be measured by every one to see exactly what the financial impact is. I suspect that these figures do not include the cost to the country of communications data being used by criminals to commit fraudulent financial transactions, or to extort money.

SCOPE:
11.Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?
The Bill has a similar definition to RIPA and the Data Retention Regulations, but I can find no mention anywhere of Facebook, Google, Skype and other providers which are alleged to cause problems. This deliberately vague definition and the ability of the Secretary of State to redefine what equipment must be installed by CSP "By Order" effectively allows the government to monitor what it likes. When I have asked specific questions about what will be monitored I have been told that this is not disclosed. We must simply trust this and every future government not to abuse these undisclosed powers. The definition of a CSP is very broad and could include anyone who operates or has control over any communications device, which could be everything form TVs to ADSL routers to PCs, and Tablet computers, so manufacturers of consumer electronics could be forced to install surveillance software on devices in our homes.

12.Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?
There is a vast list of government departments that can access communications data, and I am concerned that access to personal communications data will become routine among many government departments as fishing trips to see if there is anything of interest. As the numbers of requests increases, the oversight for each request will reduce. The chances of staff, criminals, tabloids, and private investigators getting illegal access to private personal communications data is great. Should so many government agencies be investigating "serious crime and terrorism" which is the stated reason for the invasion of privacy? Surely if there is criminality then the police should investigate and there should be no problem in getting judicial authority for access to communications data.

13.How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?
Google, Facebook, Twitter, Microsoft (Skype) already provide communications data for UK Police and only refuse data if they are not convinced that the data is legitimately required, but will comply with court orders. The government would not be likely to persuade these providers to allow direct real time access to their databases, and would be unlikely to be able to force them to comply with requests they feel are unjustified. However using DPI to scrape data out of Facebook, Twitter, Google and hundreds of web mail providers is probably unrealistic due to the frequent changes and the effort to keep changing filters.

USE OF COMMUNICATIONS DATA:
14.Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?
The Bill appears to give almost unrestricted access to communications data which I believe is open to abuse, e.g. Police simply needs to be considering investigation a crime or possible disorder. All requested for communications data should require judicial authorisation.

15.Is the proposed 12 month period for the retention of data too long or too short?

SAFEGUARDS:

16.Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?
The Bill puts no limit on the number designated senior officers and allows them to delegate authority to other staff. Busy Police officers are likely to create many designated officers as the number of requests for data increases. Police will likely use this surveillance database as their first call in any investigation, and criminals may manipulate it to provide false alibis. There should be a requirement to request all communications data through a judicial authority, and there must be a good reason to intrude on the private life of individuals. Without judicial oversight I don't think this legislation can properly comply with Article 8, but I am not a lawyer.

17.Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?
See 16 above. Perhaps Police might get out on the streets more and do standard conventional policing rather than sitting in their office searching through peoples private communications data. There must be judicial oversight of all requests for personal data, if its easy it will be routine, if its routine, it will be abused, officers can make good money selling access to mobile phone locations.
If the government wants safeguards against abuse of surveillance then it should be mandatory for the victim of surveillance to be informed of the surveillance and the reason on every occasion when legal action is not taken within 12 months of the surveillance. This will clearly highlight any unjustified use of surveillance although I doubt very much that the government would want to alert innocent people to abuses of these powers in this way.

ENFORCEMENT:
21.Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?
There is a strong tendency among the Police to close ranks and protect there own, and there will be a reluctance in government to have any abuse of these powers reported in the press so I suspect that most abuse of these powers will be dealt with by light touch internal disciplinary measures. There should be mandatory jail time for abuses by those applying for surveillance that is not justified, and minimum fines for every designated person that authorised the requests. This would make people more careful, and would reduce fishing trips.

TECHNICAL:
22.Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?
Using Deep Packet Inspection the contents of data communications can be examined to take the communications data element from the stream. In order to examine SSL based communications (https) as used in banking Gmail and many other online sites it is necessary to employ a man in the middle attack and have access to the providers private keys, or use a fake SSL certificate to keep the browser happy and allow the equipment to access the communications with the security removed. British companies such as Gamma International have been supplying DPI based surveillance equipment to repressive regimes to allow them to monitor secure communications used by opposition groups and dissidents, so that opposition can be crushed, before it can build momentum.

It would be necessary to maintain very large numbers of filters to extract communications data from the data streams of different sites and the task of maintaining these filters as web sites are updated, could become very demanding. Although I think this is possible if not a very practical way to get and store communications data, I suspect that it would result in more than basic communications data being captured, to be sure of getting it all. The storage requirements are likely to be enormous, and if vast numbers of government staff need 'near real time' access to the data then it is likely to be very difficult to both keep it

secure and provide the data near real time, so I suspect that security will suffer.

23.How safely can communications data be stored?
Data *can* always be securely stored, but the cost of security is in the ease and speed of access, so there will always be a trade off between ease of access and security. With the very large numbers of requests for data I suspect that security will suffer and data will fall into the wrong hands. The government has been very unwilling to disclose technical details of this project as they were with the ID Cards project, and I suspect it will be an expensive failure as ID Cards were, or worse an insecure Orwellian monitoring system which is routinely illegally accessed.

24.Are the proposals for the filtering arrangements clear, appropriate and technically feasible?
The proposals for filtering do not mention Deep Packet Inspection, the hacking of SSL with man-in-the-middle attacks or Data Mining because this would alert the media to the dangers of this proposal. I am confident that these highly intrusive tools will be used, but I am not confident that that the goals of maintaining access to communications data from social media and web mail system from all of the thousands of providers on the Internet is at all feasible. It would probably be relatively simple to extract data from twitter, because of its relatively simple format, but the task of maintaining filters for all of the different social media and email sites on the Internet would be an enormous task, and is therefore not technically feasible. If the intention is simply to monitor peoples Twitter, Gmail, Hotmail, Google+ and Facebook posts then it would be feasible.

25.How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?
There are already measures that would circumvent the measures in the draft bill, for example a VPN product that I wrote and my employer sells to customers that provides an encrypted VPN with the traffic split across multiple ADSL lines from multiple ADSL providers (this is for resilience against line and provider failures). The proposed surveillance would have a distributed database across those ISPs but it would not be practical to link the DPI to decrypt the packets, and the data on each provider would only be a fraction of the data stream. As these proposals get closer to implementation (if they ever get that far) then developers of Open Source software who value their privacy will develop tools that have a higher level of security so that they are not practical or are impossible to break. Criminals paedophiles and anyone who values their privacy will use tools that enable them to maintain their current levels of privacy, so all that will be monitored are the stupid and the innocent.

Using high grade encryption to foreign servers would allow those who do not wish to be monitored to pass all of their Internet traffic through a country that does not monitor its peoples Internet traffic or does not share surveillance with the UK. The harder the state attempts to control and monitor the people the harder many people will try to maintain their freedom and privacy.

26.Are there concerns about the consequences of decryption?
My understanding of the current state of the art for mass state decryption of SSL encrypted traffic, is to use a man-in-the-middle attack and a fake or RIPA requested SSL certificates. The browser accepts the SSL certificate and makes a secure connection to the government black box which then makes a connection to the target site, and re-encrypts the traffic. This allows the black box to have a clear text view of the data as it passes through. The problem here is that some implementations of this hacking technique are safer than others, for example the DPI box by Cyberoam used the same fake certificate for every box so they were allowing anyone with another Cyberoam box or access to the shared certificate to access the data e.g. via a wireless link. There is a danger that these proposals will expose the decrypted data to criminals so that they can commit bank fraud, simply by paying or coercing a government or CSP employee to pass on personal communications data. There have been many leaks of data that have been used by private investigators to provide data to clients e.g. News of the World journalists, this will simply be another source.

There are plenty of encryption techniques that will not be possible to decrypt on a mass surveillance basis,

and criminals and people who value their privacy will use these, this will probably result in innocent people who simply want to use the Internet without state surveillance being criminalised.

August 2012

The Bar Council of England and Wales

Introduction
The Bar Council represents and, through the independent Bar Standards Board, regulates over 15,000 barristers in England and Wales. Barristers are independent, specialist advocates who provide a vital, front-line public service and a pool of expertise from which the majority of the judiciary is drawn, on whose independence the Rule of Law and our democratic way of life depend. The Bar Council's members include barristers who regularly advise and appear in court proceedings on behalf of public bodies, including Government departments and investigatory and prosecuting authorities.

It is the view of the Bar Council that the current regime for obtaining information about individuals' private communications and activities is not fit for purpose, and does not provide the protections which we would expect of any liberal democracy. The law's general overreaching of the proper protection of privacy is exacerbated by the failure of the Regulation of Investigatory Powers Act 2000 (RIPA) properly to protect legal professional privilege; a failure which is carried over into the draft Bill. This written evidence lays out the Bar Council's concerns and, in particular, makes recommendations for the protection of legal professional privilege.

"How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?"

The Bar Council has serious concerns about provisions contained within the Draft Communications Data Bill to extend the RIPA regime to include internet and mobile phone based communications data. These fail to strike an appropriate balance between citizens' privacy and the public interest in a society governed by the Rule of Law.

According to JUSTICE, since RIPA came into force there have been at least 2.7m requests for communications data and over 4,000 authorisations for directed surveillance (e.g. watching an individual's home). This excludes warrants and authorisations on behalf of the security services.[32]

In its excellent report, "Freedom from Suspicion: Surveillance Reform for a Digital Age", JUSTICE states:

"RIPA has not only failed to check a great deal of plainly excessive surveillance by public bodies over the last decade but, in many cases, inadvertently encouraged it. Its poor drafting has allowed councils to snoop, phone hacking to flourish, privileged conversations to be illegally recorded, and CCTV to spread."

No doubt public officials – including the police and security services – find it operationally convenient to be able to obtain as much information as possible about citizens' private communications, and to do so covertly, i.e. without the knowledge of the data subjects. But convenience is not the test: the critical question for compliance with Article 8 of the European Convention on Human Rights is whether the gathering, retention, or subsequent use of information is necessary in a democratic society in pursuance of a defined legitimate aim.

Given the evidence that the current regime (which was supposed to bring domestic law into line with the UK's ECHR obligations) has failed to protect individuals from excessive intrusion into the privacy of their communications and other activity, any rebalancing of the system should be in the direction of further restraining the powers of public bodies so that they are targeted at those genuinely under suspicion of serious wrongdoing. The Protection of Freedoms Act was a welcome, if limited, step in that direction. It is

[32] http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf

deeply worrying that the Government now proposes to reverse the modest progress made in the last session of Parliament by proposing a wholesale extension of official access to communications information.

We would add that it is far from clear that the proposals in the draft Bill are compatible with EU law. The powers of Member States to require communications and internet service providers routinely to retain user data were harmonised by the Data Retention Directive 06/24/EC – largely at the insistence of the UK, which held the Council Presidency at the relevant time. It is hard to see how the UK can unilaterally impose a requirement on communications and internet companies to retain, and permit official access to, wide categories of data beyond those defined in the Directive. Indeed, the compatibility of the existing Directive with privacy rights is currently awaiting consideration by the Court of Justice of the European Union on a reference from the Irish High Court. That follows a series of decisions of various Member State courts (including the German Constitutional Court) striking down domestic legislation transposing the current Directive on grounds relating to infringement of privacy. Given that the main policy driver behind the Bill is the perceived external threat to national security, it makes sense from a political as well as a legal standpoint for measures of this kind to proceed on the basis of European consensus.

Legal Professional Privilege

One issue of particular concern to the Bar Council, given our close interest in issues relating to administration of justice, is legal professional privilege (LPP) – the right to private communication between a lawyer and their clients. RIPA makes no mention of LPP, and consequently the relationship between LPP and the authorities' powers to obtain private information was never debated when the Regulation of Investigatory Powers Bill was before Parliament. The power to override LPP only came to light with a 2009 judicial decision of the House of Lords, In Re McE.[33] The present state of affairs is highly unsatisfactory. We respectfully invite the Committee to urge the Government to (a) take the opportunity of the proposed legislation to restore the protection of LPP in relation to existing RIPA powers, and (b) ensure that any new powers similarly respect LPP.

Background: RIPA and LPP

The right of a person in custody to private consultation with a lawyer is expressly protected in statute. Section 58(1) of the Police and Criminal Evidence Act 1984 (PACE) declares: "A person arrested and held in custody in a police station or other premises shall be entitled, if he so requests, to consult a solicitor privately at any time."

The importance of an accused being able to confer with their lawyer in private has also been emphasised in numerous cases on the ECHR, decided in the UK and in Strasbourg. Former Lord Chief Justice Lord Taylor summed up the importance of LPP when he observed that:

"... a man must be able to consult his lawyer in confidence, since otherwise he might hold back half the truth. The client must be sure that what he tells his lawyer in confidence will never be revealed without his consent. Legal professional privilege is thus much more than an ordinary rule of evidence, limited in its application to the facts of a particular case. It is a fundamental condition on which the administration of justice as a whole rests."

LPP is subject to the sensible limitation that it does not protect communications made in furtherance of a criminal purpose. This is sometimes known as the "iniquity exception". It exists to prevent abuse of the lawyer-client relationship.

The need for reform of RIPA became apparent in 2009, when the House of Lords decided In Re McE, a Northern Ireland appeal. The House held that Part 2 of RIPA permits the covert surveillance of meetings

---

[33] [2009] 1 AC 908 - http://www.publications.parliament.uk/pa/ld200809/ldjudgmt/jd090311/mce-1.htm

between defendants and their lawyers, even though no express provision of the Act authorises it and despite the careful protection of LPP by PACE.

Part 2 of RIPA deals with covert surveillance and use of covert human intelligence sources (CHIS). Section 27 of RIPA provides that

"Conduct to which this Part applies shall be lawful for all purposes if (a) an authorisation under this Part confers and entitlement to engage in that conduct on the person whose conduct it is; and (b) his conduct is in accordance with that authorisation."

Significantly, and as a sign of the lack of clarity inherent in the current regime, the judges were not of the unanimous view that section 27 of RIPA 'trumps' section 58 of PACE. Lord Phillips of Worth Matravers dissented, observing (at paragraph 41):

"While RIPA enables authorisation of surveillance of communications to which LPP attaches at common law it does not, in my view, enable authorisation of invasion by covert surveillance of the express rights given by statute to a detainee to consult a lawyer privately. It would not be incompatible with the Convention for power to be granted in exceptional circumstances to carry out such surveillance, but I consider that the power should be granted by a statute that adequately defined those circumstances and prescribed who was to ascertain that they existed."

Lord Phillips summarised the importance of LPP at paragraph 45 when he said that "The rationale for LPP is that it is necessary if clients are not to be inhibited from being frank with their lawyers." His Lordship stated that the concern of the client in these circumstances is that the communication may be disclosed and then used to their detriment.

If the state is able to eavesdrop on legitimately privileged communications for the sake of gathering intelligence, there will be an inevitable 'chilling effect' upon clients, who will feel unable to speak openly with their lawyers. This would seriously undermine the fundamental human right afforded by LPP. It creates a grave risk of miscarriages of justice, a risk which has unfortunately materialised in recent high-profile cases involving use of CHIS and which emphasise the need for LPP to be explicitly protected by legislation.

Undercover police officers PC Mark Kennedy and DC Jim Boyling, infiltrating protest groups pursuant to RIPA authorisations, maintained their cover while fellow protesters were prosecuted and tried for offences. In Kennedy's case (R v Barkshire & Others), "significant non-disclosure" (as the Court of Appeal found) of his role led to 20 overturned convictions and cases dropped against six other campaigners.

The present Lord Chief Justice, Lord Judge, expressed disquiet that an undercover police officer may have been party to legally privileged communications between the defendants and their lawyers. The concerns of the Lord Chief Justice were confirmed in the case of DC Boyling (R v Jordan), when it emerged that DC Boyling had indeed attended meetings with the defendant and his solicitor.

The Barkshire and Jordan cases demonstrate the serious problems likely to arise when persons acting under RIPA authorisations obtain access to privileged information. This is not simply a privacy or confidentiality issue: there are wider concerns about fair trial when serving police officers covertly access privileged information and are in a position to pass it on to the Crown.

The Bar Council's concerns extend beyond the criminal law. An individual who is bringing a civil action against the state could at the same time be subject to surveillance by the state. This could be in circumstances where there is no basis for supposing that the individual is pursuing some criminal purpose rather than genuinely seeking advice on his civil claim. That prospect, in the light of the rationale for LPP

articulated by Lord Phillips, is a disturbing one. It is also ironic, given that RIPA was prompted in the first place by the judgment of the European Court of Human Rights in Halford v. UK, a case relating precisely to a public authority accessing legally privileged communications.

The facts of McE related to surveillance. But the reasoning in the case applies equally to the other covert investigation techniques governed by RIPA: interception of communications, acquisition of communications data and use of CHIS. We say more below about the specific area of communications data in the context of the current draft Bill.

The Bar Council is not the only body to have concerns about LPP in this context. This was highlighted by Nick Pickles, Director of Big Brother Watch, when he gave evidence to the Committee on Tuesday 17 July:

"RIPA explicitly fails to recognise privileged communications. The Bar Council and the Law Society have both been very clear that there is no recognition for privileged communications at all in the existing regime."34

The Government's position to date

The previous Government gave a partial response to In re McE by making two orders under powers contained in RIPA. One order concerned directed surveillance,35 the other CHIS.36 The orders alter the authorisation procedures where the authorities seek to target legally privileged communications. There were also revisions to the Codes of Practice.37

The 'safeguards' supposedly provided by these instruments are insufficient. Where surveillance is intended to acquire privileged information, the Code of Practice provides that it should be undertaken only in "exceptional and compelling circumstances". However, the range of cases in which this "exceptional" course should be taken is extremely ill-defined. The code refers to threats to national security or to "life or limb". In our view, the phrase "threat to life or limb" lacks clarity and, while it may catch (as was no doubt intended) serious intentional offences of personal violence, it could extend to more minor offences where physical injury results from lack of reasonable care or from breach of a duty that gives rise to strict liability. Meanwhile, the test set out in the Code for the authorisation of surveillance that is likely but not intended to acquire privileged information is identical to the statutory test for any authorisation for intrusive surveillance under RIPA; it contains no special protection for privileged material.

The overarching difficulty, however, is that these changes do not address the fundamental point that covert investigatory powers should not be used to target privileged communications. The 'status quo' should, in our view, be the protection of LPP in all but those circumstances in which legal privilege is being abused for criminal purposes. In any event, the orders do not apply to interception of communications and acquisition of communications data.

As such, it will not be sufficient simply to tweak these existing codes of conduct, all of which operate on the assumption that RIPA allows LPP to be violated for investigatory purposes.

It is regrettable that the present Government has so far continued to defend the current RIPA regime in relation to LPP. During the scrutiny of the Protection of Freedoms Bill in the Lords, Baroness Hamwee tabled a New Clause, drafted by the Bar Council, to remedy the position (please see Appendix). In Grand

---

[34] http://www.parliament.uk/documents/joint-committees/communications-data/uc170712ev4HC479iv.pdf

[35] http://www.legislation.gov.uk/uksi/2010/461/introduction/made

[36] http://www.legislation.gov.uk/uksi/2010/123/introduction/made

[37] http://www.legislation.gov.uk/uksi/2010/462/introduction/made

http://www.legislation.gov.uk/uksi/2010/463/introduction/made

Committee for that Bill, the Minister pointed out that that "no-one can regard themselves as beyond the law or immune from investigation or prosecution".38 The Bar Council respectfully agrees. Our proposal would not have placed anyone beyond the law. The New Clause would have preserved the iniquity exception: privilege does not attach to information held, or communications made, in furtherance of a criminal purpose. More importantly, the New Clause simply would have brought RIPA into line with other legislation: see below.

The Minister also referred in Grand Committee to the 2010 decision of the Northern Ireland High Court, RA's application for judicial review, 39 arguing that the court had been satisfied with the safeguards afforded by the revised Surveillance Code of Practice. But in that case the court only dealt with the issue of safeguards in relation to the subsidiary question of how material collected from surveillance should be retained and eventually destroyed. On the central issue of whether the police could properly conduct surveillance during meetings between the applicant and his solicitor, the High Court ruled – not surprisingly – that it was bound to follow In re McE. If anything, this case emphasises the importance of Parliament addressing the question of LPP.

It is significant that RIPA contains no express provision about privilege, so the issue was not debated when the legislation was considered in Parliament. Instead, a significant departure from existing law came about not through open debate and votes by both Houses, but by the retrospective application of rules of statutory construction.

Whenever Parliament has had an opportunity to consider LPP – as in 1984 when PACE was under consideration, and again in 1997 before enacting the Police Act -- it has consistently voted to protect it, subject to provisions which prevent the abuse of privilege for a criminal purpose. Any extension beyond these powers needs to be openly debated in Parliament and in public.

The draft Bill

For all those reasons, the Bill as introduced should contain provisions amending RIPA to restore the protection of LPP.

If any of the new powers proposed by the draft Bill are eventually approved by Parliament, these too should be enacted in terms that provide expressly for the protection of LPP. It is important to appreciate that access to communications data raises confidentiality issues every bit as important as more obviously invasive powers such as interception of content, the carrying out of surveillance or the use of CHIS. In a series of judgments beginning with Malone v. UK (1984) Ser. A No. 82, the European Court has been at pains to point out that information about who called whom, when, for how long, etc., raises privacy issues in principle every bit as significant as interception of content. The distinction between content and data has been further blurred by technological developments such as search engines, cloud computing and voice-over-internet communications. In the context of LPP, information about who consulted which lawyers is itself highly sensitive and, in conjunction with other information available to the authorities, is liable to enable the nature and content of privileged communications to be guessed at with a high degree of accuracy.

"If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?"

---

[38] http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/111215-gc0001.htm#11121597000383

[39] http://www.bailii.org/nie/cases/NIHC/QB/2010/99.html

The Bar Council shares the concerns voiced by JUSTICE, Big Brother Watch, Liberty and others regarding the necessity of extending the interception regime to information which, despite being labelled mere "data", can be extremely revealing.

Nevertheless, we appreciate the need for the authorities to utilise carefully targeted interception and surveillance tools in the interests of crime-fighting and national security. Our primary concern is that the regime on which these new powers will be pinned is not fit for purpose and already overbroad in its reach and effect.

Should the Government choose to pursue the plans laid out within the draft Bill, we urge it to add provisions to amend RIPA in order to protect properly legally privileged communications. We hope that the Committee will appreciate the importance of such safeguards, and we encourage it to consider this issue when making its recommendations to the Government.

August 2012

BCS, The Chartered Institute for IT

BCS is governed by a Royal Charter which defines our purpose: to promote the study and practice of Computing and to advance knowledge and education for the benefit of the public. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

The Royal Charter enables the Institute to admit qualified members; without our 70,000 members we would be unable to undertake many of our charitable activities to promote IT at all levels. Under the Charter, BCS is required to establish and maintain standards of professional competence, conduct and ethical practice for information systems practitioners.

As a professional body, BCS represents its members and the IT Profession as a whole on issues of importance, and liaises with other professional bodies, the government, industry and academics to initiate and inform debate on IT strategic issues. We also deliver a range of professional development tools for practitioners and employees and as a leading IT qualification body; we offer a range of widely recognised professional and end-user qualifications.

Consultation Questions:

General:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

BCS, The Chartered Institute for IT believes that there are inconsistencies between purpose and proposal.

The purpose stated by Theresa May is: "to protect public; bring offenders to justice by ensuring that communications data is available to the police/security/intelligence agencies". However, she also notes that police, the Serious and Organised Crime Agency (SOCA) and Her Majesty's Revenue and Customs already "have access to the full range of communications data." All these agencies are the ones stated by her (above). So, if they already have access 'to the full range' it is not clear why further powers are needed. Later on (and inconsistent with the previous statement) it is said that communications data – regarding email and internet – is less available and harder to access.

It is noted that 'other authorities' have access to communications data, but do not have access to, for example, the location of a mobile phone. It appears then that the location of a mobile phone for 'other authorities' presents a problem. The definition of 'other authorities' however, lists some organisations outside of the scope of the Bill as stated in its purpose (above). The 'other authorities' that are included in the above purpose i.e. a police force, SOCA, intelligence services appear to already be catered for. Additional 'other authorities' are the Scottish Crime and Drug Enforcement Agency, Her Majesty's Revenue and Customs and "any such public authority not falling within paragraphs (a) to (f) as may be specified for the purposes of this subsection by an order made by the Secretary of State." BCS considers this to be ambiguous and of concern.

(Note the list of 'legitimate' purposes (where the right to non-interference is not obligatory), on page 100 of the draft Bill and copied here on page 7, under heading Safeguards. The list is extensive and appears to be wider in scope than the purpose stated by Theresa May quoted above.)

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

The Institute does not believe that the case is entirely convincing. We are of the opinion that there are inconsistencies between the stated purpose and proposal.

On the one hand, the Government says it already has access, but on the other that, 'email and internet' pose problems. Another problem, according to Theresa May's statement, is that currently access to communications data is retrospective and "in some cases the police need to access data in near real time, notably where lives may be at risk (e.g. during a kidnap)."

It is not clear how the proposed Bill addresses this 'near real time' issue – as currently, "the police and some other public authorities" can access specified communications data, after demonstrating it is 'necessary to investigation and proportionate to aim and objective'. As far as we can see in the proposed Bill, such demonstration of necessity (and getting authorisation to access data) remains a requirement. The Institute presumes that the 'specified communications data' mentioned above is only data that providers already hold and that the new aspect of the Bill is to require Internet Service Provider's (ISP) to collect and store communications data (for minimum of 12 months). This would go a long way to address the problem of email and internet communications data.

Again, the problem of 'near real time access' may be helped by ISP's collecting communications data, but a 12 month storage period (or any period longer than, say, 14 days) is irrelevant to this problem.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

By virtue of the fact that information collected showing a person's location (e.g. the mobile phone issue mentioned above) is of particular interest to 'relevant public authorities', added to that is an interest in 'who is communicating with who, for how long, and how often'. This information could be of interest to others who have not been authorised to access it. Despite the extensive requirements of 'security, integrity, codes of conduct' etc. it is very likely, based on evidence from data breaches in the last year that interested parties will gain access.

The collection of data about individuals using digital services is already a growing concern, such as the web browsing tracking, collecting social networking data and profile building. It could be argued that government 'tracking/profiling' in the interests of the security of citizens might be justified. The big difference between commercial interest and the state interest is the impact on and consequences to that individual as a result of state scrutiny. Being a 'suspect' has consequences (sometimes life-changing and traumatic), but a suspect is not a criminal until evidence and a court says so.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

The Institute is interested to know to what extent the measures undertaken in other countries (e.g. China, Russia) compare to what is being proposed here. Arguments often put forward concern the protection of national security and citizens requiring intelligence. The UK Government is not only required to protect the nation, but also to act in the interests to ensure public welfare. These arguments could be equally made in other countries.

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

The Institute is not aware of any alternative proposals that the Government could consider.

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

The Institute has no view on the options beyond those already expressed in the response to previous questions.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

The Institute recognises the difficulties of reconciling the protection of the public while maintaining individual civil liberties in a free society. A more in depth assessment of the proposed provisions of the Bill and their direct impact on individual civil liberties would increase awareness and enable a more constructive debate on the merits of, and the necessity for new provisions.

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base? What might be the effect on business?

The Institute considers this to be feasible. It would certainly be interesting to see whether an argument based on loss of business would influence a government that is apparently responding to the need "to protect public, bring offenders to justice by ensuring that communications data is available to the police/security/intelligence agencies" to the extent that civil liberties and public trust in public authorities could be at stake. For instance, is business interest a higher priority than protecting the public and national security?

Costs:

9. Is the estimated cost of £1.8bn over 10 years realistic?

It is difficult to determine whether this is realistic as the detail is lacking. Government cost predictions on projects are however notoriously substantially under-budget and often not feasible technically.

The Institute believes that the cost of complying with requests from subscribers for personal data via the Data Protection Act 1998 would increase but are unclear if operators or government (thus Freedom of Information Act) could be considered as data controllers for this additional information.
The cost of storing this information can vary greatly between operators dependent on contractual agreements with their suppliers i.e. if they are 'pay as you use' rather than one off payments for equipment.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?

The Institute considers it difficult to make a judgement without knowing what the figure is based on.

Note: on both points (9) and (10) the argument made in (8) above applies – either the proposals made in the draft Bill are vital (to public and national security) or they are not. If they are not, the Government should not be pursuing this line – it is dangerous (to the public), controversial (with due cause), challenging to implement (operational complexities, technical challenges, jurisdiction challenges) and most likely can be bypassed by the very people law enforcement agencies are interested in.

Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

The Institute has no view on the options beyond those already expressed in the response to previous questions.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

a) Police/security/intelligence agencies as specified in the opening section of the Bill, as noted in (1) above.
b) No, not without some stringent protections for the public, and democracy, in place.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

It is difficult to see how communications service providers based overseas could be persuaded to participate in such a scheme. Therefore consideration should be given to what type of information security measures based on legally binding commercial arrangements could be put in place that would meet UK requirements.

It is likely other governments may be interested in the data collected. The Institute would like clarification on whether service providers operating under such governments would be able to legally resist any information requests.

Use of Communications Data:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

The Institute considers it important to use the communication data to detect crimes where many lives could be at stake.

15. Is the proposed 12 month period for the retention of data too long or too short?

It is difficult to say, as the reason (i.e. purpose of the Bill) for keeping data is not clearly stated.
As noted above, in the case of an abduction and risk to life 12 months is not relevant, probably also not relevant to plotting a terrorist activity or street riots. 12 months could however be relevant to a money-laundering investigation, or organised crime investigations.

There seems to be a conflict between Clause 4 Subsection (1a) [which implies use of a rolling 12 month period for each communication data item stored] and Clause 6 Subsection (3) [which implies that each operator can choose to delete data items at regular intervals of less than or equal to one month thus a data item may be destroyed at the 12 month anniversary but at the next pre scheduled interval, variable dependent on operator, post 12 month anniversary].

Safeguards:

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

(i) It is important to note that any system, even with checks and balances, is open to abuse.

(ii) Page 99 of the draft Bill states: The permitted purposes pursue the legitimate aims set out in clause 9(6), namely:

a) in the interests of national security,
b) for the purpose of preventing or detecting crime or of preventing disorder,
c) for the purpose of preventing or detecting any conduct in respect of which a penalty may be imposed under section 123 or 129 of the Financial Services and Markets Act 2000 (civil penalties for market abuse),
d) in the interests of the economic well-being of the United Kingdom,
e) in the interests of public safety,
f) for the purpose of protecting public health,
g) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,
h) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,
i) to assist investigations into alleged miscarriages of justice, or
j) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition
   (i) to assist in identifying P, or
   (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

The Institute believes a warrant system would be more appropriate. This would be resource heavy.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

It is likely that all of the roles mentioned will in practice involve other persons identified to deal with these issues – the scale of what is proposed is likely to exceed the amount of time needed to undertake this very serious work, i.e. ongoing scrutiny and management.

Parliamentary Oversight:

19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

The Institute holds no particularly view about whether the arrangements for parliamentary oversight of the powers within the draft Bill are satisfactory.

Enforcement:

20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

The Institute has no view on the options beyond those already expressed in the response to previous questions.

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

Given the level of assurances and framework indicated in the draft Bill to safeguard the process of access, which emphasise the seriousness of what is being accessed, it would seem reasonable to apply a similarly strong penalty for those who do not take their responsibilities seriously.

Technical:

22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

There is no current technology available to capture/intercept all communication data exchange between Near Field Communication enabled smartphones which are in close proximity.

23. How safely can communications data be stored?

We believe that no guarantee of safety could ever be given.

Note that under "3. Data security and integrity"
A telecommunications operator who holds communications data by virtue of this Part must—
(a) secure that the data is of the same quality and subject to the same security and protection as the data on any system from which it is derived, and
(b) protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure."

In (a) above, the security of data on 'any system from which it is derived' may not be very robust and in (b) this applies to any data held according to the Data Protection Act – and there are many instances of data loss, breach, unauthorised access, etc.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

The Institute believes that they are not at all clear. It is difficult to understand what the proposals are.

113 page 48 states "In practice, the Secretary of State or designated public authority may contract with an approved body to undertake the day-to-day operation of the filtering arrangements. However, legal responsibility for ensuring the effective and lawful operation of the filtering arrangements, and complying with the duties imposed by clauses 14 to 16, will remain with the Secretary of State or other designated public authority."

The Institute would welcome explanation about what the 'contract with an approved body' means. We would like to know who is involved in the approval process and whether this might be outsourced to a private company.

Furthermore, any delegation of operational authority from the Secretary of State to a public authority does not remove ultimate responsibility from the Secretary of State - but what is the practical relevance of that responsibility? What consequences would there be to the Secretary of State in cases of misuse or error (leading to breaches of information)? Past experience has shown that the most a citizen could expect is the

resignation of the Secretary of State. Without proportionate consequences the emphasis on the Secretary of State as 'protector of a code of conduct' that provides assurance to the citizen and general public, is arguably rather meaningless.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?

There are various technical means available to those who wish to circumvent these measures.

Individuals using Near Field Communication enabled smartphones in close proximity may be able to circumvent attempts to capture communication data.

26. Are there concerns about the consequences of decryption?

The Institute has no view on the options beyond those already expressed in the response to previous questions.

August 2012

Mark Benson

General:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

Yes. The Home Office has clearly laid out that it wants a record of what everyone in the UK does on the Internet, regardless of suspicion of guilt.

Running content filters for small and medium businesses which capture some 'communications data' it is incredible to see what information can be gleaned even if you don't have the content of the communication, particularly where web site addresses are concerned. The prospect of any one organisation have access to that much sensitive data (whether stored in one database or many) is frightening.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

No. While there will always be situations where having more information would prove useful, there can be no justification in a democracy for such intrusion into personal privacy, regardless of whatever safe guards are claimed to protect the data and restrict access.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

The proposals do nothing to assuage the potential for misuse. If it can be misused it will be, as we have seen time and time again.

Again, no amount of justification should allow blanket monitoring in a democracy.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

The models for this type and scale of monitoring would be China or Iran. These are not models we should be aspiring to. Courts in Germany, Romania and the Czech Republic have found similar arrangements in their respective countries to be unconstitutional.

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

There is a risk that the UK will be viewed with the same caution and consideration, that those for whom privacy is a consideration, apply to places with legislation like the Patriot Act. I myself avoid running servers in certain countries due to their internet policies and concern for the security of the data.

Costs:

9. Is the estimated cost of £1.8bn over 10 years realistic?

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5□6bn. Is this figure realistic?

Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?
From the perspective of an IT professional the definition of communications service provider is worryingly vague. As an individual who runs his own email server and several servers for small and medium enterprises, the wording of the draft bill "The term 'telecommunications operator' is defined in clause 28 as a person who controls or provides a telecommunication system, or provides a telecommunications service." would appear to consider me a 'Telecommunications Provider'. While there are provisions in the bill to potentially offset the financial impact, the task would be beyond the scope of the services I can provide.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?
I would rather no organisation have access to blanket 'communications data'. It does not matter if this data is in one or many databases, the scope of the monitoring and potential for data mining is frightening. If this comes to pass, access should be limited to Police and the Security Services only, with judicial oversight. At no point should the list of those with access, change without public debate.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?
While it may be possible to seek and obtain the cooperation of the larger players (e.g Google, Facebook etc), the choice and popularity of services on the internet is in a constant state of flux. Pursing them to provide information on uk subscribers that it may not even be aware it has, would be like herding cats.

Use of Communications Data:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

15. Is the proposed 12 month period for the retention of data too long or too short?
Typically, due to storage constraints, servers store logs for a few weeks, with archiving that may be as long as 3 months. Servers or appliances with high throughput may only store logs for a matter of days or not at all. This is usually a design decision and is done to aid maintainability, functionality and usability. The cost of storing the data would likely be disproportionately high for SMEs, let alone the question of how to actually do it in the first place.

Safeguards:
16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?
With respect to Article 8 ECHR, the use of 'communications data' (as mentioned in section 8 of DRAFT COMMUNICATIONS DATA BILL, EUROPEAN CONVENTION ON HUMAN RIGHTS MEMORANDUM BY THE HOME OFFICE) to compare the data collected for a telephone service with that for email or web browsing is misleading as internet data is not charged 'per call'. ISPs do not require this information (i.e. individual email or web sessions) to bill their customers.

The memorandum itself states "*By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified.*".

The justification being serious crimes and ideally, only monitoring of data with a warrant, from that point in time forward. To expect 12 months of data to be on hand for everybody is fundamentally wrong.

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?
A warranty system should be the default case. Only law enforcement agencies should have access via a warrant system. If other public authorities have a case to pursue then they should pursue it thought the appropriate law enforcement agencies. The likely impact would be to deter flippant use of the system. If such a system is ever put in place, the barriers to entry must be so high as to make every use of the system as onerous to those seeking data as the burden to privacy is to the individuals monitored.
18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

Parliamentary Oversight:
19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

Enforcement:
20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?
21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

Technical:
22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?
It is possible to capture data from common ports (i.e. email on port 25, web traffic on port 80), identify that protocol and strip out the communications data. However if encrypted and/or obfuscated it may not be possible to extract any meaningful data.

Capturing data for all ports and protocols may prove difficult. Doing so for all traffic that passes through a large ISP may not be practical due to the amount of processing and storage requirements.

However due to the layered nature of the many and varied protocols that enable communications on the internet, one layers 'communications data' is likely embedded in another layers payload (or 'communications content'). So to state that "Nothing in these proposals will authorise the interception of the content of a communication." is disingenuous because at some point it will be necessary to intercept, store and reconstitute the 'communications content' (however briefly) of one protocol to enable the extraction of 'communications data' of another protocol contained within.

23. How safely can communications data be stored?
That depends on the risks you want to mitigate against and how much money you want to throw at the problem. You need to consider physical security, should the systems be physically isolated and can all ISPs accommodate the requirement, isolated from the network, secure from physical intrusion, safe from adverse conditions (floods, fire, social unrest, theft etc) and user security. One or more people will have to setup and administer the systems. Are they considered fit to have access to that system? What safe guards and penalties are there for staff at an ISP collecting that data?

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?
The proposals are vague when taken in the context of filtering large amounts of data which would require very specific parameters and the likely results would only be apparent after filtering the data. Also determining the precision of the results would require very specific goals that may not be apparent to whoever is doing the actual filtering. The technical feasibility depends on the systems that store the data, how it is stored, the system used to manipulate and filter the data and the skill of the person creating the data filter.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?
There are myriad ways to circumvent the measures in the draft bill. For example, it's as easy as running a Virtual Private Network (VPN), TOR connection or connecting to a Darknet.
It takes minutes to setup a VPN. VPNs are commonly used by business users to securely access their company network from a public network.

TOR obfuscates user traffic allowing the traffic to be routed to random TOR exit points around the world. TOR has been instrumental in opposing repressive regimes around the world.

Darknets are essentially decentralised private networks that anyone can join . They implement their own rules i.e. anonymity and no logging of connection information.
It is also possible to use proxies to anonymize your connection. With anonymous email services that do not require any subscriber information, anonymous remailers and a few of the above it is easy to circumvent the measures in the draft bill.
It is also easy to connect to TOR or a Darknet over a VPN and/or one or more proxies.

26. Are there concerns about the consequences of decryption?
While it may be technically possible, the time and effort required would likely be high unless other means are available i.e. known weaknesses in the encryption, decrypting traffic with trusted certificates or a 'man in the middle' attack or mandated back doors. As these would likely be exploited by criminals and bored teenagers, or quickly detected by security researchers or legitimate users, it wouldn't be long before any useable exploits became public and were 'fixed' or alternatives appeared.

Moreover, decrypting encrypted data to get at 'communications data' would undermine point to point security and render things like internet banking, ecommerce and VPNs untrustworthy.

August 2012

Dr Paul Bernal

The draft Communications Data Bill raises significant issues – issues connected with human rights, with privacy, with security and with the nature of the society in which we wish to live. These issues are raised not by the detail of the bill but by its fundamental approach. Addressing them would, in my opinion, require such a significant re-drafting of the bill that the better approach would be to withdraw the bill in its entirety and rethink the way that security and surveillance on the Internet is addressed.

As noted, there are many issues brought up by the draft bill: this submission does not intend to deal with all of them. It focuses primarily on three key issues:

1) The nature of internet surveillance. In particular, that internet surveillance means much more than 'communications', partly because of the nature of the technology involved and partly because of the many different ways in which the internet is used. Internet surveillance means monitoring not just correspondence but social life, personal life, finances, health and much more. Gathering 'basic' data can make the most intimate, personal and private information available and vulnerable.
2) The vulnerability of both data and systems. It is a fallacy to assume that data or systems can ever be made truly 'secure'. The evidence of the past few years suggests precisely the opposite: those who should be most able and trusted with the security of data have proved vulnerable. The approach of the draft Communications Data Bill - essentially a 'gather all then look later' approach – is one that not only fails to take proper account of that vulnerability, but actually sets up new and more significant vulnerabilities, effectively creating targets for hackers and others who might wish to take advantage of or misuse data.
3) The risks of 'function creep'. The kind of systems and approach envisaged by the draft Bill makes function creep a real and significant risk. Data, once gathered, is a 'resource' that is almost inevitably tempting to use for purposes other than those for which its gathering was envisaged. These risks seem to be insufficiently considered both in the overall conception and in the detail of the Bill.

After looking at these issues from an overall perspective, this submission will address some of the questions specifically asked by the Committee.

I am making this submission in my capacity as Lecturer in Information Technology, Intellectual Property and Media Law at the UEA Law School. I research in internet law and specialise in internet privacy from both a theoretical and a practical perspective. My PhD thesis, completed at the LSE, looked into the impact that deficiencies in data privacy can have on our individual autonomy, and set out a possible rights-based approach to internet privacy. The draft Communications Data Bill therefore lies precisely within my academic field. I would be happy to provide more detailed evidence, either written or oral, if that would be of assistance to the committee.

1 The Nature of internet Surveillance

1.1 As set out in Part 1 of the draft bill, the approach adopted is that *all* communications data should be captured and made available to the police and other relevant public authorities. The regulatory regime set out in Part 2 concerns accessing the data, not gathering it: gathering is intended to be automatic and universal. Communications data is defined in Part 3 Clause 28 very broadly, via the categories of 'traffic data', 'use data' and 'subscriber data', each of which is defined in such a way as to attempt to ensure that all internet and other communications activity is covered, with the sole exception of the 'content' of a communication.

1.2 The all-encompassing nature of these definitions is necessary if the broad aims of the bill are to be supported: if the definitions do not cover any particular form of internet activity (whether existent or under development), then the assumption would be that those who the bill would intend to 'catch' would use that form. That the 'content' of communications is not captured (though it is important in relation to more

conventional forms of communication such as telephone calls, letters and even emails) is of far less significance in relation to internet activity, as shall be set out below.

2 Communications Data and the separation of 'content'

2.1 As noted above, the definition of 'communications data' is deliberately broad in the bill. On the surface, it might appear that 'communications data' relates primarily to 'correspondence' – bringing in the ECHR Article 8 right to respect for privacy of correspondence – and indeed communications like telephone calls, emails, text messages, tweets and so forth do fit into this category – but internet browsing data has a much broader impact. A person's browsing can reveal far more intimate, important and personal information about them than might be immediately obvious. It would tell which websites are visited, which links are followed, which files are downloaded – and also when, and how long sites are perused and so forth. This kind of data can reveal habits, preferences and tastes and can uncover, to a reasonable probability religious persuasion, sexual preferences, political leanings etc, even without what might reasonably be called the 'content' of any communications being examined – though what constitutes 'content' is contentious.

2.2 Considering a Google search, for example, if RIPA's requirements are to be followed, the search term would be considered 'content' – but would links followed as a result of a search count as content or communications data? Who is the 'recipient' of a clicked link? If the data is to be of any use, it would need to reveal something of the nature of the site visited – and that would make it possible to 'reverse engineer' back to something close enough to the search term used to be able to get back to the 'content'. The content of a visited site may be determined just by following a link – without any further 'invasion' of privacy. When slightly more complex forms of communication on the internet are considered – e.g. messaging or chatting on social networking sites – the separation between content and communications data becomes even less clear. In practice, as systems have developed, the separation is for many intents and purposes a false one.[40] The issue of whether or not 'content' data is gathered is of far less significance: focussing on it is an old fashioned argument, based on a world of pen and paper that is to a great extent one of the past.

2.3 What is more, analytical methods through which more personal and private data can be derived from browsing habits have already been developed, and are continuing to be refined and extended, most directly by those involved in the behavioural advertising industry. Significant amounts of money and effort are being spent in this direction by those in the internet industry: it is a key part of the business models of Google, Facebook and others. It is already advanced but we can expect the profiling and predictive capabilities to develop further.

2.4 What this means is that by gathering, automatically and for all people, 'communications data', we would be gathering the most personal and intimate information about everyone. When considering this Bill, that must be clearly understood. This is not about gathering a small amount of technical data that might help in combating terrorism or other crime – it is about universal surveillance and profiling.

3 The broad impact of internet surveillance

3.1 The kind of profiling discussed above has a very broad effect, one with a huge impact on much more than just an individual's correspondence. It is possible to determine (to a reasonable probability) individuals' religions and philosophies, their languages used and even their ethnic origins, and then use that information to monitor them both online and offline. When communications (and in particular the internet) are used to organise meetings, to communicate as groups, to assemble both offline and online, this

[40] See for example the work of Daniel Solove, e.g. *Reconstructing Electronic Surveillance Law*, Geo. Wash. L. Review, vol 72, 2003-2004,

can become significant. Meetings can be monitored or even prevented from occurring, groups can be targeted and so forth. Oppressive regimes throughout the world have recognised and indeed used this ability – recently, for example, the former regime in Tunisia hacked into both Facebook and Twitter to attempt to monitor the activities of potential rebels.

3.2 It is of course this kind of profiling that can make internet monitoring potentially useful in counterterrorism – but making it universal rather than targeted will impact directly on the rights of the innocent, rights that, according to the principles of human rights, deserve protection. In the terms set out in the European Convention on Human Rights, there is a potential impact on Article 8 (right to private and family life, home and correspondence), Article 9 (Freedom of thought, conscience and religion), Article 10 (Freedom of expression) and Article 11 (Freedom of assembly and association).[41] Internet surveillance can enable discrimination (contrary to ECHR Article 14 (prohibition of discrimination) and even potentially automate it – a website could automatically reject visitors whose profile doesn't match key factors, or change services available or prices based on those profiles.

4 The vulnerability of data

4.1 The essential approach taken by the bill is to gather all data, then to put 'controls' over access to that data. That approach is fundamentally flawed – and appears to be based upon false assumptions. Most importantly, it is a fallacy to assume that data can ever be truly securely held. There are many ways in which data can be vulnerable, both from a theoretical perspective and in practice. Technological weaknesses – vulnerability to 'hackers' etc – may be the most 'newsworthy' in a time when hacker groups like 'anonymous' have been gathering publicity, but they are far from the most significant. Human error, human malice, collusion and corruption, and commercial pressures (both to reduce costs and to 'monetise' data) may be more significant – and the ways that all these vulnerabilities can combine makes the risk even more significant.

4.2 In practice, those groups, companies and individuals that might be most expected to be able to look after personal data have been subject to significant data losses. The HMRC loss of child benefit data discs, the MOD losses of armed forces personnel and pension data and the numerous and seemingly regular data losses in the NHS highlight problems within those parts of the public sector which hold the most sensitive personal data. Swiss banks losses of account data to hacks and data theft demonstrate that even those with the highest reputation and need for secrecy – as well as the greatest financial resources – are vulnerable to human intervention. The high profile hacks of Sony's online gaming systems show that even those that have access to the highest level of technological expertise can have their security breached. These are just a few examples, and whilst in each case different issues lay behind the breach the underlying issue is the same: where data exists, it is vulnerable.[42]

4.3 Designing and building systems to implement legislation like the Bill exacerbates the problem. The bill is not prescriptive as to the methods that would be used to gather and store the data, but whatever method is used would present a 'target' for potential hackers and others: where there are data stores, they can be hacked, where there are 'black boxes' to feed real-time data to the authorities, those black boxes can be compromised and the feeds intercepted. Concentrating data in this way increases vulnerability – and creating what are colloquially known as 'back doors' for trusted public authorities to use can also allow those who are not trusted – of whatever kind – to find a route of access.

---

[41] For a more detailed analysis of the human rights impact of the Bill, see my contribution to the *UK Constitutional Law Group Blog*, at http://ukconstitutionallaw.org/2012/07/11/paul-bernal-the-draft-communications-bill-and-the-echr/

[42] For details of the individual data losses discussed here, see Chapter 5, Section 2, of '*Do deficiencies in data privacy threaten our autonomy and if so, can informational privacy rights meet this threat*', available online at http://etheses.lse.ac.uk/321/

4.4 Once others have access to data – or to data monitoring – the rights of those being monitored are even further compromised, particularly given the nature of the internet. Information, once released, can and does spread without control.

5 Function Creep

5.1 Perhaps even more important than the vulnerabilities discussed above is the risk of 'function creep' – that when a system is built for one purpose, that purpose will shift and grow, beyond the original intention of the designers and commissioners of the system. It is a familiar pattern, particularly in relation to legislation and technology intended to deal with serious crime, terrorism and so forth. CCTV cameras that are built to prevent crime are then used to deal with dog fouling or to check whether children live in the catchment area for a particular school. Legislation designed to counter terrorism has been used to deal with people such as anti-arms trade protestors – and even to stop train-spotters photographing trains.

5.2 In relation to the Communications Data Bill this is a very significant risk – if a universal surveillance infrastructure is put into place, the ways that it could be inappropriately used are vast and multi-faceted. What is built to deal with terrorism, child pornography and organised crime might creep towards less serious crimes, then anti-social behaviour, then the organisation of protests and so forth. Further to that, there are many commercial lobbies that might push for access to this surveillance data – those attempting to combat breaches of copyright, for example, would like to monitor for suspected examples of 'piracy'. In each individual case, the use might seem reasonable – but the function of the original surveillance, the justification for its initial imposition, and the balance between benefits and risks, can be lost. An invasion of privacy deemed proportionate for the prevention of terrorism might well be wholly disproportionate for the prevention of copyright infringement, for example.

5.3 The risks associated with function creep in relation to the surveillance systems envisaged in the Bill have a number of different dimensions. There can be creep in terms of the types of data gathered: as noted above, the split between 'communications data' and 'content' is already one that is contentious, and as time and usage develops is likely to become more so, making the restrictions as to what is 'content' likely to shrink. There can be creep in terms of the uses to which the data can be put: from the prevention of terrorism downwards. There can be creep in terms of the authorities able to access and use the data: from those engaged in the prevention of the most serious crime to local authorities and others. All these different dimensions represent important risks: all have happened in the recent past to legislation (e.g. RIPA) and systems (e.g. the London Congestion charge CCTV system).

5.4 Prevention of function creep through legislation is inherently difficult. Though it is important to be appropriately prescriptive and definitive in terms of the functions of the legislation (and any systems put in place to bring the legislation into action), function creep can and does occur through the development of different interpretations of legislation, amendments to legislation and so forth. The only real way to guard against function creep is not to build the systems in the first place: a key reason to reject this proposed legislation in its entirety rather than to look for ways to refine or restrict it.

6 Responses to specific questions raised by the Committee

1 The Home Office has made it reasonably clear what it hopes to achieve through the draft Bill, but as noted above the effect of the Bill could be very different from the aims. The nature of internet surveillance means that rather than being an updating or modernisation of existing law regarding the interception of communications, this is something on a wholly different scale: a form of 'total surveillance', impacting upon vastly more aspects of people's lives than just their 'communications'.
2 The Government has not made a convincing case for the need for the new powers: to justify the vastly higher level of surveillance, compelling evidence needs to be presented that not only is the

threat level high enough but the powers effective enough to make the case. Neither point seems to have been satisfied.

3 As discussed in sections 1-3 above, the proposals in the draft Bill represent a huge intrusion into individuals' privacy: one above and beyond anything in the current landscape.

4 The powers envisaged in the Bill would put the UK amongst the most privacy intrusive in the world. In general, only police-states and other despotic regimes have similar powers.

5 The first and most obvious alternative is simply not to bring in this legislation. If anything, the UK should be looking to reduce the level of privacy intrusion on the internet: tightening the restrictions in RIPA and looking towards a repeal of the Data Retention Directive (and the corresponding UK law). Peter Hustinx, the European Data Protection Supervisor, called the Data Retention Directive the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects – that criticism should be taken much more seriously, and the UK could play a key role in this regard. We should be leading the world in respect for human rights: not in our level of privacy intrusion and surveillance.

6 See 5 above. One overarching piece of legislation would be preferable, but it should be one based on respect for human rights rather than on universal surveillance.

7 This kind of legislation should not be subject to any kind of 'quid pro quo'. There is nothing in the field that compares to internet surveillance.

8 No comment.

9 See 10 below

10 This figure, and the figure in question 9 above is highly speculative – the assumptions made and their reliability should be treated with a great deal of scepticism. I would refer the committee to the analysis by Professor Peter Sommer in his submission to the committee: I fully endorse Professor Sommer's analysis.

11 As noted in section 2 above, the whole idea that communications data and content can be effectively separated is effectively fallacious, and it is hard to see how the definition of communication data can be meaningful in the future, as technologies and their uses develop. In practice, the scope of systems created to effect this legislation is likely to encompass almost all data used not only in 'communications' but in the use of the internet.

12 Those public authorities able to access communications data should be restricted to an absolute minimum, and it should not be possible for the Secretary of State to vary this list by order. Granting such a power to the Secretary of State would be tantamount to building function creep into the legislation (see section 5 above): extensions to powers should require Parliamentary scrutiny.

13 From a practical perspective, these plans are likely to be supremely ineffective, and the result is likely to be more pressure on UK ISPs to provide more data: if Google (for example) aren't likely to comply with regulations, the ISPs through which people in the UK access Google would be expected to intercept and gather all traffic to Google sites, extending the definition of 'communications data' appropriately. Again, this brings in a form of function creep.

14 The definitions in Clause 9(6) are currently so broad that it could be possible to fit almost any activity within the scope of the act. For example, the clause suggests (9(6)(c) 'detecting crime or… preventing disorder', without any clarification as to the seriousness of the crime or disorder that would allow access to be granted. Other terms are even more contentious: Clause 9(6)(d) could be used to justify access to investigate copyright infringement, for example. Though these are, as noted in the explanatory notes to the bill, the same terms as used in section 22(2) of RIPA, that should not be used as a reason to accept the terms: rather, as a realisation that section 22(2) of RIPA is too broadly couched. It is important to understand the impact of the breadth of these terms in combination with the universality of surveillance as discussed in sections 1-3 of this submission. Effectively, what is being put forward by this bill is universal internet surveillance for almost any purpose that the authorities require.

15 No comment.

16 This system seems unsatisfactory. The idea of warrantless access is in itself highly questionable and open to abuse, but if it must be introduced there should be precise definitions – the level of

seniority should be set extremely high and the processes used must be transparent, recorded, and fully accountable.

17 A warrant system would be much more appropriate – but, as noted throughout this submission, the safeguards, and in particular any warrants, should be required to gather the data, not to access the data that has already been gathered.

18 No comment.

19 Arrangements for parliamentary oversight are not satisfactory. As noted in response to q12 above, the Secretary of State should not have the power to vary the list of authorities without Parliamentary oversight. Moreover, bills like these, envisaging compromises in individual's privacy and human rights, would be better with sunset clauses requiring full parliamentary scrutiny at regular intervals and votes in order to renew the powers.

20 No comment.

21 Penalties should be higher, and failure to adhere to the Code of Practice should amount to an offence. However, the key point should be that fewer public authorities should have access to the data, so that offences of this kind should be less likely to occur.

22 Quite simply no! See section 2 of this submission.

23 The failure to understand the fundamental vulnerability of data and systems is one of the biggest problems with the concept of this Bill. Data, however it is stored, is vulnerable. See section 4 of this submission

24 The filtering arrangements are reasonably clear, probably technically feasible, but likely to be inappropriate and disproportionate. They amount to the creation of a search engine of the entire database – and as noted above, that database effectively covers the entirety of people's internet activity. This is the crux of the Bill.

25 As David Davis MP noted, 'only the incompetent and the innocent' will get caught by this bill. The real 'villains' will be able to find ways to circumvent this kind of data gathering. See 'Conclusions' below.

26 No comment.

7 Conclusions

7.1 The premise of the Communications Data Bill is fundamentally flawed. By its very design, innocent people's data will be gathered (and hence become vulnerable) and their activities will be monitored. Universal data gathering or monitoring is almost certain to be disproportionate at best, highly counterproductive at worst.

7.2 This Bill is not just a modernisation of existing powers, nor a way for the police to 'catch up'. It is something on a wholly different scale. We as citizens are being asked to put a huge trust in the authorities not to misuse the kind of powers made possible by this Bill. Trust is of course important – but what characterises a liberal democracy is not trust of authorities but their accountability, the existence of checks and balances, and the limitation of their powers to interfere with individuals' lives. This bill, as currently envisaged, does not provide that accountability and does not sufficiently limit those powers: precisely the reverse.

7.3 Even without considering the issues discussed above, there is a potentially even bigger flaw with the bill: it appears very unlikely to be effective. The people that it might wish to catch are the least likely to be caught – those expert with the technology will be able to find ways around the surveillance, or ways to 'piggy back' on other people's connections and draw more innocent people into the net. As David Davis MP put it, only the incompetent and the innocent will get caught.

7.4 The entire project needs a thorough rethink. Warrants (or similar processes) should be put in place before the *gathering* of the data or the *monitoring* of the activity, not before the accessing of data that has already been gathered, or the 'viewing' of a feed that is already in place. A more intelligent, targeted rather

than universal approach should be developed. No evidence has been made public to support the suggestion that a universal approach like this would be effective – it should not be sufficient to just suggest that it is 'needed' without that evidence, nor to provide 'private' evidence that cannot at least qualitatively be revealed to the public.

7.5 That brings a bigger question into the spotlight, one that the Committee might think is the most important of all: what kind of a society do we want to build – one where everyone's most intimate activities are monitored at all times just in case they might be doing something wrong? That, ultimately, is what the draft Communications Data Bill would build. The proposals run counter to some of the basic principles of a liberal, democratic society – a society where there should be a presumption of innocence rather than of suspicion, and where privacy is the norm rather than the exception. Is that what the Committee would really like to support?

August 2012

Big Brother Watch

General:
Firstly, we would begin by reaffirming our view that the operation and oversight of the Regulation of Investigatory Powers Act is deeply flawed, and to add further legislation that is based upon this Act without first undertaking a comprehensive review of RIPA is negligent to the point of recklessness.

The Bill is so broadly drafted it is challenging to deduce exactly what the Home Office is proposing or how it will work. Part 1 and the numerous delegated powers make detailed scrutiny extremely challenging.

This Bill ends the presumption of innocence as we know it. It represents a shift of targeted surveillance of those under suspicion of either having committed or in the process of committing an offence to surveillance of the entire populous just-in-case some of them eventually commit crimes. The remarks of the Metropolitan Police Commissioner Bernard Hogan-Howe, that these powers are to enable the police to "eliminate the innocent", summates neatly the critical reversal of reasonable suspicion no longer being required to monitor someone's communications.

The Home Office has failed to make any case about why Britain should be the first democratic state to implement this kind of policy. Nor has the Home Office responded to the legitimate concern that this policy adds legitimacy of the surveillance pursued in China or Iran, which British foreign policy has sought to prevent in other countries.
I would also draw the committee's attention to a counter-terrorism whistle-blower who told the Irish Post that the threat of an Irish dissident attack on the London Olympics was deliberately over-stated by the Government and security services. He told the newspaper

"There is no basis whatsoever to support that theory. It appears to be a propaganda exercise by the security services."
In a civil society this change is a fundamental one that cannot be understated. Indeed, it is questionable whether a society that introduced such indiscriminate and widespread monitoring could be described as civil. The Bill makes surveillance the norm and individual privacy the exception.

With respect to 'the wider landscape on intrusion of privacy' we would submit that this is on a par with no other existing piece of legislation, indeed it runs contrary to much of the consumer protection on privacy that Big Brother Watch has campaigned for and supported. For example, we have campaigned for a wider definition of 'personal information' to ensure that non-personal identifiers are included and therefore require consent to be sought before data like IP addresses can be recorded and processed.

The Home Office has also failed to offer any real evidence of how the current powers are lacking. For example, the German Federal Criminal Police Office mentions 381 criminal cases in which law enforcement agencies were hampered by a lack of telecommunications connection data – compared to the more than 6 million criminal offences committed every year in Germany this represents a marginal share of 0.01 per cent. Furthermore, only two of these 381 cases had a link to terrorism, despite repeated claims that terrorism is one reason for retaining telecommunications data. The Home Office has not been able to offer any substantial statistical or comprehensive assessment of the current regime.
It also marks an equally significant change of asking CSPs to monitor use of third party systems. How this will work in light of modern encryption has not been addressed in any substantive way, nor has the wider question of CSPs essentially becoming private surveillance operations. The market response will be for deliberately private by design CSPs to emerge, or means of communicating that defeat the CSP monitoring arrangements.
These technologies are already being launched and developed to address legitimate security and privacy risks, and the Home Office has wholly failed to deal with this issue. For example, various browsers are now

designed to alter the user to compromised Certificating Authorities and have recently started alerting users who are targets of state surveillance via "man-in-the-middle" attacks.

There is a clear risk that the third party services used will incorporate some of these technologies, and at the same time drive consumers to alternative CSPs. As technology improves, the risk is that the Bill leads to an even greater diminishment of capability by exacerbating currently weak demand for these services. Particularly for sensitive and high value businesses, they may well make corporate decisions to relocate to territories that are moving to enhance privacy protection, for example Germany.

Some aspects of the Home Office's presentation of the Bill have been misleading at best. The shift to mobile, web-based communication is revolutionary transition from fixed communications. To describe the proposals in the Draft Communications Data Bill as maintaining an existing capability is wholly disingenuous. Monitoring the use of mobile communications (in particular location data) and the use of email and web browsers is not maintaining an existing capability but developing a wholly new one.

This point is particularly relevant to postal services, which can certainly not be described as either new or technology related, but are included in the scope of the Bill.
From communications data it is possible to deduce a significant degree of someone's personality, habits and condition - whether visiting a place of worship (location data every Sunday at 10am, for example) or accessing legal advice (divorce law firm) or support (Samaritans via e-mail or Alcoholics anonymous website). None of this is possible under the existing capability.

The Home Office has also sought to justify the legislation as being a tool to fight paedophiles and terrorists. Yet the impact assessment for the Bill recognises HMRC are the main financial beneficiary, while a consultation on which public authorities should be given access beyond those organisations named in the Bill is already under way.

This echoes the early stages of the Regulation of Investigatory Powers Act, which was similarly proposed for only a few agencies and for serious crimes but has since been extended to cover hundreds of public authorities and used for trivial matters, in some cases for behaviour that is not criminal.

The Home Office has also sought to paint a distinction between Labour's plans under Intercept Modernisation and the Communications Data Bill based upon the premise that the Bill does not create a 'single database'. This is wrong factually and technically. Then Home Secretary Jacqui Smith wrote in the 2009 consultation foreword: "this consultation explicitly rules out the option of setting up a single store of information for use in relation to communications data."

It is also unclear how the filtering arrangements will work without some element of data centralisation.

The broader point is that the difference between a single database and several separate but connected databases is largely semantic.

As the information Commissioner's response to the 2009 Home Office consultation stated, this fundamentally changes the relationship between the individual and the state
Surveillance in and of itself does affect behaviour. As The German Federal Constitutional Court warned: "Fear of surveillance and the danger that what one says or writes is being recorded and later combed through before being transferred to be further exploited by other authorities can in itself lead to self-censorship and other forms of reticence to communicate with others and to the emergence of more conformist modes of behaviour."
With respect to other countries, the central lesson is to collect less data.

Instead of diverting a significant amount of resource to a speculative IT project, the Home Office should be investing in better forensics capability in police forces to deal with the data they already collect from suspects and in the course of investigations.

The Home Office has recognised even if this project is 100% successful, it will still leave a capability gap of 15%. This is where the real threat lies and the nature of communications evolution means that this figure will continue to grow rapidly, even with this programme.
Indeed, the Home Office has approached the issue from the mind-set of someone who believes that the only thing that needs to be resolved before one could boil the ocean is for a large enough pan to be designed. It misses the wider – and more fundamental – point about the limits of what is being considered. The situation requires a serious re-thinking of surveillance powers, investigatory techniques and not a lazy policy response that has been on the shelf in the Home Office for a decade.

The 90 day detention without charge policy when first proposed was orchestrated and supported by many of the same organisations and individuals that are now calling for this legislation. The Committee will recall the dire warnings of what would happen if the powers were not granted, and note their similarity with many of the arguments now being deployed.
Indeed, as the 7/7 Inquest recognised, it was not a lack of information that hampered that investigation but failures to process and act upon existing information.

This was highlighted in the 7/7 Inquest report, which stated: "Post 7/7 enquiries revealed that between 22nd February and 15th June 2005 there were forty one telephone contacts between mobile phones attributed to Tanweer, Khan, and Lindsay and hydroponics outlets. It is unlikely these could have been detected by surveillance given the large number of untraceable "operational" phones used by the bombers and only attributed to them once their identities and details were known."

The ICO's Surveillance Society Report (2006) makes this point clearly. It states "It is far from clear that even national security will be enhanced through this technology, and that it would perhaps be better served by improving border security and conventional intelligence gathering, underscored by the August 2006 alleged Atlantic flight terrorist plot involving more than 20 Britons. Although the US Administration claimed that the operation showed the need for more advanced passenger data, the alleged plot was foiled by the use of informers, undercover agents and tip-offs, and it is hard to see how advanced ID systems would have provided anything more effective."

The Data Retention Regulations are currently subject to legal challenge and we would support the argument that the existing regulations are disproportionately intrusive and should be reviewed.

Evidence from Germany questions the benefit on criminal investigations. In 2008 data retention came into force, yet the clearance rate for Internet crime in Germany did not change significantly (2007: 82,9%, 2008: 79,8%), nor on the average clearance rate for all crime (2007: 55,0%, 2008: 54,8%).

This Bill would fundamentally reverse the premise that only those reasonably suspected of crimes can be put under surveillance. To suggest there is a legislative balance to this to rebalance civil liberties understates the gravity of this change.

The risk to business goes beyond the effect on CSPs – as recognised by the Vice President of the United States at the UK's cyber security conference when he said: "When businesses consider investing in a country with a poor record on Internet freedom, and they know that their website could be shut down suddenly, their transactions monitored… they'll look for opportunities elsewhere."

There is also a clear risk that the system will hamper innovation by CSPs. The Bill makes provision for the Home Secretary to specify "equipment or systems" to be used. This will become a requirement of operation in the UK, so the future architecture of CSPs will be designed around integration and operation with the required equipment. Accordingly, the Home Secretary's specified equipment will become a constraint on the CSP and networks, hampering innovation and putting the UK at an economic disadvantage.

This is particularly critical at a time when 4G mobile networks and fibre-optic broadband are being explored, both hugely important to economic growth. However, the wider issue is that unforeseen technology may be simply incompatible with the UK's infrastructure as a result of the Home Office's requirements. Given the history of Government IT projects it is not credible to think that the Home Office will be able to keep pace with technology by frequently updating its specified equipment and systems, and this may also incur significant costs.

There is also a question of whether this creates competition issues between those providers covered by an Order and those not. Equally the ability of organisations to properly secure the data collected will depend on their ability to invest in security provisions, an issue not explored in the Bill's impact assessment either in terms of the cost to suppliers or the impact on different size providers.

Costs

In light of the fact that the Home Office has refused to publish a breakdown of how the £1.8bn figure is calculated, it is fair to say that this project bears all the hallmarks of previously catastrophic Government IT projects and that the estimated cost is not realistic.

Indeed, when asked about the likely escalation of costs in parliament, the Minister himself could not bring himself to say that he had confidence in the cost estimates. (9 July 2012 : Column 16)

Particularly given the nature of this project, there is a clear question about whether the filtering provisions are based upon claims from suppliers about products that could deliver this functionality. As the Public Administration Committee recognised, Government is not an 'informed buyer' of technology products and is heavily beholden to suppliers for expertise. Sadly this relationship has been frequently abused by suppliers, often in near-monopolistic or cartel-like fashion,

The project goes against several tenets of procurement best practice, including the Cabinet Office's own benchmark that projects worth over £100m should not proceed. If the Home Office's openness in the legislative process is any indicator, the likelihood is that this will produce a proprietary solution that will not be an off-the-shelf product, requiring on-going maintenance that cannot be sourced from another provider. This 'lock-in' is a major driving factor in cost escalation in future years.

It is also worth noting that one of the critical failures in the IT procurement landscape is the inability of the public sector to accurately detail the specifications of the required system. Given that the services involved will by their nature have to change regularly, this challenge is even more pronounced in this case and therefore the magnitude for unforeseen 'change request' costs much greater.

It should also be noted that these problems are not 'legacy' issues –a report published in July 2012 by the National Audit Office (NAO) found that the delivery of a £385 million Immigration Case Work (ICW) IT system for the UK Border Agency is a year behind schedule and exceeded its original 2011-12 budget by £28 million. The report went on to say "We found [the IT project] had suffered from a loss of focus, poor governance structures and optimism bias in planning and reporting."

The Home Office has also refused to publish a breakdown of the benefits have been calculated, further suggesting they will not stand up to scrutiny. Indeed, the history of 'criminal asset recovery' is characterised by hugely over-ambitious estimates of the financial amounts involved. The Committee will recall the Asset Recovery Agency's track record of not even recovering enough to cover its own costs.

Scope

The definition of communications service provider is so broad as to be almost meaningless. As Paul Bernal at the University of East Anglia law school says, the draft Bill is so broadly written it could even be used to monitor carrier pigeons.

In defining communications systems, the phrase "signals serving for the actuation or control of any apparatus" [s28(1)(a)(ii)] is so broad it could include a television remote control, a wireless thermostat or door entry systems.

The inclusion of the details of "the use made by any person of a postal service" is extremely broad and equally unprecedented.
Which public authorities should be able to access the data is intrinsically linked to the purposes for which data can be accessed. If the supposed 'gap' the Home Office has referred to is a threat to national security and public safety, it is puzzling why HMRC are also able to access communications data.

In so far as existing communications data is held, it should be for judicial oversight to justify any request for communications data is acceptable. This safeguard would be far more effective than the crude step of trying to produce a list of the organisations can/cannot access data.

To be fully effective this would be based upon a narrowly drawn list of purpose for which data could be accessed.

It should absolutely not be permissible for the list of either purposes or public authorities to be extended without full Parliamentary debate and approval, either through delegated legislation or by Order.

It is difficult to foresee how overseas providers could be compelled to comply, particularly where situations arise where the requirements of the Bill are contrary to domestic law, for example 'do not track' style privacy regulation.
Equally, where service providers have international operations, it is not guaranteed that they are aware where a service user is originating from, therefore deciding whether they should be logged or not.

Use of Communications Data:
The list of purposes for which communications data could be accessed is so broad it is difficult to envisage a criminal offence (or indeed a civil one) which would not be covered by the scope. From unpaid parking tickets to dog fouling and road traffic offences, because the list has been duplicated from the Regulation of Investigatory Powers Act the same well documented issues with RIPA remain.

Our own research under the Freedom of Information Act has confirmed that Humberside Police currently use communications data for categories including 'other non-crime' and road traffic offences. (Supplied in Appendix A)

The Home Office has offered no data on the need for a 12 month retention period, and while we would not accept the premise that data should be retained the period of 12 months appears to have little basis in investigatory need.

Our own research has found that under existing arrangements there are huge variations in the way Communications Data is accessed by police forces. For example, Kent Police officers in two years made 7664 requests for data, with 3237 of those rejected internally. In the same period Merseyside made approximately 30,000 requests with 500 rejected internally.

Safeguards
The main safeguard in any legal system is that the person wronged has the ability to seek redress. Under RIPA and as remains the case under this Bill, an innocent person who had their communications data wrongly accessed would not be able to seek redress as they would most likely never know what had taken place. With just 10 people found to have been wrongfully surveyed from more than three million RIPA authorisations (and five of those 10 the members of one family) it is impossible to say with any confidence that the Commissioner/Tribunal model of oversight is working or indeed fit for purpose.

We support the view that law enforcement agencies should, like public authorities, require a warrant to access communications data. The current investigations into the scale of data being passed from law enforcement agencies to the media and other organisations – most notably the construction industry blacklist – highlight just how far from robust the existing authorisation scheme is.

The wider risk is that the data would be stolen or sold. The type of data being collected will clearly be of commercial value, either from personal gain or industrial espionage. The current legal position of the Government is that it has not enacted the custodial provision for breaches of Section 55 of the Data Protection Act. As such, the deterrent for deliberately abusing data collected is extremely weak.

Furthermore, there is a danger the data collected would be monitored without the knowledge of the CSP. In the case of foreign powers or industrial espionage, this could have a seriously detrimental impact on the UK's national interest.

We would question whether the powers of the commissioners would allow them, for example, to order a technical audit of any hardware installed, or to see the access logs of any system they choose to inspect. Currently the Information Commissioner relies on negotiated permission with respect to private companies, something that has proven to be a serious hindrance in the Google StreetView investigation, for example.

Parliamentary Oversight

The series of powers conferred on the Home Secretary to make orders that would dramatically alter the scope of the Bill is a direct circumvention of Parliamentary oversight.
The fact that the Joint Committee has not yet seen a draft Order, and that the Minister was unable to say when questioned that it would see such a draft order, highlights how assurances of Parliamentary oversight are not reassuring.

Enforcement:
As previously highlighted, the fact that there is not a custodial punishment available to the courts in the event of someone deliberately accessing data they are not entitled to access is a critical failing in the enforcement process.

It should absolutely be an offence to fail to comply with the Code of Practice.
Enforcement should not only pursue the public authority responsible, but also the Senior Authorised Officer responsible for the request.

The question of whether CSPs could be prosecuted or challenged for complying with the Bill in other jurisdictions has not been addressed.

Technical
The technology exists where communications take place entirely 'in the open', however it is far from clear if there is a suitably technological solution where parts or all of the communication are encrypted, re-routed or deliberately disguised in other ways. The need to inspect the content of communications to assess this would appear to be prohibited by the Bill, so even if suitable technology did exist it is unclear if its use would be legal.
It is a legitimate concern that the technology itself would be a target for either attack or surveillance, in particular to organised crime or foreign powers. The Greek Vodafone episode calls into question how capable CSPs are of securing law-enforcement access mechanisms against a deliberate and sophisticated attack.

Measures can be taken to mitigate the risk of loss, abuse or wrongful disclosure but it is impossible to say without qualification that the data can be stored securely. The only absolute protection is for the data to not be collected in the first place.

It is important to note that the normal commercial incentives to maintain data security do not apply to data where the CSP does not want to store the data. Indeed, it may be a perverse incentive to weaken protection – or at least fail to put in place adequate protection – to support the argument that the CSP does not wish to be responsible for this kind of surveillance.

The proposals for the filtering agreements are so opaque it is almost impossible to critique them. The detail of the filtering is entirely absent from the Bill, and assurances of privacy protection seem to deliberately ignore the wider processing undertaken by the filters.
The Bill does not explicitly forbid or require that it is technically impossible to undertake searches based on a particular profile, or that only one item of metadata can be added. For example, detailing all the identities of mobile phones in a particular geographical area at a certain time, or the identity of every person who has visited a specific website. This 'fishing trip' style policing is the very hallmark of the Bill and a total reversal of proven investigative methods.

Given the Home Office accepts the Bill will still leave a capability gap of 15% (and that is assuming the Bill is 100% successful, a tall order given the history of Government IT projects) it is clear that individuals and organisations will be able to circumvent the Bill.
The fact that technologies currently in use to protect intellectual property, corporate interests, enable secure remote working and support secure consumer transactions will in various ways circumvent the provisions of this Bill illustrates the magnitude of the technical challenge.

The Bill is inevitably based on today's landscape, at a time when the direction of travel for consumers and organisations is moving towards more security, more encryption and more privacy.

It is also unclear how the proposals will enable the identification of communications of people in the same 'open' online space – for example a computer game with an online play function where hundreds of people may be involved in the same game – as there is no direct person-to-person communication.

There are of course less technical means of circumventing the Bill, from meeting in person to the kind of cheap, disposable SIM cards acknowledged in the 7/7 inquest.
Encryption is the basis of internet security. Any success in decryption – if possible without a complicit third party (for example a certificating authority) will lead to greater efforts to encrypt content and more advanced forms of encryption. It will also undermine consumer protection when using online services and make British businesses and critical national infrastructure vulnerable to malicious intent. This is a wholly counterproductive outcome which highlights the absurdity of this legislation.

August 2012

Caspar Bowden

Caspar Bowden is an independent advocate for information privacy rights. He was an expert adviser to Opposition parties in the House of Lords for five bills[43], and author of the first paper on communications data retention[44] and the most comprehensive online resource on RIPA[45]. From 2002-2011 he was Chief Privacy Adviser to Microsoft in 40 countries, and from 1998-2002 was Director of the Foundation for Information Policy Research (www.fipr.org). He is a specialist in Data Protection policy, EU and US surveillance law, privacy research in computer science, and a fellow of the British Computer Society. He advises several civil society associations, and sits as an independent expert on the EU Committee for implementing the Data Retention Directive[46]. The opinions in this submission are the author's own and do not represent any organization.

Summary and Recommendations

"The Data Retention Directive is without doubt the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects" - Peter Hustinx[47], European Data Protection Supervisor

The Communications Data Bill[48] is the most dangerous long-term threat to a free society ever proposed by a democratic government, and should be rejected in its entirety. This response is lengthy to provide historical and policy context to the Joint Committee[49] integrating knowledge from several disciplines.

Over two decades the UK has been in the vanguard[50] of a core group of five European countries[51] seeking systematic Internet surveillance. A blanket *retention* regime gives law-enforcement an "Internet Tardis" to go back in time and find out retrospectively what anyone was thinking about, who they were talking to, and where they were. A *preservation* regime is opposed by security bureaucracies because they would be obliged to seek authorization case-by-case (and they might be held to account for those decisions retrospectively).

No official scheme for preservation has ever been published. The author has consistently advocated for data preservation as the only viable alternative policy to retention, and the following summary proposals develop a position first outlined eleven years ago, which respects human rights, with proportionate and effective means for law-enforcement:

- Quick-response preservation on persons who have been identified as facing a real and immediate serious threat, and designated vulnerable groups.
- Convicts of specified crimes released on license must register their means of electronic communication for data preservation during a prescribed period.

---

43 RIPA 2000, H&SCA 2001, ATCSA 2001, ID Cards Acts 2005/6

44 "CCTV for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation ", Caspar Bowden, Computer and Telecommunications Law Review 2002 (http://scholarship.law.duke.edu/dltr/vol1/iss1/47/)

45 Information Centre for the Regulation of Investigatory Powers Act (www.fipr.org/rip/)

46 Platform for Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime (http://ec.europa.eu/transparency/regexpert/detailGroup.cfm?groupID=2230)

47 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf

48 Draft Communications Data Bill 14th June 2012 http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf

49 http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/

50 Duncan Campbell 28.06.1999, Britain Sneaks "Enfopol" Plan Into Action, (http://www.heise.de/tp/artikel/2/2989/1.html also http://www.heise.de/tp/artikel/6/6398/1.html)

51 UK, Germany, France, the Netherlands, Sweden

- Case-by-case judicial authorization for preservation, targeted at those reasonably believed to be engaged in criminal activities (with emergency procedures). Similar reforms should be made for prior judicial approval of interception warrants. Targets should be notified afterwards of preservation and/or interception where suspicions prove unfounded (unless there are compelling reasons not to do so).
- A centre for analysis of preserved data, intended to investigate links between criminal groups, and generate new targets for preservation (subject to judicial authorization)
- Replace the current three Commissioners with a unified Surveillance Commission, reporting to Parliament, with multi-skilled investigators including human rights and computer experts, credibly able to detect and deter abuse, corruption, and insider attacks.
- A fixed ceiling on the number of interception warrants, and a larger ceiling for targets of communications data preservation, which could only be altered by Parliament.

The dichotomy of data retention versus data preservation

"There was something called liberalism. Parliament, if you know what that was, passed a law against it. The records survive. Speeches about liberty of the subject."
Brave New World 1932, Aldous Huxley (and biographer of Père Joseph, Richelieu's eminence gris)

The policy choice between data retention and preservation is a sharp dichotomy. Either data exists or it doesn't. The main objections of principle to mandatory systematic retention of communications data are:

- a "time machine" to scrutinize everyone's past behaviour without prior reason is tyrannical
- Internet and mobile usage patterns reveal sensitive data about e.g. politics and intimate life
- mass-surveillance of every online social relationship is incompatible with a free society
- location data has special privacy risks because it can easily be correlated with other data
- claims that it is necessary just to "maintain police capabilities" don't stand up to scrutiny
- communications data may be equally (or more) intrusive than interception of content
- most criminals could be caught by targeted data preservation rather than blanket retention
- data retention has only happened through rushed legislation in response to shocking events
- if retention of communications data is justifiable, why not every other kind of data also?

Proponents of data retention often say they cannot understand the reasons of objectors. They say that the data will only be accessed with proper authority when justifiable; obviously circumstances exist in which no amount of foresight can guarantee that useful data will have been preserved. UK public opinion has never registered strong objections (unlike e.g. Germany which has seen protests in 40 cities[52]), and the police insist the data is vital. So why object?

The essential reason is that although public opinion does not seem today any more concerned about the intensification of surveillance capabilities using "traffic analysis", "data-mining", "social network analysis", that is a very short term view. Ubiquitous personal communication technologies are here to stay, and because of exponentially falling data storage costs, in the long run two contrasting states of society can be envisaged. Subject to exceptions, the default must be either that individuals determine whether and when their history is recorded, or data will exist about everyone all the time. At some point in the future, most people *will* understand the reality of "dataveillance"[53] and the loss of associated freedoms. UK policy is based on the idea that so long as this doesn't happen there is "no chilling effect, no problem" for democracy.

Another argument often heard from government is "Google/Tesco envy" - what about the mountains of data (more or less) lawfully accumulated in the private sector? Why should the state not also collect "Big

52 http://www.vorratsdatenspeicherung.de/content/view/161/79/lang,en/

53 http://www.rogerclarke.com/DV/

Data" and use for socially beneficial purposes? The weight of disinterested opinion amongst information privacy and security experts is clear. Indiscriminate accumulation of personal data is storing up trouble and the vaunted benefits of Big Data often amount to exploitation without compensation, which will likely have socially regressive[54] outcomes. Intense commercial lobbying is already underway to deflect and dilute regulation which could prevent these harms.

New computer science research shows how "privacy engineering"[55] can maintain the autonomy and discretion we depend on to explore new social and personal experiences, seek medical treatment and spiritual advice, and enable journalists to research confidentially what it would be impolitic to report with attribution. However data retention and the slow pace of legal reform is rapidly demolishing most traditional possibilities for such privileged professional and political privacy. Even in the US, with the Constitutional primacy given to freedom of expression and indemnities to the press [56]

> *Reporters Committee for Freedom of the Press, an advocacy group, said the effect of the current investigation comes on top of a growing awareness by journalists in the last two years that the government often tracks employees' e-mail and telephone contacts. "Reporters are beginning to resort to the old practice of meeting on a park bench to avoid leaving an electronic trail"*

From Data Retention to data-mining

"The biggest problem is that Member States use retention today not only to combat terrorism and serious crime. After the so-called e-Privacy Directive, such data may be used for other purposes, such as crime prevention or the protection of public order, which is a very vague term... The application must be strictly limited to terrorism and serious crime." EU Commissioner Celia Malmström[57] 7th July 2012

Communications data retention is a policy made in Britain.

The lineage of traffic analysis (analysis of patterns of communications about who-is-talking-to-whom) as an intelligence technique can be traced back to WW2 and even WW1.[58]

In 1991 an ITV documentary on electronic surveillance included an interview with a former Joint Intelligence Committee official[59], who disclosed the existence of a memorandum from Sir Peter Marychurch (Director of GCHQ) which seems to have suggested the data-mining of domestic communications data for security purposes.

Police, security and intelligence organizations have been seeking to establish mandatory systematic data retention since at least 2000. An unpublished paper[60] from the major UK Agencies collectively lobbying the

---

54 e.g. behavioural advertising will discriminate against the least affluent, least able to participate in commercial life

55 Digital Privacy: Theory, Technologies and Practices. Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis, Costas Lambrinoudakis (eds). Auerbach Publications (Taylor and Francis Group), 2007

56 New York Times 1st August 2012 "Inquiry Into U.S. Leaks Is Casting Chill Over Coverage" (http://www.nytimes.com/2012/08/02/us/national-security-leaks-lead-to-fbi-hunt-and-news-chill.html?_r=2&pagewanted=all&pagewanted=print)

57 http://www.faz.net/aktuell/politik/europaeische-union/eu-innenkommissarin-cecilia-malmstroem-wir-waren-sehr-geduldig-mit-deutschland-11808962.html

58 George Danezis , Richard Clayton, Introducing Traffic Analysis (2007) (http://research.microsoft.com/en-us/um/people/gdane/papers/TAIntro-book.pdf)

59 ITV World in Action 1991, "Defending the Realm", Nick Davies interviewing Robin Robison (former JIC official)

60 "Looking To The Future" submission to the Home Office for legislation on data retention from ACPO, ACPO(S), HMC&E, SS, SIS, GCHQ (21st August 2000) - (http://cryptome.org/ncis-carnivore.htm)

Home Office to introduce a "National Data Warehouse" was posted on the Internet and is worth re-reading for its precocious ambition.

> 4. WHAT TYPE OF DATA SHOULD BE RETAINED? ..**All** communications data generated in the course of a CSP's business **or routed through their network or servers,** involving both Internet and telephone services, within a **widely interpreted** definition of "communications data"
>
> - ...The Agencies' position is, therefore, that data should be retained for **FIVE YEARS**.
>
> 6.6.4 If the figures are expanded to try and establish the global cost of data storage and retrieval across the UK market, it is estimated to amount to around **£9 million per annum**

The kernel of the CDB was already fully formed in 2000, before the Olympics, national scale rioting, 7/7, Iraq, Afghanistan, and 9/11. There is the difference of a still staggering demand for a longer retention period than has ever been contemplated in any country[61], the estimated costs are now twenty times higher[62] (£1.8bn over 10 years), and the agenda of generalized data-mining is now (more or less) out in the open, albeit euphemistically dubbed "Filtering" (of humongous amounts of data which ought not to be created for retention in the first place except in some rickety 60's TV dystopia).

Bowden's 2002 paper on data retention went to press before ACTSA 2001 passed, but stated

> Automated trawling of traffic databases is a powerful form of mass-surveillance over the associations and relationships that constitute private life. It also reveals the sequence and pattern of thought of individuals using the Internet – it could be described as "closed circuit television for the inside of your head"
>
> ...At the same time (NCIS) were lobbying in secret to warehouse the entire population's traffic data, the Director of NCIS wrote that "conspiracy theorists must not be allowed to get away with the ridiculous notion that law enforcement would or even could monitor all emails."[63]

One of the major purposes of traffic analysis of communications data is to identify targets through pattern analysis. The DG for counter-terrorism at the Home Office asserted in evidence to the Draft CDB Committee that

> Charles Farr[64] (Q28): If you have the data provided for in this legislation, then you can resolve increasingly anonymous communications, which are a feature of the communications environment in which we live. To put it another way, if you have the right kind of data, issues of anonymisation cease to be a significant problem.

9/11 and "Warrantless Wiretapping" in the US

In a different forum, three days later, a senior technical expert who designed very large-scale traffic analysis systems for the National Security Agency (the US counterpart to GCHQ) explained how, on the contrary, mobile telephone anonymity could always be maintained with elementary tradecraft

---

61 except for Poland, which legislated 8 years briefly by accident in the mid 00's, and then swiftly repealed

62 http://www.computerworlduk.com/news/it-business/3364147/governments-data-snooping-bill-will-cost-18bn/

63 http://www.guardian.co.uk/technology/2000/jun/15/security.internet

64 Uncorrected Oral Evidence Taken Before The Joint Committee On The Draft Communications Data Bill (10th July 2012)- http://www.parliament.uk/documents/joint-committees/communications-data/ucJCDCD100712Ev1.pdf

> William Binney[65]: "buy throwaway phones and keep buying them...the most secure way is for you to buy two phones, give one to your friend and you take one, it will show up in the graph as a link, an isolated link, but you'll not be connected anywhere"

It seems unlikely that such a simple counter-measure would not be well understood by terrorists, even if traffic analysis would be effective against opportunistic perpetrators of less serious crimes.

Mr. Binney became a whistleblower because he was concerned that the NSA was spying on Americans illegally using traffic analysis of communications data, very much as is being proposed in the "Request Filtering" Clause 14 of the UK draft CDB bill. In his remarkable speech, worth watching in its entirety, he describes how the NSA had already sought such data illegally in February 2001[66] (i.e. before 9/11 and the passage of the notorious Patriot Act). After 9/11, the NSA initiated several further communications mass-surveillance activities which became known collectively as "warrantless wiretapping" including one codenamed *Stellar Wind*. These programs only came to light as a result of diligent investigative reporting using information provided by NSA (and FBI) whistleblowers concerned about violations of the US Constitution and statute law. For several years, these whistleblowers (and journalists and editors) have been threatened with prosecution on specious charges. Although still not widely reported, a consistent pattern to have emerged is that official channels for escalation, investigation and Congressional scrutiny were thwarted with the complicity of some of the most senior legislative and judicial authorities. Only after the revelations of New York Times journalists James Risen and Erich Lichtblau were published in 2005 (after their newspaper censored itself for a year until after the 2004 election) did a complaisant Congress "make what had been illegal, legal" (in the words of another NSA whistleblower Thomas Drake[67]) through passing the Protect America Act 2007 and the FISA Amendment Act 2008.

RIPA s.16(3) – (effectively) "Warrantless Wiretapping" inside the UK?

The relevance of all the above to the UK is that in an almost unnoticed section of RIPA 2000, the same issue had been anticipated and legalized pre-emptively. There was substantial debate on this point in the House of Lords as a result of amendments and briefing[68] from the Foundation for Information Policy Research. Lord Bassam responded to points in debate in a letter[69] to Lord Phillips of Sudbury

> **Lord Bassam**: ....in some cases selection (of traffic for mass surveillance) will unavoidably be applied to all intercepted communications. This selection is in practice designed to collect *external* communications that fit the descriptions in the certificate. It is therefore not likely to catch many internal communications. It would of course be unlawful to ***seek*** to catch internal communications in the absence of an overlapping warrant or a certificate complying with [Section 16(3)]

Although the front-benches then played down the issue (as a result of briefing from GCHQ), some back-benchers remained dissatisfied at Report[70] stage

> **Lord Lucas**: Both (front-bench) noble Lords seemed to be striving extremely hard to give the Government the benefit of the doubt and to find some way in which what is written plainly and clearly in the Bill should not be true. It is absolutely obvious what is in the Bill--at least it is to me--and that is, yes, trawling becomes legal. The Home Secretary has to renew the warrant every three

---

65 Keynote at HOPE 9 conf (New York City, 13th July 2012, http://www.youtube.lu/watch?v=hqN59beaFMI 1hr 12m).

66 ibid 32m

67 DemocracyNow interview with Thomas Drake 26th March 2012 http://www.democracynow.org/2012/3/26/part_2_former_nsa_employee_thomas 49m

68 http://www.fipr.org/rip/#Overlapping

69 http://www.fipr.org/rip/Bassam%20reply%20to%20Phillips%20on%20S.15.3.htm

70 Lords Hansard 12th July 2000 – http://hansard.millbanksystems.com/lords/2000/jul/12/regulation-of-investigatory-powers-bill#S5LV0615P0_20000712_HOL_383

> months, but he can trawl on grounds of economic well-being and serious crime, as well as terrorism, to any extent that he wishes.

By analogy, two US senators[71] have recently blocked renewal of the corresponding 2008 law because

> (they asked for) an estimate of the "number of people located in the United States whose communications were reviewed by the government pursuant to the FISA Amendments Act." The Office of the Director of National Intelligence responded that it was "not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed under the authority of the FAA."

However the analogy between the controversy over RIPA 2000 s.16(3) and the FISA Amendment Act 2008 s.1881a does not hold in four important senses. Firstly, the controversy in the US has been documented in books[72], magazines[73] [74], newspapers[75], current affairs television programs[76] and websites[77] (although it remains little understood in the legislature) as a result of insider whistleblowers concerned that the categorical protections promised to US citizens by statutes and the Constitution were being illegally subverted.

In contrast in the UK, the issues arising from RIPA 16(3) have only been considered (outside of government) by a few members of the House of Lords and a handful of surveillance policy analysts (and never by a Parliamentary Select Committee, or the Intelligence and Security Committee, POST, or the Investigatory Powers Tribunal – unless perhaps in secret). There has been exactly one press article[78], and no books or television discussion whatsoever.

A second difference from the US situation is that the UK statutes do not promise any analogous categorically superior protections to UK citizens, indeed they cannot do so because discriminating by nationality in this way would be incompatible with the Human Rights Act[79]. Instead RIPA defines *external* communications as those which begin or end outside the UK, and "certificated" warrants for trawling through these using super-computers to search for abstract "factors"[80]. The Bassam letter reveals the government in 2000 well-understood that the *external* concept was incoherent for digital communications using multi-layered protocols, split into datagrams, and autonomously routed through packet-switched networks. However this issue was far ahead of what Parliament could then assimilate, so there was no proper deliberation of the consequences for privacy and freedom, in the way that is now happening – to some extent – in the US. The comparison between the UK and the US is especially relevant because of the

---

71 http://www.wyden.senate.gov/news/press-releases/wyden-places-hold-on-fisa-amendments-act-extension

72 Erich Lichtblau "Bush's Law: The Remaking of American Justice", 2008, Pantheon

73 Jane Mayer, The New Yorker "The Secret Sharer" (http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all) 23rd May 2011

74 James Bamford, Wired "The NSA Is Building the Country's Biggest Spy Center" 15th March 2012 (http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/)

75 Siobbhan Gorman, Wall Street Journal "NSA's Domestic Spying Grows As Agency Sweeps Up Data" (http://online.wsj.com/article/SB120511973377523845.html) 10th March 2008

76 PBS "The Spy Factory" 3rd February 2009 (http://www.pbs.org/wgbh/nova/military/spy-factory.htm)

77 http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy

78 The author attempted to brief newspaper and broadcast current affairs editors without any apparent interest, resulting in only in http://www.guardian.co.uk/technology/2000/aug/10/news.onlinesupplement

79 A v. Secretary State Home Department [2004] UKHL 56, [2005] 2 AC 68

80 Factors may select according to traffic patterns (who-is-talking-to-whom), keywords, voiceprints, and algorithms also exist for searching texts for paraphrased meaning ("latent semantic indexing").

longstanding intelligence ties between NSA and GCHQ, and their Internet surveillance capabilities are much larger than all other democratic countries.

Thirdly, whilst the intentional warrantless mass-surveillance documented in the US has been widely criticized as illegal, we do not know if any analogous domestic mass-surveillance has been authorized under RIPA S.16(3) certificated warrants. The Interception Commissioner has never referred to that section in his published annual reports, or indeed made any reference to "certificated" (trawling) warrants[81]. Interpretation of the 16(3) clause requires unraveling nested and interlocking clauses, phrased in triple-negatives using pseudo-technical jargon. No open jurisprudence or scholarship can develop because of the secrecy provisions of RIPA. The UK lost a relevant case at the ECtHR in Strasbourg in 2008[82] but that concerned the previous IOCA 1985 law. The Bassam letter is all that is known, but we do not even know if the IoCC is aware of that letter, agrees with or enforces its prohibitions, or understands its technicalities.

Fourthly, there are some indications[83] [84] [85]that the *Stellar Wind* program in the US mainly or wholly concerned data-mining analysis of "non content metadata" (such as communications data but perhaps other kinds of transactional records also), not mass-interception of the *contents* of communications. The distinction is habitually muddled in (every country's) press coverage and legislative debate, but traffic analysis is the primary technique for selecting what "content" gets intercepted in both targeted and mass-surveillance of communications. It might explain the blasé confidence of US administration officials that this type of data-mining did not break the FISA law – at least not in the way most critics alleged.

However the privacy-invasive reality of traffic analysis in bulk is not adequately recognized in US or UK law. The post-9/11 surveillance-industrial complex is founded on the shibboleth that whilst "content" deserves the protection of a warrant, "mere" communications data engages privacy rights to a vastly lesser extent, and its acquisition may be self-authorized by law enforcement agencies. This legal fiction is precariously sustained by law enforcement agencies carefully avoiding test cases which might update binding precedents dating from the era of mechanical telephone exchanges[86].

The Anti-Terrorism Crime and Security Act 2001 Ch.11 introduced a power to compel blanket retention of communications data, if service providers declined to do so "voluntarily". The Liberal Democrats introduced an amendment which sought instead only to permit preservation of data "directly or indirectly related to national security"[87].

> Lord Phillips of Sudbury: ...whatever the Minister thinks about mass trawling and mass surveillance, the Home Office knows that that is precisely what these clauses relate to. It is their ability, via the Secretary of State's direction, to require the entire industry to retain its entire stock of traffic data for an unlimited period. It is that power that enables the security industry to have access, via the Regulation of Investigatory Powers Act and the Data Protection Act, to this huge warehouse of information. We on this side of the House have repeatedly said that we are not content with the balance as struck. That is why we want the amendment to remain.

---

81 Except in the first report which dubiously invented "overlapping" warrants http://www.fipr.org/rip/#Overlapping

82 Liberty and others v UK no. 58243/00 [2008] ECHR

83 http://en.wikipedia.org/wiki/NSA_call_database

84 US wiretap law authority Orin Kerr on 15th December 2008 (http://www.volokh.com/posts/1229325134.shtml)

85 Newsweek 12th Dec 2008 (http://www.thedailybeast.com/newsweek/2008/12/13/now-we-know-what-the-battle-was-about.html)

86 Tokson M, Automation and the Fourth Amendment, Iowa Law Review, 2011 (http://128.255.56.99/~ilr/issues/ILR_96-2_Tokson.pdf)

87 Lords Hansard 13th Dec 2001 (http://www.publications.parliament.uk/pa/ld200102/ldhansrd/vo011213/text/11213-17.htm)

> ...NCIS is building—and has made it quite clear that it wants to go on building—a national traffic data warehouse. That is its aim. Indeed, a senior member of that body said recently, "We want to have all the information we can lay hands on. It's up to you fellows to stop us".

In an exhausting debate between both Houses, in which few parliamentarians grasped the conceptual difference between retaining data on the entire population versus the small fraction about whom prior suspicions might exist, the amendment was only accepted by the government in a fog of confusion with a seemingly incoherent rationale[88]. A QC's Opinion[89] later obtained by the Information Commissioner found that blanket retention was "a breach of the right to privacy", anticipating subsequent arguments over the EU Data Retention Directive[90], but the ICO chose to acquiesce to the Home Office and offered no further resistance.

Waiting for Strasbourg (or Luxembourg) ?

Several Constitutional Courts around Europe have ruled that blanket data retention is unlawful[91]. A case initiated by Digital Rights Ireland which will test the human rights compatibility of the DR Directive is now in progress at the ECJ[92]. The ECtHR has recognized in unambiguous judgments[93] that the right to private life under Article 8 is engaged by (a) processing communications data per se, or (b) the "mere" *collection* of data about individuals (irrespective of whether it is examined), or (c) the indiscriminate accumulation of data about entire populations. Putting a/b/c together, logically the Court ought to find (when a suitable case arrives) that the principle of blanket retention of communications data for the purposes of traffic-analysis through data-mining is at least a disproportionate violation of Art.8, and perhaps also that not only is this unnecessary in a democratic society, it is incompatible with democracy. This conclusion can also be deduced from the General Comment on the right to privacy in International Covenant of Civil and Political Rights[94].

> Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a ***case-by-case basis***.

---

88 Commons Hansard 13th Dec 2001, David Blunkett (Home Secretary): "The amendment, in relation to part 11 therefore suggests that we should try to separate out those parts of data. As I tried to explain on a number of occasions, including last night, it is not possible to do that, but **paradoxically, because it is not possible to do it, it is not reasonable to suggest that we should not do it**. I am therefore prepared to accept the amendments that have been tabled. **In order to be able to implement what they want, we will have to retain the data**, so that it can be accessed to test out whether the intelligence services are right in believing that it is relevant in tackling terrorists. That is how stupid the Liberal Democrats are." (!?) (http://www.publications.parliament.uk/pa/cm200102/cmhansrd/vo011213/debtext/11213-36.htm)

89 Ben Emmerson QC (31st July 2002 - http://www.guardian.co.uk/technology/2002/jul/31/internet.politics)

90 Kosta Eleni, Valcke Peggy (2006) "Retaining the data retention directive", Comp Law & Sec Report, Vol 22, Issue 5, p.370-380 http://www.law.kuleuven.be/icri/publications/824a2_Kosta,Valcke_2006_CLS_DataRetentionDirective.pdf

91 e.g. Romania which found that "a positive obligation that foresees the continuous limitation of the privacy right and the secrecy of correspondence makes the essence of the right disappear" http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

92 Case C-293/12 http://curia.europa.eu/juris/fiche.jsf?id=C;293;12;RP;1;P;1;C2012/0293/P

93 ECHR (a) Malone v. UK *(1984) and Copland v. UK (2007), (b) Amann v. Switzerland (2000) and Rotaru v. Romania (2000), (c) S and Marper v. UK (2008)*

94 CCRP General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17) : . 04/08/1998 (http://www.unhchr.ch/tbs/doc.nsf/%28Symbol%29/23378a8724595410c12563ed004aeecd?Opendocument)

However US and ECHR jurisprudence diverge fundamentally over the privacy sensitivity of communications data. US courts have held so far that individuals have no expectation of privacy in traffic and location data because they are necessarily divulged to "third-party"[95] service operators. The UK tried out a similar argument at Strasbourg in Copland v UK[96] 2007

> UK: Although there had been some monitoring of the applicant's telephone calls, e-mails and Internet usage …this did not extend to the interception of telephone calls or the analysis of the content of websites visited by her. The monitoring thus amounted to nothing more than the analysis of automatically generated information … which, of itself, did not constitute a failure to respect private life or correspondence

The ECtHR completely rejected this view in their judgment

> 43. The Court recalls that the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an "integral element of the communications made by telephone" (see *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A no. 82, § 84). The mere fact that these data may have been legitimately obtained by the College, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 (ibid). Moreover, storing of personal data relating to the private life of an individual also falls within the application of Article 8 § 1 (see *Amann*, cited above, § 65). Thus, it is irrelevant that the data held by the college were not disclosed or used against the applicant in disciplinary or other proceedings.
>
> 44. Accordingly, the Court considers that **the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and INTERNET usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8**. (emphasis added)

One of the most thorough recent examinations of the legality of the EU Retention Directive emphasized that in any determination of the compatibility of the principle of retention [97] "the fact that traffic analysis and data mining can be realistically performed using the retained traffic and location data is an aggravating factor to be considered."

A Finnish Red Herring

The Explanatory Notes of the draft CDB floats a specious compliance argument at footnote (2)

> See e.g., K.U. v Finland [2008] ECHR 2872/02, at para. 49 ("....Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and
> Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of
> others. ...It is nonetheless the task of the legislator to provide the framework for reconciling the various
> claims which compete for protection in this context.")

---

95 American Bar Association Journal "The Data Question: Should the Third-Party Records Doctrine Be Revisited?" (http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/) 1st August 2012

96 http://www.bailii.org/eu/cases/ECHR/2007/253.html

97 Feiler, L., "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection", European Journal of Law and Technology, Vol. 1, Issue 3, 2010. (http://ejlt.org//article/view/29/75)

K.U. v Finland appeared around the time of Marper, but attracted little comment or analysis at the time in comparison, and the prominence given to it by the Home Office shows they think it is their best riposte to ECtHR's deprecation of indiscriminate collection.

But despite the (uncharacteristic) rhetorical sideswipes at Internet anonymity, it is much weaker than it seems because these remarks were in *dicta.* It is not entirely clear whether the author of the judgment understood the point, but it was not necessary in this case to consider the justifiability of blanket and indiscriminate retention of data which would not otherwise exist. The data at issue in the K.U. case did exist, but Finnish law was defective in not allowing its use to investigate the crime. It is not reasonable to assume that the ECtHR would wish to finesse such a massively important question, so the case cannot bear the the significance the Home Office implies.

Interactions with Data Protection law

"We should select any person from the inhabitants of the Earth...using no more than five individuals...he could contact the selected individual using nothing except the network of personal acquaintances" - Frigyes Karinthy[98] 1929

Communications data, even without any information about the content of communication, can reveal highly sensitive information in surprising ways. Much information is revealed through the *social graph* of relationships between individuals, particularly if each connection is annotated with strength information, such as how often two individuals communicate.

Inferring "sensitive data" from the social graph[99].

For example, introverts might communicate more often with a smaller circle of contacts who are all related, while extroverts might tend to communicate less often but with a larger circle of contacts from different social spheres, revealing a basic profile of personality. Such information can be revealed simply through patterns of communication, which sociologists have studied for decades prior to the advent of widespread Internet communication[100].

Much more powerful inferences can be drawn using the principle of *homophily* - most people are much more likely to communicate frequently with individuals who are like them. It is a robust phenomenon and has been observed across cultures and a large number of personal traits, including age, occupation, social class, religion, political affiliation, gender and sexual orientation, and also including implicit traits like intelligence, attitudes, values, and aspirations[101].

In these ways, social network analysis of communications data can generate sensitive (aka "special category") personal data, without any knowledge of the content of communications. Data Protection Authorities have remained silent about this problem (it has scarcely been addressed in any Art.29 Opinion[102]), perhaps because it seems too corrosive to a definable concept of sensitive personal data.

With the advent of online social networks, researchers have recently been able to acquire sufficiently large datasets to demonstrate the power of large-scale inference using homophily. Given information about private traits of some individuals, such as sexual orientation or religion, it is possible accurately to predict

---

98 originator of the postulate of "six degrees of separation"

99 I am grateful to Joseph Bonneau for help with this passage

100 Wasserman, S. & Faust, K., Social Network Analysis, Cambridge University Press, 1994

101 McPherson, M., Smith-Lovin, L. & Cook, J., Birds of a feather: Homophily in social networks, Annual Review Of Sociology, Annual Reviews, {2001}, Vol. {27}, pp. {415-444}

102 Art.29 2010 WP 171 on online behavioural advertising "if an ad network provider processes individual behaviour in order to 'place him/her' in an interest category indicating a particular sexual preference they would be processing sensitive data"

this trait for many other individuals using the social graph.[103] Very similar experiments have successfully demonstrated prediction of users' political affiliation[104] [105] [106], gender [107] [108], and hobbies[109]. This type of inference could improve significantly given a more fine-grained social graph with information about the frequency and duration of communication between individuals.

Limits to the scope of communications data – Big Browser

"If you give me six lines written by the most honest man, I will find something in them to hang him" - Cardinal *Richelieu* (1585-1642)

The definition of communications data in the draft CDB are essentially unchanged from RIPA 2000. The definition included the name (or IP address) of web-sites browsed (www.bbc.co.uk), but excludes anything "after the first slash" (www.bbc.co.uk/news/uk-politics-18003315).

It is worth recalling the sequence of events which resulted in this limitation. During the RIPA debate in the House of Commons, FIPR warned[110] that any logs of web-pages visited (in the transparent caches of an ISP or logs retained by hybrid communication services incorporating search engines or portals) could be caught in the vague definitions, and promoted amendments to draw out the government's position in the House of Lords. A quickening tempo of adverse media coverage[111] in the trade and broadsheet press increased the pressure for changes and clarifications which had been impassively blocked for many months previously

> Lord Lucas: ...the identity of every single web page that is visited is known. It is as if under the heading "communications data" the Government are able to know about every shop that I have visited and every page of every book, magazine or article I have read. If I make a request to a search engine, in most formats that counts as communications data because it is a signal to actuate the search engine.
>
> Lord Cope of Berkeley: ..."communications data" on the Internet widens the issue a great deal, in particular, in relation to visits to websites, and so on. ... We believe that it may be necessary to have greater controls over the extent of this intrusion than at present.
>
> Lord Bassam: It is becoming clear that the current definition is not adequate... I do not have a new definition of "communications data" to offer today

---

103 This approach was famously demonstrated in the case of sexual orientation, where a very simple algorithm using only binary friendship connection information and a small number of men known to be homosexual was sufficient to predict the sexual orientation of about 6,000 students at MIT with about 80% accuracy

104 Lindamood, J., Heatherly, R., Kantarcioglu, M. & Thuraisingham, B. Inferring private information using social network data, Proceedings of the 18th International Conference on World Wide Web, ACM, 2009, pp. 1145-1146

105 Mislove, A., Viswanath, B., Gummadi, K.P. & Druschel, P. You are who you know: inferring user profiles in online social networks, Proceedings of the Third ACM International Conference on Web Search and Data Mining ACM, 2010, pp. 251-260

106 Zheleva, E. & Getoor, L. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles, Proceedings of the 18th International Conference on World Wide Web, ACM, 2009, pp. 531-540

107 Kozikowski, P. & Groh, G. Inferring Profile Elements from Publicly Available Social Network Data 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust 2011, pp. 876-881

108 Xu, W., Zhou, X. & Li, L. Inferring privacy information via social relations, Data Engineering Workshop, 2008. ICDEW 2008. IEEE 24th International Conference on 2008, pp. 525-530

109 Agarwal, A., Rambow, O. & Bhardwaj, N. Predicting Interests of People on Online Social Networks, CSE '09: International Conference on Computational Science and Engineering

110 FIPR Press Release on RIP Third Reading HoC debate 9th May 2000 http://www.fipr.org/rip/PR3RHC.htm

111 http://www.fipr.org/rip/#Observer250600

The mini-debate[112] shows the House of Lords at its zenith as a revising chamber, but its powers to convert forensic cross-examination into textual changes were (and are) rather modest. The critical factor was a general loss of confidence in the Executive's competence about the subject's technicalities, which obliged the Bill team to make unusually sweeping revisions to these and other sections, under an intense degree of press scrutiny[113] to "keep them honest", resulting in the definitions we have today for *Subscriber*, *Traffic* and *Use* data[114].

Police requests to access *Subscriber* data (for account billing) have never needed judicial authorization, but this category inaptly includes device serial numbers which can track behavior. *Traffic* data is the most privacy-sensitive (who-is-talking-to-what-or-whom) which also includes location data (GPS coordinates or mobile base-station IDs). However despite the hard-won Big Browser amendment, a technique involving *Use* data means **content** could still be deduced through "fingerprinting"[115] the pages of websites.

This loophole should be closed as part of a new concept of regulating the *mode of analysis* for human rights compliance (see below), but it will need Commissioners with technical as well as legal expertise to apply (see below on IoCC oversight)**.**

The problem of schizoid-jurisdiction

A problem which has developed in the past decade is that some providers of Internet services with headquarters in the US have developed the practice of rejecting the application of EU jurisdiction for purposes of Data Protection (for example relying on Safe Harbor for minimal fulfillment of the rights of the data subject), but on the other hand they will respond locally and directly to demands from law enforcement authorities for access to communications data (without insisting on the analogous step of requiring LEAs to invoke MLAT procedures). There is no legal basis for such a schizoid attitude to recognizing jurisdiction, and this practice only continues because (a) the organizational functions for data privacy are often disconnected from the servicing of law enforcement requests, and (b) some DPAs and even the Council of Europe may be aware of these practices but find it expedient to turn a blind eye absent a sharp test of data subject rights. Nevertheless, personal data are being processed within the EU when law enforcement demands are serviced in this way and data subjects are entitled to full exercise of their rights against the Controller within EU jurisdiction.

It is totally unclear how foreign service providers outside the UK (or the EU) are going to be required to comply with the *provisions* of the CDB, but there is clearly the risk that the problem of schizoid jurisdiction, and lack of full, prompt and effective enforceability of rights could be further aggravated.

Subject access rights to "third party" communications data ?

> ***Explanatory Notes Clause 5: Access to data***
> 30. Subsection (1) stipulates that communications data held by a telecommunications operator under Part 1 can only be accessed in accordance with the provisions in Part 2 or as otherwise authorised in law. *These may include a request under section 7 of the Data Protection Act 1998 (which provides an individual with the right of access to personal data)* or in pursuance of a court order.

---

112 http://hansard.millbanksystems.com/lords/2000/jun/19/regulation-of-investigatory-powers-bill-2#S5LV0614P0_20000619_HOL_458

113 The author briefed more than 100 journalists over a 12 month period from 1999 until Royal Assent

114 Draft CDB Clause 28(3): Data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication is not "traffic data" except to the extent that the file or program is identified by reference to the apparatus in which it is stored.

115 https://blog.torproject.org/blog/experimental-defense-website-traffic-fingerprinting

This clause ostensibly ensures a Data Protection right of subject access (which was not expressly included in the corresponding section of RIPA Pt.1 Ch.2), and thus ought to be welcome in principle. However it is actually a bear-trap, which could mean that most of the new data collected would be ineligible for subject access.

The major purpose of CDB is blanket collection of metadata about use of "3rd party services" (e.g. those not operated by the user's ISP), to be collected by Deep Packet Inspection (DPI) boxes located throughout the UK network infrastructure (not necessarily just the retail operator with whom the user has a billing relationship). The owner of the DPI box (or the Clause 1 apparatus) will be the putative Data Controller for purposes of subject access, but they may not know (directly or indirectly) the identity of the person whose data is being collected. Because the DPA 1998 did not give any effect to four crucial words of Recital 26 ("or by any other person") of the EU DP Directive, data is only regarded as personal in the UK if it is directly identifiable by the Controller, together with other information that is or may likely come to be in the Controller's possession. Therefore the Controller will be entitled to refuse access to any data which it cannot exclusively and directly associate with the subject. This might include any data possibly being relayed by the user on behalf of another party (e.g. peer-to-peer routing protocols such as Skype[116]). The position is not even clear for the user's direct communications with another party. The ISP only knows the association between the user's IP address and subscriber account details; it does not "know" about the user's identifiers and handles at other protocol levels of abstraction (but the ISP will nevertheless be obliged to install DPI boxes which do capture metadata from these higher levels of abstraction). The Controller may even refuse to grant an access request on the grounds that the party with whom the user is communicating (if that is a natural person) has at least co-equal status as a data subject, and only agree to fulfill the request with the express consent of the other party.

Will the user be able to make a subject access request to the operator of filtering apparatus in Clause 14, namely the Secretary of State, perhaps as a putative (co-)Controller of the DPI boxes? It appears this has not been provided for in Clause 5 or elsewhere, and several DPA 1998 exemptions might be arguable, notably s.28 (national security) and/or s.29 (prevention/detection of crime). Data processed by GCHQ or for national security would be categorically exempt from most parts of the DPA.

Moreover, the proposed new EU DP Regulation, which would otherwise be expected to broaden the UK concept of personal data (at last unambiguously) to include indirectly identifiable data, will not fill this lacuna if the UK's position[117] on the new Regulation in the Council of Ministers prevails. The UK wishes that only "easily identifiable" data should be considered personal (footnote 12), to delete the Recital highlighting the dangers of profiling (footnote 11), and "questioned whether so-called (online) identifiers which were never used to trace back to a data subject should also be considered as personal data" (footnote 14; see also footnote 45).

The combined effect of these UK positions on the new DP Regulation would mean that perhaps most of the captured data about 3rd party services would be ineligible for subject access, and result in a calamitous evisceration of data subject rights. The following steps would disarm this bear-trap:

> (a) a right of access must be established against the Secretary of State, with explicit wording to prevent invocation of DPA s.28/29 exemptions, and
>
> (b) a broad meaning of personal data comprehending Recital 26 of the EU DPD should be adopted (or that in the unmolested new Regulation – which already has some weasel-worded Recitals that need excision)

---

116 See Stevens et al. "I Know Where You are and What You are Sharing" - (www.mpi-sws.org/~stevens/pubs/imc11.pdf)

117 www.statewatch.org/news/2012/jun/eu-council-revised-dp-position-11326-12.pdf

The effect of (a) and (b) must be for the data subject to be able to invoke the distributed data-mining machinery of (Clause.14) Filters to discover what personal data – in a broad sense – the totality of the CDB system knows about them. Any data which could be associated with the data subject as a result of a Request Filter ought to be eligible. Only in this way can the data subject be guaranteed a right of "information self-awareness" which will allow them to regulate their conduct in the sense of ECHR Art.8 quality-of-law requirements. This is a core reason for the existence of the right of subject access.

Distributed data-mining : the core of the Communications Data Bill

Although it has been touted as a concession to and measure protective of civil liberties, from a technical viewpoint it is cold comfort that the draft CDB is based on the idea of leaving data in the distributed custody of service providers, because very probably the notion of a centralized database was always going to be impractical. Few organization have experience of designing national-scale centralized data warehouses for communications data. The NSA tried with their TrailBlazer[118] project which failed expensively. NSA systems architect and whistleblower William Binney explained[119] the key problem with orthodox relational databases was that they could not ingest new data fast enough, so became backlogged. He had some success obviating this problem using fast database structures suitable for very large working memory sets, and explained that once the connections in the "national social graph" grew to a certain scale, the growth in complexity began to flatten out because already established connections began to be repeated. However collection of all the data desired by the architects of CDB is probably out of reach even of these highly optimized techniques, and the intention is clearly to use the distributed computational technique commonly known as MapReduce[120]. Essentially this is an efficient way for applying a function to a vector of data physically distributed across many machines, bringing the intermediate results back to a central location, and then performing a final reduction of intermediate results to produce a finished massively-parallel computation.

This is what is described in Clause 14, and the explanatory memorandum reads like marketing jargon from a surveillance trade fair[121]. In fact it may be the first clause of legislation derived from a sales brochure.

> Explanatory Memorandum 82.
>
> ...The Request Filter may: a) provide **details of different options** the Request Filter may employ to provide a response to a specific public authority data request; and b) for each identified option, provide **details of the anticipated levels of interference** and the **likely precision** of the returned results. The information provided by the Request Filter will enable the designated senior officer to **understand how the Filter will answer particular questions**, and will guide him through the **process of determining which questions he believes it is necessary and proportionate to ask**, taking into account the filtering and processing which will be undertaken and the **volume of filtered data** which will be disclosed.

An amendment which removed the following highlighted parts of the "MapReduce Clause" would neutralize the capacity to do distributed data-mining (and thus prevent the system being used with capabilities equivalent to a centralized system).

---

118 http://en.wikipedia.org/wiki/Trailblazer_Project

119 Keynote at HOPE 9 conference (New York City, 13th July 2012, http://www.youtube.lu/watch?v=hqN59beaFMI 50m).

120 http://en.wikipedia.org/wiki/MapReduce

121 ISS World: "Big Data Analytics and Massive IP Intercept" http://issworldtraining.com/ISS_WASH/track2.html

14(2)b (i) obtaining the data **or data from which the data may be derived**,

(ii) processing the data **or the data from which it may be derived** , (and **retaining data temporarily** for that purpose)

Compounding the hyper-Orwellian menace of data-mining a national traffic data warehouse (described by a former DPP[122] as a "*hellhouse* of personal and *private* information"), is the foreseeable risk that insiders could collude to bypass controls. Using seemingly legitimate Filters which triggered distributed queries to many DPI boxes, information about a surreptitious target could be extracted (under the rubric of "**retaining data temporarily** for that purpose"). It would be very difficult to detect or prove this was happening and the IoCC as presently operating would find nothing suspicious in the log files (assuming he was even looking).

The role of the Interception of Communications Commissioner

The 2011 report[123] of the Interception of Communications Commissioner (IoCC) is the most detailed since the first report was published in 1987. The most serious deficiency of the oversight regime is only fleetingly acknowledged – it's all (literally) a paper exercise.

> "the possibility of successful deliberate abuse is very small indeed, if **statutory** channels are being used".

The reports have always been silent about how abuse by insiders with the technical or administrative ability to bypass the paperwork might be deterred or detected, yet that is surely one of the major risks.

FIPR successfully promoted a RIPA amendment[124] allowing the IoCC to insist that reliable and verifiable technical means[125] must be designed into interception and communications data logging equipment, but he has never referred in any report to exercising these powers, and it appears that efforts at verification are confined to comparing paper copies of documents held by different parties.

The IoCC always has appeared primarily to rely on those he is charged with overseeing, themselves volunteering reports of their own mistakes. Errors are lamented and usually rather trifling (typically a transposed digit). But over 27 years, the IoCC has never discovered any serious wrongdoing in interception practices whatsoever (that he has revealed publicly).

This year, for the first time, the report quantifies errors discovered by the inspection regime (rather than self-reported). However the size of the random sample (out of a half-million requests – each of which may involve data about many individuals) is not given, without which the overall number of undetected errors can only be guesstimated, but there are likely to be thousands. The IoCC has replied that it is "not possible" to give the sample size. Why not?

The report mentions that two individuals have suffered very serious consequences through such errors, but appears blind to the statistical inevitability than many more victims of such errors must be suffering equally serious injustices.

---

122 Sir Ken McDonald, 31st Dec 2008 (http://www.guardian.co.uk/uk/2008/dec/31/privacy-civil-liberties)

123 Interception of Communication Commissioner 2011 Report www.intelligencecommissioners.com/docs/0496.pdf

124 Lord Bassam's remarks on Amendment 50A 10th June 2000 (http://hansard.millbanksystems.com/lords/2000/jun/19/regulation-of-investigatory-powers-bill#S5LV0614P0_20000619_HOL_82)

125 A survey of suitable methods is outside the scope of this paper but might include a hardware trusted computing base, cryptographically signed and verifiable audit trails of program code and data, and multiple simultaneous distributed log files

Overall the UK appears relatively secretive and compares poorly to other countries in the degree of Parliamentary involvement in the oversight process according to a comprehensive recent report to the European Parliament[126]

> In the case of oversight of information sharing, it is doubtful if the current UK arrangements satisfy the standards proposed by the UN Special Rapporteur. Domestic legislation fails to outline 'clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence'. **Nor does it explicitly prohibit the use of foreign intelligence services to circumvent national legal or institutional controls**....the UK experience underlines the **need for critical distance from the executive** to be woven into oversight arrangements (especially in such procedural questions as appointment of overseers and reporting) if public confidence is to be retained .

In contrast, under the French system a "qualified person" (with deputies) is appointed by an independent control Commission (CNCIS[127]) to conduct **prior** validation of all counter-terrorist requests for communications data, and the Commission also applies scrutiny retrospectively. The Commission also ensures **prior** authorization of all interception warrants (turning round emergency requests within one hour), which are capped below a fixed number expressly for the purpose of protecting civil liberties. Authorizing departments must apportion this quota ceiling between themselves, and make provision for their own contingency reserve. Recently the independence of CNCIS was tested by a complicated political scandal about circumvention of procedures by the country's most senior intelligence official, whose objective was to trace the communications of journalists at *Le Monde* and inhibit their exposure of illegal donations to the governing party[128].

Case studies which don't stack up

This year the IoCC has endorsed[129] several "case-studies", six of which are offered in support of present policy on communications data (studies 2, 3, 12, 13, 14, 15). However from easily traced media reports, a different picture emerges which prompts some skepticism about the impression he gives

- Case Study 2 – it isn't clear if the suspects were identified from cellsite analysis (but that may be the case). It isn't clear if other investigative means might have identified the suspects. Once the suspects had been identified, it appears substantial other evidence was available and obtained.
    - "officers were led to Kinson Common on April 8 during a surveillance operation on target suspects... As the search continued so did the surveillance operation and Lammali was spotted with friend Ryan Dear collecting something in a holdall from an area of nearby Redhill Common. They were stopped by officers and found to be in possession of five further

126 Aidan Wills, Mathias Vermeulen 2011: Parliamentary Oversight Of Security And Intelligence Agencies In The European Union (http://www.europarl.europa.eu/committees/en/libe/studiesdownload.html?languageDocument=EN&file=48800)

127 Commission nationale de contrôle des interceptions de sécurité - 18ème rapport d'activité - Année 2009 http://www.ladocumentationfrancaise.fr/docfra/rapport_telechargement/var/storage/rapports-publics/104000489/0000.pdf

128 http://fr.wikipedia.org/wiki/Affaire_Bettencourt#Violations_pr.C3.A9sum.C3.A9es_du_secret_de_l.27enqu.C3.AAte_et_du_secret_des_sources

129 IoCC Annual Report 2011 ibid.

shotguns belonging to Mr Langdown."[130]

- Case Study 3 – concerns access to subscriber data to confirm the identity of an already known suspect, and thus does not demonstrate any necessity for prior retention of traffic/location data.
- Case Study 12 – the suspect was not identified using communications data. The case could not be traced, so it isn't clear whether another investigative strategy could have led to a successful prosecution
    - A fingerprint from the scene identified a suspect from the Northampton area and two of his known associates subsequently became suspects. Mobile telephones were identified for the three suspects
- Case Study 13 – the suspect was not identified using communications data. News reports indicate that blanket retention was not necessary for detection or prosecution
    - "Police investigating the assault and robbery in Kilmaurs found traces of his DNA on a handbag and arrested Gable as he arrived back from a trip to Northern Ireland on a ferry. Specialist software was used to download information from the sat-nav device in his car. It located him at or close to each of the crime scenes. He was found to have been just 20 seconds away from one of the auto tellers he used to steal cash"[131]
- Case Study 14 – concerns access to subscriber data to confirm the identity of an already known suspect, and does not demonstrate any necessity for prior blanket retention of traffic/location data.
- Case Study 15 - the identity of the suspect was already known, and a strategy of communications data preservation may well have been sufficient for prosecution of ongoing offences.

Thus only one out of six relevant case studies gives plausible support for the strict necessity (rather than mere usefulness) of prior blanket retention of the entire population's traffic and location data. Allowing that news reports may not tell the whole story, nevertheless if the IoCC is retailing these cases at face-value, presumably chosen for their persuasiveness, what does this tell us generally about his standards of logical rigour in applying a test of necessity?

What does the IoCC consider "necessary and proportionate" ?

Under the UK regime, almost all jurisprudence about interception and communications data takes place invisibly within the cranium of the IoCC, and almost nowhere else.

On pp.27 of the 2011 report it states that inspectors

- "seek to ensure...the disclosure required was necessary and proportionate to the task in hand"

The IoCC was asked by the Open Rights Group (ORG) to explain the methodology for verifying that authorizations/notices scrutinized by random sampling were in fact necessary and proportionate. For example, is it the IoCC's view that his functions are discharged if he satisfies himself that the designated person believed at the time the authorization was necessary and proportionate, or does the IoCC apply his own judgment of necessity and proportionality, or does he use a test such as the "manifestly unreasonable" standard for judicial review? Here's the reply:

> (21/8/12) The inspectors examine the justifications for necessity and proportionality that have been set out in the application. The inspectors will also scrutinise the decision made by the designated person (recorded in their written considerations). The necessity and proportionality tests for

130 http://www.bournemouthecho.co.uk/news/districts/bournemouth/9341126.How_violent_Bloxworth_robbers_were_caught/?ref=rss

131 http://www.bbc.co.uk/news/uk-scotland-glasgow-west-15491273

> communications data are quite specific – in order to justify **necessity** under Section 22(2) the applicant **must make the link** between the crime/offence (or other purpose), the suspect, victim or witness; and the phone or communications address
>
> – in order to justify proportionality the applicant must explain **how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation**, provide a justification as to how the specific **date/time periods requested are proportionate** and **consider, if relevant,** whether the objective could be achieved through less intrusive means. **Collateral** intrusion must also be considered and any **meaningful** collateral intrusion described (for example, the extent to which the privacy of any individual may be infringed and why that intrusion is justified in the circumstance). The case must be made for each specific data request and the application supporting the request should stand on its own. If the inspector has concerns that the tests have not been met, they will speak to the applicant and/or the designated person. The inspector may also ask to see further supporting documentation (such as the case file, policy logs, operational book etc).

These replies raise many questions about the spirit of ECHR compliance, without concrete information illustrating what is and is not judged acceptable. How many people's data can be accessed to investigate what types of crime, what happens to that data subsequently, especially if something unexpected is found? Can a request be widened if nothing is found initially? Is anything done systematically to detect attempts at fishing expeditions? What is the policy on disclosure of communications data access to defence counsel? There is no published policy on any of these matters.

The IoCC was also asked about patterns of communications between people and websites (see above Inferring "sensitive data" from the social graph) and whether he applied particular safeguards, or required a higher level of justification, for this mode of analysis. He replied:

> All communications data requests are protectively marked under the Government Protective Marking Scheme (GPMS). Once **disclosed**, the communications data is subject to DPA. DPA is not overseen by the Interception of Communications Commissioner.

This reply illustrates a key deficiency of the current oversight regime, which fails to regulate the *modalities of analysis* of information about private life which is in scope of ECHR Art.8, but may be wholly or partially exempted from Data Protection, and treated as out of scope by the IoCC. The nature and application of the algorithms used for data-mining and traffic-analysis may seriously infringe human rights; this is a serious lacuna in UK legislation.

Appendices

Queries about police oral evidence given to Joint Committee

Both Gary Beautridge and Trevor Pearce (repeatedly) confused the Interception Commissioner with the Information Commissioner in their evidence, casting some doubt about their actual familiarity with oversight procedures.

However there is a much graver concern about the good faith of the police evidence to the Committee on 12th July[132], when it was stated:

---

132 http://www.parliament.uk/documents/joint-committees/communications-data/uc120712Ev3HC479iii.pdf

> (Q142) Peter Davies: For some time it has been possible, roughly or more precisely, to locate a mobile telephone through the use of communications data. A team I have led has used that as almost the **sole** means of detecting a serious double murder in one of my previous forces ....(Q146) ...related to a retired couple shot dead in their home on the coast of Lincolnshire in August 2004 by, as it turned out, the pre-eminent organised crime group then operating in Nottinghamshire. Bluntly, without communications data relating to contacts between mobile phones **it would not have been possible to detect that crime** and lock up the people responsible. ..(Q147)...Bluntly, there were other people involved in the conspiracy whom it might have been possible to prosecute and convict, but who it but who it was not possible to prosecute and convict **because there was a data loss** in that investigation

Tracing this case using the details provided leads to news reports suggesting this account is materially misleading :

> **Police failed to protect innocent couple executed in gangland revenge attack, damning watchdog report reveals**[133]
>
> The IPCC upheld five of seven complaints made by the Stirlands' family. They found:
>
> • After the shooting incident at their Nottingham home, Mr and Mrs Stirland were given neither protection nor help by Nottingham police.
> • That incident was "not properly investigated, despite rumours circulating about who was responsible".
> • Nottinghamshire Police's failure to share intelligence with Lincolnshire Police about the threat to the Stirlands was "unacceptable".
> • The response to Mrs Stirland's call about the prowler was "delayed and unsatisfactory".

Moreover it emerged two years later at the inquest that

> **Stirland revenge hit men 'known before killings'**[134] Police had identified Nottingham crime boss Colin Gunn's **team of six hit men weeks before** two killed a couple in a revenge attack, an inquest jury heard....The former officer, who remained anonymous, said the two men who killed the Stirlands had been named as part of Gunn's team of hit men.

Although this case was offered in evidence as an illustration of the necessity of blanket data retention, in actuality it precisely illustrates how diligent and proactive use of targeted data preservation could both prevent and detect crime. Had communications data *preservation* commenced promptly about suspects identified weeks before the crime, *prima facie* police might well have been able to prevent the crime as well as catch the perpetrators. Furthermore, it emerged, contrary to the conclusions of the IPCC investigation[135] that:

> **Corrupt officer fed data to Colin Gunn on Stirlands**[136] A corrupt detective searched Nottinghamshire Police computers for intelligence about a couple killed in a gangland execution, an inquest heard.

It seems ironic that the police cite a fatal case of police corruption and its subsequently botched investigation, as justification for blanket retention of data about the entire population. It would be more logical to propose blanket retention of data on the entire police force. This is probably not the conclusion drawn by the Committee from the evidence heard.

---

133 Daily Mail 22nd February 2008 (http://www.dailymail.co.uk/news/article-517442/Police-failed-protect-innocent-couple-executed-gangland-revenge-attack-damning-watchdog-report-reveals.html

134 BBC News Online 3rd Feb 2010 (http://news.bbc.co.uk/2/hi/uk_news/england/nottinghamshire/8496826.stm)

135 http://www.ipcc.gov.uk/documents/stirland.pdf

136 BBC News Online 17th Feb 2010 (http://news.bbc.co.uk/2/hi/uk_news/england/nottinghamshire/8496826.stm)

Costs estimates for prior judicial authorization to access traffic data

In the 7th July evidence session[137], Angela Patrick of JUSTICE made the suggestion (Q274) that additional costs for introducing prior judicial (magistrate) authorization to access data could be estimated by extrapolating corresponding Home Office figures provided for the Protection of Freedoms Act (which required local authorities to get magistrate approval)

Here is the calculation, based on the Home Office's published estimates for PoFA[138] (£ 670k p.a), and the new 2011 Interception Commissioner's report.

Local authorities requests comprise 0.4% of the total (pp.39 IC). Suppose magistrates ought to approve the 48% (pp.29 IC) of requests comprising traffic or usage or location (or combined) data - i.e. all requests not purely for account subscriber data (pp.29 IC). The rationale is that subscriber account data is retained anyway, and that does not reveal dynamic behavioral data which is very privacy sensitive.

Therefore the initial estimate = 0.670 / (0.004 x 0.48) = £349m per year

However, there is a discrepancy, because the the Home Office figures say "we have assumed there will be **5,500** authorizations based on last year's usage (and we assess the magistrate's assessment will take 20 mins)", whereas the IoCC says "during the period covered by this report 141 local authorities notified me they had made use of their powers to acquire communications data, and between them they made a total of **2,130** requests. This is an increase from the previous year's figures (134 local authorities, 1,809 requests)."

Accordingly we reduce the £349m figure pro rata: (2130/5500) * 349 = **£135m per year**[139]

It should be emphasized this estimate is an upper bound based on a large extrapolation. A comprehensive system which integrated prior judicial authorization of interception warrants and communications data, could triage different cases to specialized magistrates, and so be much more cost effective overall[140].

August 2012

---

137 http://www.parliament.uk/documents/joint-committees/communications-data/uc170712ev4HC479iv.pdf

138 RIPA and Local Authorities, IA No: HO0031 Final, Home Office 22/12/2010 http://www.homeoffice.gov.uk/publications/about-us/legislation/freedom-bill/ripa-local-ia?view=Binary

139 However, it might fairly be said that the magistrates considering traffic/usage/combined data requests will be making more complex decisions about proportionality and necessity. The Home Office estimates the total cost of magistrate's time as £365/hr (inclusive of court overheads)

140 The French CNCIS regime is not based on separate judicial authorization, but manages prior scrutiny of both interceptions and communications data access, with organizational independence, at much less cost

Greg Callus

1. I am a freelance journalist, about to start a new career as a commercial barrister, and have a particular interest in digital developments as they affect the worlds of journalism and law. This submission is in a personal capacity, and does not necessarily reflect the views of any employer, group or academic institution with whom I am (or have been) affiliated. This submission, however, owes a significant debt to colleagues at the Open Rights Group and allies, but in particular to Alice Ross of The Bureau of Investigative Journalism ("TBIJ").

GENERAL THOUGHTS

2. There are other submissions which are far better placed to express a view on issues such as the Technical, Costs, Scope and Enforcement. My submission will focus almost entirely on the Safeguards questions.

3. Briefly, though, I would make just a short comment about the distinction between Content of communications and Communications Data. The distinction is recognised in RIPA, with Content requiring a higher degree of oversight, both in terms of original approval for interception, and in the post-hoc scrutiny by the Interception of Communications Commissioner's ("ICC") inspectorate. Communications Data interceptions are seen as less intrusive. I do not believe this is actually true.

4. Because of my work, I generally have to be incredibly careful about what I publish – it should be truthful, it should be within the law, it should not embarrass me. Consequently, there is little (if anything) that I write (whether for my own purposes, or in published form, or in private communications) that I would not be prepared to see in the public domain. I self-edit, even self-censor, because I consider anything I commit to written form might come back to haunt me.

5. This is overcautious, to be sure, but no more so than even a slightly-clever criminal or terrorist. The care-cum-paranoia I would expect to be exhibited by a serious criminal or terrorist would mean that most of them would communicate expecting a degree of interception, and self-censor accordingly. Self-censorship of communications renders intercepted Content less useful, but also less intrusive.

6. Conversely, show me someone's web-browsing history or who they send a text message to at 2am, and I'll know much more about them. Communications Data is less obviously-rich information, but it is capable of telling you more about a person than self-censored content ever will. What medical conditions did they google? Which Facebook profiles did they dwell on longest? Which mobile phone masts in Red Light Districts did their phone most-frequently use? Communications Data isn't just proto-Content data, or a preliminary stage of investigative data: it offers perhaps a better (yet more intrusive) insight into the private life and thoughts of the user of a communications tool. You can avoid saying anything significant in an email or phone call, but it's significantly harder to avoid your location being given away by your mobile phone. By reflecting the often-unconscious communications of the user (or their device), Communications Data is capable, even likely, to say more about the target's private life than Content Data ever will. Ideally, the bar for accessing Communications Data would be as high, if not higher, than for accessing Content Data. This may be unrealistic given the demands of the Home Office and current practice, but the assumption that Communications Data is "less-intrusive" needs examination.

SAFEGUARDS

7. I have little to add to the expected submissions by civil liberties groups on the warrants required for Content Data and the inspection regime. The biannual inspections seem to me to be relatively appropriate oversight for the few hundred such warrants issued by Warrant-Issuing Departments

("WIDs"). Similarly, I have no insight to offer on the issue of safeguards surrounding Prisoner Communications. My submission shall focus on the safeguards surrounding interception under the current Chapter II of RIPA: warrantless interception of Communications Data.

8. There is no need to burden the Committee with an explanation of the current RIPA safeguard functions, but in the interests of brevity, I will designate the major roles of RIPA authorisation with their initials: Designated Person ("DP"), Single Point of Contact ("SPoC"), Senior Responsible Officer ("SRO"), and Communications Service Provider ("CSP").

9. There are three safeguards issues that need to be addressed, though their issues overlap significantly:

   (a) the workings of the internal safeguard mechanism (DP, SpoC, SRO)
   (b) the sufficiency of the ICC and its inspectorate as an external safeguard
   (c) the transparency of the two safeguards to external oversight by the press/public

   The first is self-evidently important, and is scrutinised in the ICC's annual report, and those reports offer both quantitative and qualitative cause for concern. The second issue is not a matter of quality but of scale – essentially the disproportionate volume of Communications Data requests, versus the small size of the inspectorate. These two problems could both be ameliorated by greater transparency (requiring better data capture in the first instance), so that journalists could stand a better chance of holding public authorities to account for their failures. The issue of transparency and open data-sharing by both public authorities and the ICC is therefore of the utmost concern.

10. The best independent work on the internal safeguards has been done by Alice Ross of The Bureau of Investigative Journalism ("TBIJ"). She submitted a series of Freedom of Information ("FoI") requests to all the Police Forces in England & Wales, and Scotland, asking for the numbers of RIPA access requests from 2006-2011 and the proportion rejected by the DP. Her spreadsheet indicates that eleven of the thirty-eight forces (including the Metropolitan Police) have not provided this data at time of submission. Her report is summarised here: http://www.thebureauinvestigates.com/2012/04/05/variations-in-police-access-to-phone-records-raise-concerns-about-oversight/

11. Ross found significant disparities between police forces in the rates of rejection of RIPA requests by DPs, ranging from 0.19% to over 30%. Whilst some demographic/geographical factors (urban/rural, size of force etc) might explain part of this, either some forces were operating an incredibly lax system of internal push-back by DPs, or other forces were submitting to the DP a high proportion of inappropriate RIPA requests. Either would be worrying, and our inability to say which it is should also be of concern. The adequacy of training, and the standardisation of procedures should be a priority in making the internal regime more robust if it is to continue. This would also help manage the error rate identified as rising in the most recent ICC report.

12. There is worrying anecdotal evidence, both from Ross but also in the recent ICC Annual Reports, that the strict operational independence of DPs from the investigating unit seeking the RIPA request is not universally guaranteed. This amounts to self-authorisation of warrantless interception and in my view is the most-troubling failure of the internal mechanism of oversight. Whilst very occasional instances in Specialist Forces (such as anti-corruption units investigating the police themselves) might require this to ensure secrecy of operations internally, there should be no excuse for the majority of public authorities not having an entirely operationally-independent DP.

13. Ross also notes that councils seem to be especially troublesome – 9% of errors related to the insufficient seniority of the DP, there was frequent failure to give reasons for approval, and an instance where an Applicant was also both the DP and the SPoC. It is strange that the ICC is not vocally dissatisfied with the use of RIPA powers by councils, who collectively account for 0.4% of total applications but 10% of total identified errors.

14. In the course of investigating aspects of the Phone Hacking scandal raised by the Leveson Inquiry proceedings, I wrote an article on the current state of the ICC inspection regime, and its failings. It should be of extreme embarrassment to us all that one of the largest-scale scandals in modern times was rooted in the misuse of intercepted Communications Data (especially 'pinging' mobile phones to ascertain the location of celebrities), that the New York Times reported that it was partly due to information obtained unlawfully over the course of many years, and that this entire situation went unnoticed in the reports of the ICC. I mean no criticism of those involved – merely that the volume of requests versus the funding provided for external scrutiny and safeguards were so mismatched as to make the task impossible. It is the system of oversight that is insufficient, not the efforts of those with an impossible task on their hands. If hundreds of millions of pounds are to be spent as proposed by the Draft Communications Bill, is it too much to expect proportionate sums should be spent on rigidly enforcing privacy rights?

15. My article on RIPA and pinging can be read here: http://gregcallus.tumblr.com/post/20290988744/phone-hacking-more-pinging-still-government-policy and a particularly interesting response by leading Liberal Democrat blogger Mark Pack may also be worth your time: http://www.markpack.org.uk/31123/six-reasons-the-interception-of-communications-commissioner-has-failed/

16. To give a quick indication of scale, in last year's ICC report, the rate of Communications Data access requests was up to 552,000-or-so, an increase of 5% on the previous year. There is no perfect way of correlating this to number of people affected: several individuals' data can be affected by a single request, but a single individual can be the subject of many access requests. However, the volume of requests alone should give pause for thought as to how this scale of requests can ever be scrutinised by a Chief Inspector and five colleagues, who also have to oversee the 500+ Content Data warrants by WIDs, and prisoner communications interceptions as well. Sampling would be the only way, and sampling is identifying worrying numbers of errors, but when even a single instance of unlawful communications interception is so deep a breach of the individuals privacy, I do not think that the paucity of external review is anything close to being adequate.

17. Of greatest concern is the estimated 31,000 interceptions of Communications Data under the Urgent Oral Procedure (up from 21,000 or so the previous year). Designed to save time in life and limb danger, for terrorist plots in progress and kidnappings, it lowers the standards of oversight and record-keeping, making scrutiny by either the ICC inspectorate or others almost impossible. A 50% increase in Urgent Oral RIPA requests suggests either a startling leap in the detection of kidnappings and terrorist activity that somehow eluded the nation's press, or a growing misuse of more lax routes to accessing Communications Data.

18. Lack of data - even the total numbers of RIPA applications (versus the numbers granted) is not universally available - and data paucity make the system of safeguards opaque to external review. In many police forces, we cannot know how many access requests are made, how many are informally rejected, why they are rejected. The types of process-management software commonplace in commercial entities for order/invoice management (as built by companies such as SAP or ORACLE) seems woefully lacking in the non-commercial trade in Communications Data. A centralised secure system for request handling, authorisation by DP, communication to SPOC and then onto SCP, return of data, all with time stamps, reason codes and computerised identity checks would greatly assist the susceptibility of the RIPA regime to both ICC and journalistic scrutiny.

19. Earlier this year, as part of a story I was working on, I sent an FoI application to the Home Office requesting the names and ranks (only) of the past-and-present DP, SpoC, and SRO at each Police Force in England & Wales. My FoI request was turned down on grounds that releasing the names would be a breach of the Data Protection principles, which is an allowable exception albeit (in my view) woefully misapplied in this case. Internal review of this decision saw it upheld, and so I have referred the case to the Information Commissioner's Office.

20. The Data Protection principles are important, but the role of scrutinising large-scale surveillance is a public role, and the public are entitled to know who fulfils that role. How else can a journalist discover the relationships between operational staff and the DP who authorises their interceptions? How else can journalists discover a DP who also acts as a SPoC? How can it be private personal information for any police officer to hold the position of "Senior Responsible Officer" for RIPA authorisations at her police force, and yet journalists are not able to know whom to hold responsible, or even how senior she might be?

21. I have confidence that the ICO will follow case-law in this area, and compel the Home Office to release what information it has, but this is a common theme in RIPA stories. Compared to more mature processes such as civil litigation proceedings, or criminal justice from arrest onwards, the RIPA regime is incredibly awkward and opaque. Alice Ross told me that she was unable to even contact the ICC's office (sometimes referred to as the IoCCO) – unable to actually get an address or phone number for them, let alone reach a press officer for comment.

22. The RIPA regime ousted the classical role of the judiciary in issuing warrants for invasive searches. It is unlikely that the Draft Communications Bill will radically change that position. If we are to accept the permanent loss of formal judicial scrutiny in favour of internal authorisation and a small inspectorate, then two things become necessary: transparency of the internal safeguards process, and an improved working relationship between the IoCCO and the press, so that in lieu of the additional manpower that seems unlikely to be forthcoming, the inspectorate can rely on support of journalists in holding public authorities to account.

23. In the time and space available, this could only be a whistlestop tour of concerns from the perspective of investigative journalism. I hope that it brings some small novelty of perspective or information that might prove useful for your purpose. If there is any way in which I can assist the Joint Committee further, please do not hesitate to contact me.

August 2012

Graeme Carter

1. The draft Bill is the electronic equivalent of placing a Government official in every postal sorting office to record the details of all mail.

2. As David Davis MP has stated, career criminals (or anyone with any understanding of internet technology) will be able to evade the measures proposed.

3. Previous legislation such as RIPA has been misused as documented in newspaper reports. Can there be any doubt that the current proposals will similarly be misused?

4. Officials throughout the ages have sought this degree of surveillance. Will nobody stand up to them?

5. Just because something is made possible through technology does not make it desirable: if you couldn't do it in one medium, you shouldn't do it in another.

6. These proposals succeed because few MPs and no ministers have the moral fibre to tell the public that if we wish to retain our historic liberties we may pay a 'price' in increased exposure to terrorist and other risks. Officials trade on this weakness by advising ministers that they can stand up in front of the cameras to say they have done their best.

7. If more people die in road traffic accidents than through terrorism, what does that say about today's priorities and decision taking?

8. Other Acts have taken the power to issue warrants out of the hands of magistrates and into the hands of unelected officials. How much more of this is to be tolerated?

9. If this Bill becomes law then at the very least the senior investigating officer in a case should have to request a magistrate's warrant to obtain data, or, failing that, a warrant should be signed by the elected Police Commissioner for the area.

August 2012

Sean Cheshire

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill? Gathering data on every UK citizen, regardless of if a crime has been committed

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill? No

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy? It fits so well, it completely squashes any privacy</sarcasm>

4. What lessons can be learnt from the approach of other countries to the collection of communications data? Require warrant before data is collected

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider? Require warrant before data is collected

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data? Zero retention

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties? Sack all the law makers, and have them start again

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business? communications service providers will have a significant barrier to entry, as the costs involved in setting up the monitoring required are prohivitive
Costs:

9. Is the estimated cost of £1.8bn over 10 years realistic? No – 1.8bn every year will be closer to the real costs

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5 6bn. Is this figure realistic? What benefits?
Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill? Scope is too wide to make this a reasonable question

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order? No variation. Warrant required.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty? Unrealistic for any overseas provider – Sovereign law applies only to state not any other state

Use of Communications Data:
14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect? Use of data should be used to detect the crimes listed in the warrant

15. Is the proposed 12 month period for the retention of data too long or too short? Too long – Zero retention unless provided for by a warrant

Safeguards:
16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR? Warrant required for specific investigation

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be? Warrants required for all agencies, to include Secretary of State, and all government organisations, including MI5/6

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible? No

Parliamentary Oversight:
19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory? No. Parliament cannot be trusted, as they came up with this legislation in the first place.

Enforcement:
20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill? No penalties should be imposed until a warrant system is in place

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence? Any public authority that inappropriately accesses the data should have any evidence obtained from that access barred from any and all courts. Individuals that access the data for personal reasons should be dismissed, and investigated for criminal trespass. This would apply to law enforcement and MPs without exception

Technical:
22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content? In the current context, it is available, but unless the amounts given in my answer to question 9 are taken into account, the cost would be prohivitive

23. How safely can communications data be stored? By not storing it in the first place.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible? No.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ? with current technology, fairly easy. A private VPN to another country will provide you with a whole bunch of encrypted data. Only those who are inherently stupid (which the police can catch without help) or those that have nothing to hide will get their data stored. Those that are technologically smart, or have the money to pay someone to set it up for them, will be safe, as their data would be in a format that could not be decrypted.

26. Are there concerns about the consequences of decryption? No, for the reason listed in the answer to question 25

August 2012

The Coalition for a Digital Economy

1. Introduction

1.1 The Coalition for a Digital Economy (Coadec) is an independent, non-profit organisation that works to give UK digital startups and entrepreneurs their own voice in policy discussions and support legislation and other government policies that foster a vibrant, innovative and sustainable digital economy for Britain. We are made up of a wide range of members of the UK innovation community, including entrepreneurs, leaders of tech-driven startups and SMEs, inventors and developers, and many others who believe that the future of Britain lies in the success of its digital economy.

1.2 We are aware of many individuals and organisations that will respond to the consultation on the arguments surrounding the draft Bill's impact upon civil liberties and the technical problems surrounding the implementation of such a bill, we will be responding on the basis that the bill may have detrimental effect on the businesses of the digital startups and entrepreneurs that we work with who will fall into the categories of Communications Service Providers (CSPs).

1.3 We understand the Government's aim and the CSPs we work with allow for and are more than keen to comply with lawful requests for data. In the UK we have some of the best time for disclosure in the developed world and there are many existing methods for Government to obtain communications data from CSPs. On examining some of the new provisions within this Bill the businesses we work with were extremely concerned on a number of fronts.

1.4 As requested by in the Joint Committee's call for evidence, we have kept our submission brief. The discussion points below seek to address the most relevant questions to the businesses we work with, but not all of the questions in the call for evidence.

2. Definitions

2.1 With regards to the definitions of communications data and Communications Service Provider, it is unclear whether the Home Office intended for these to be quite as broad as they could be theoretically applied.

2.2 The definitions as they currently stand throw up questions such as would small and medium CSPs be included? Does it matter if communications is only a small aspect of your business? Is the location of the servers an issue?

2.3 Under the current proposals any business providing any element of communications could be required to collect data on their subscribers. This means it would not just be big digital businesses who specifically provide a communications service, such as a social network or an email provider, but also retail sites that allow buyers to communicate with sellers, a recruitment website that allows employees to respond to adverts, a personal finance site that has contactable advisers, and many more.

2.4 These unclear definitions would create a legal uncertainty around digital startups and whether they would be required to comply with these measures. Uncertainty is a major disincentive for investors. At a time when we are looking to increase inward investment in UK businesses, certainty in clear definitions is vital.

3**. Costs**

3.1 We are disappointed by the lack of consultation undertaken by the Home Office before these measures were proposed. When conducting the Impact Assessment to support the Bill which determined the cost level announced, the Home Office only consulted users of the data. In failing to consult more widely with the CSPs who would be expect to deliver these systems it is difficult to see how the costs have been determined.

3.2 There are further unknown factors that mean the previous costs calculated as there remain too many unknown factors in the proposals. As mentioned earlier in this response the definitions are extremely broad, so it is difficult to determine the number of businesses that will be affected. If there is no provision for small businesses, every single entrepreneur developing a digital business with some communications element could be required to invest time and capital developing a system to comply and recoup the costs.

3.3 This wouldn't just apply to existing digital businesses. The costs for this policy are to be applied on a 10-year basis, however 10 years ago many of the services we regularly use today didn't exist such as Twitter, Facebook, Gmail and Skype. As UK startups grow, and the aim of seeing world leading digital communications businesses to rival existing organisations to come from the UK is realised, this cost could increase phenomenally in a few short years.

4. Collection and retention

4.1 As well as the initial concerns about whether digital startups and SMEs would be required to comply with such an order, most of the businesses we spoke to were disturbed by the possibility of being asked to develop standardised systems for data collection and to retain data they would not normally collect.

4.2 Entrepreneurs, and early stage startups which often consist of teams of 2 or 3 people would face huge challenges installing collection systems and setting up automated access systems without compromising the security of their systems. Increasingly startups are encouraged to develop using lean techniques to develop products and services without large amounts of initial funding, and one of the most important principles behind this is minimum viable product. The idea is to create a version of a product or service that serves a test function and release it as soon as possible in order to continue to iterate and release repeatedly to refine the product.

4.3 Being forced to build into each iteration a standardised system for collecting, retaining and making accessible communications data would severely impact upon a digital businesses ability to do product development and the systems will in all likelihood have to be regularly updated to cope with growth and any additional services that have been added.

4.4 Asking startups to retain data that they do not need in the course of their business would seem to add an additional barrier to entry and capital expense in collection resources and impact upon their existing relationships with the customers. This was a core concern of the businesses we spoke to about these proposals who value the privacy of their customers data. They were shocked at the possibility of being asked to retain data without their subscribers knowledge and potentially being asked to disclose this without the option of having oversight of the data that would be released.

4.5 This would take away the control customers have over the privacy and use of their data out of their hands. For customers not based in the UK this would in all likelihood drive them to use systems based elsewhere and businesses based outside the UK would be able to market their services on the basis that they did not automated systems to provide law enforcement agencies with customers data without any oversight when in competition with a UK based firm.

5. Innovation

5.1 Asking digital businesses to standardise their data collection systems fundamentally misunderstands the way digital businesses are developed. The very architecture of a digital business rests upon the way they handle the data they collect. If digital businesses are forced to standardise this you risk killing innovation and keeping UK businesses stuck in 2012 for the foreseeable future.

5.2 We already face a shortage of skilled coders and developers in the UK, and the Government has recognised this and kick-started the process of reforming ICT GCSEs to make them more able to deliver programming skills desperately required in digital industry. If you inhibit their ability to innovate they will be increasingly likely to be attracted by the prospect of growing their business abroad.

6. Growth of startups

6.1 In the UK over 8.3% of our GDP is generated through the Internet, which is a larger share than any other EU economy. In 2010 this was worth £121 billion. In a time where we are looking to this vital source of growth creating a new a barrier to entry would seem to counter the Prime Minister's aim to make “the UK the best place in the world to start, run and grow a hi-tech company”.

6.2 Our fundamental concern regarding the process is that while the impact assessment seeks to determine the cost, and the Home Secretary has recognised the concern on the impact on civil liberties, no where in the Bill or in statements from the Home Office has the effect this bill will have on small businesses been recognised.

6.3 To highlight some of the arguments we have made in this submission below are two existing businesses we work with who could be required to comply with an order.

Zummer (www.zummer.co)
A social app that allows users to create a live wall for a variety of uses including an event, a topic, a question, and many other. The walls created on Zummer update in realtime, and feature photos, videos, locations, songs and comments can all be added to the live walls. Zummer was founded by Tony Million, a successful entrepreneur who previously co-developed the Sonique media player that had over 100 million users in its peak and was sold to Lycos for $55 million.
Tony told us:
"This kind of proposal creates an impossible situation where I would be expected to make all data accessible while simultaneously expecting me to clamp down on data intrusion. While the power of the internet can cause concerns for monitoring communication activity, on the flip side is it means I can incorporate my company and data in another country, which would seem far more appealing if this bill were to be passed as it is. If I was given a warrant that ordered me to hand over data then of course I would comply, but the onus wouldn't be on me to put it in a standardised format for the police, thats not my job, and doesn't earn money for me, my business, or my investors."

Teddle (www.teddle.com)
Teddle is an online service that connects providers with their community enabling customers to book quality local services such as cleaners, plumbers, carpenters, tutors and many more, instantly. Teddle was founded by Jules Coleman, Alex Depledge and Tom Nimmo and they firmly believe that local small business is at the heart of every community and their platform aims to help customers feel part of their community while also driving money and growth into the local economy.
They told us:
"We are particularly concerned about the proposals as we would find it difficult to put up, even temporarily, any extra costs of implementing a system like the one that is proposed. We would also be concerned about any extra data we would be compelled to collect from our providers who use our service which could deter them from wanting to be listed on our platform".

7. Conclusions

7.1 While we are grateful that we have been afforded this opportunity to comment on the proposals, it is our belief that many of the objections could have been addressed with a full consultation process, where expert opinion could have been consulted to avoid some of the most apparent flaws, particularly in relation to the technical issues.

7.2 The bill as it currently stands **undermines the fundamental nature of digital businesses** by dictating how they handle their data. It **threatens innovation** and **risks driving digital businesses away from the UK** by reducing the UK's competitiveness.

7.3 **There needs to be a full and proper consultation process** so the issues can be discussed and the Government can garner a proper sounding of the public's amenability towards these proposals and the businesses affected can have their considerations taken into account.

7.4 **The cost needs to be more accurately assessed** with supporting evidence and consultation with those who will be expected to deliver these system.

7.5 **The range of data that can be collected from a business should be limited to communications data they already create** as part of their regular business activities rather than additional data they do not use, and requirement for **standardising data collection should be reconsidered as it undermines startups ability to innovate and grow**.

August 2012

Wendy Cockcroft

These are my comments on the Communications Data Bill, AKA the Snooper's Charter, proposals. To cut a long story short, the proposed bill is a pointless waste of time and a massive intrusion into the privacy of the citizens and residents of the UK. It represents the venal, selfish, sleazy state of the members of the Government who proposed it and is a blight on Britain's record as a free and fair country. Get rid of it now! This is why:
General:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

It has in some ways: it wants to be able to find out who we have been communicating with on our phones, in our letters and in our emails.

However, it hasn't told us which private contractors will be involved and what for. It also hasn't explained what "a business case" for the communications data required by the local authorities is. It also hasn't told us why blanket surveillance of the population is necessary when a targeted approach would be more effective.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

No, not at all. If anything, it has convinced us that they're in thrall to the industry lobbyists who stand to gain considerably from this in terms of data mining (that's what the "business case" is, isn't it?) and management fees. It's particularly galling to learn that we taxpayers are to foot the bill for this nonsense. We're having none of it!

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

It is outrageous that any government official wants to know, without a warrant, who I've been communicating with by mail, phone, or email. It's a presumption of guilt! Haven't you heard of Habeas Corpus? Oh, wait, you're planning to get rid of it. Silly me, I keep forgetting how much you are doing to dismantle the structure of our democracy.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

Not to copy the oppressive regimes where this is in force. Have you noticed how badly their economies are doing? China is only working at the level it is because it has devalued its currencies, practices protectionism, and permits Western companies to outsource jobs to them. Stop outsourcing and the truth is revealed: oppression is bad for the economy. Contrast that with countries that do not receive the same level of FDA (foreign direct investment) and you'll see I am right.

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

The current proposals create more haystacks to hide needles in. A targeted approach with warrants required to access the data works more efficiently. Warrants safeguard our rights, and must be issued for all attempts to put anyone under surveillance. Warrants can be issued per person rather than per item, I wouldn't oppose that.

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

Get rid of all retention. Don't retain any data without a warrant!

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

Civil liberties are unbalanced as it is. Get rid of data retention except as part of a criminal investigation.

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

Costs:

ISPs themselves are best placed to tell you that. http://www.meritalk.com/pdfs/big-data/MeriTalk_Big_Data_Gap_Press_Release.pdf provides an idea of what this looks like. Bear in mind that when they collect the data they have to store it and that means buying more servers. You demand that they underwrite the cost of this pointless, wasteful exercise, and they have to pass the costs on to us. We're in the middle of a recession and I'm a web designer. This raises my operating costs. Why should I support it if it's doing nothing apart from providing a power trip for some bureaucrat? Show me A benefit. Just one.

Now think about the time spent looking for the information you want. Actually think about it. Let's make this easy enough for a politician to understand: if you have an email account and get a lot of emails, how do you find the email you are looking for? In Gmail there's a search function. I may use a name or a keyword to find what I'm looking for but it can take some considerable time, even in my own personal email account, to find the item I am looking for if the keyword or name I am using as the search term is repeated a lot in the emails I have stored.

Now multiply this by about 50 million and you'll see the problem. Some of us have multiple email accounts. I certainly do. NOW can you see the problem? And you wonder why we fight against this?

9. Is the estimated cost of £1.8bn over 10 years realistic?

No, not at all. Every time the government comes up with a projected cost for nonsense of this kind, the actual costs spiral out of control.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5 6bn. Is this figure realistic?

No, it's nonsense. First of all, we the taxpayers, who voted the liars who said they would roll back the surveillance state into office, are obliged to pay more to our ISPs to facilitate this wasteful nonsense. They will need more servers — and the warehouse space to store them in — to store our data. Actually decrypting this is another matter altogether so the data itself is just sitting there in the servers, gathering dust and cobwebs.

Then you have to pay for the man-hours to try to get hold of a piece of information using search terms that, as I pointed out earlier, may well apply to hundreds of thousands of other people. Good luck with that.

Trust me on this, the £5-6bn (probably more) will be going to the private contractors you plan to get to oversee the data retention and decryption.

Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

No, because they dismiss the legitimate concerns we have that the information will be mishandled and the powers abused.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

No. Get a warrant. And get rid of the bill.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

Ah, so you've noticed the flaws in the plan? The only solution is consolidation and permitting the centralization that would make the internet vulnerable to attack. Decentralization is what keeps it afloat. If you don't understand how it works, don't legislate for it.

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

All of them, using a warrant, in a targeted approach that accesses the communications data of the subjects of the investigation, not all of us.

15. Is the proposed 12 month period for the retention of data too long or too short?
Safeguards:

There should be no mass data retention at all. The safeguards are inadequate and as I pointed out it's a presumption of guilt.

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

Get a warrant!

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

Warrants should be required by any and all persons and agencies who wish to have access to our communications data. Warrants per person rather than by item that describe the scope and purpose of the information required, with evidence for probable cause, will suffice. Resource requirements for this would be lower because of the man-hours that would be spent digging for this information would be fewer than in a mass surveillance situation.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

No, not at all.

Parliamentary Oversight:

Pointless, since you're in the business of eroding our privacy rights. Why would someone who cares nothing for our privacy want to protect it and defend our rights? It's oxymoronic.

19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

No, not at all.

Enforcement:

Not gonna happen. Remember Jean-Charles de Menezes? That's why. You'd let something awful happen, shrug, say it's not your fault, then do it again. And again, and again.

20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

No, and I don't believe for a moment that they would be enforced at all.

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

You should just scrap the bill.

22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

Not really. Imagine a wall between you and the property of the man next door. It comes up to your hip in height. It's a boundary mark, but that's it. If you want to take a shortcut to get to his house you have only to climb over the wall. Not even climb. One leg over, then the other, and you're there.

23. How safely can communications data be stored?

Don't, except as part of a criminal investigation under judicial authority, with a warrant.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

It's all a huge pile of hogwash because there's a huge gulf between what you claim you want and what would actually happen in practice.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?

VPNs, mesh networking, coded conversations, other methods of communication including talking to each other in locations out of the reach of surveillance equipment. Stop watching James Bond and think about how people actually operate in practice. David Davies put it best when he said you'd catch the innocent and the incompetent. He's right, pay attention to him.

26. Are there concerns about the consequences of decryption?

They might interfere with the operation of the internet itself, they may create vulnerabilities for criminals to exploit... you know how vermin and weeds develop immunity to poisons? That, but on the internet. People will find ways to strengthen encryption and you will find ways to break it. See malware for details.

Conclusion:
You really haven't thought this through, have you? Stop messing with the internet and stop eroding our privacy rights. All this surveillance is a costly favour to the private contractors who have frightened you into it. Remember the Seventies and Eighties when the IRA were bombing the country? Remember the complete lack of calls for general public surveillance? I lived through that and can assure you that mass surveillance of the public is unwanted and unnecessary. Stop it now!

August 2012

Paul Connolly

I am an accountant living and working in Northampton. Although I call upon my own experiences in life, public finance and IT project finance in this document, I'm not holding myself out as an expert in any field, rather simply as an informed and concerned citizen.
Below I give my personal opinions relating to the draft Communications Data Bill and would ask that the Joint Committee consider these when deliberating the bill.
I think the bill should be completely scrapped. I have concentrated on three main reasons why I think this:

- Direct conflict with the Human Rights Act.
- Technical unfeasibility.
- Financial detriment to small business and thus creating economic damage.

1. Direct conflict with the Human Rights Act
1.1 The basic thrust of the bill is for Internet Service Providers (ISPs) to automatically collect new wider sets of data that each citizen has transmitted. No suspicion of wrong-doing is needed to warrant this expansion of collection, this information is to be gathered by virtue of the simple fact that the citizen exists and communicates.
1.2 This implies that everyone is under suspicion, that their actions have been recorded as evidence for their possible future prosecution, waiting only for the police to turn their attention to that particular citizen when the time comes to investigate them.
1.3 Promoters of this bill are quick to assure us that the "content" (e.g. the message inside the email, or telephone conversation) will not be kept, and only the "communication data" (who rang whom, when, from where and for how long) will be kept.
1.4 This statement seems intended to placate opposition to the bill, but belies the truth of the staggering power that profiling with communications data actually has. Imagine that, if Google, with current communications data, can automatically drop adverts onto your webpage that are spookily close to your own tastes and pastimes, then what a concerted effort by the security forces could put together from a yet wider and deeper set of your communications data.
1.5 The false imprisonment of the Birmingham Six springs to mind. They were in the wrong place at the wrong time but "fitted the profile".
1.6 The "communications data" as described in the bill is clearly "correspondence" as described in the Human Rights Act article 8.1. By denying the citizen's right to keep his or her data free from systematic cataloguing as evidence, the state would not be respecting private life and family of its citizens nor their correspondence.
2. Technical unfeasibility
2.1 In order to strip out from a citizen's communications the "content" and keep only the "communications data", the ISPs must use something called "Deep Packet Inspection". This is a technique performed by purpose built hardware or software (a "sniffer program") which interrogates each block of data as it comes down the line.
2.2 An analogy would be to say it is the electronic equivalent of opening the envelope that contains my letter to John, recording everything before "Dear John" and everything after "Yours sincerely", then replacing the letter into, and re-sealing, the envelope, then sending the envelope onwards to John.
2.3 In electronics communications, ISPs would need to use these sniffer programs to do this but, these days there so many of forms of electronic "envelopes" that contain this data, including, but not restricted to, email, webmail, social message, chat and gaming applications, viop (e.g. skype), instant messaging.
2.4 That means firstly, that writing and testing these programs would be enormously problematic and costly, I will explain further.
2.5 Let's take an email. The sniffer program would first have to intercept and assemble that email, figure out what is content and what is communications data, take exactly only the communications data and leave the content behind.
2.6 Remember that if even the smallest part of content data is pulled, then that data as evidence is inadmissible in court, so the program has to be honed to near perfection.

2.7 In the old days, with a conventional email, most of this communications data information sat conveniently in an area called the "header", where it was easy to get at and strip out. But with webmail, it is now mingled with the "html" code scattered in the body of the webpage.
2.8 As the use of this type of web communications grows, the complexity of these sniffer programs will need to become more sophisticated. The manipulation that these programs perform effects the webpage's transmission speed, so even if the lexicographical hurdles were somehow overcame, the speed of the internet would dramatically slow down (akin to China).
2.9 Over time the problem of this inter-mingled content and communications data within web pages would hit more difficulties:
2.10 Every time a change in the wider internet occurs, (a good example would be the current HTML-5 roll-out), webpage code would change and these sniffer programs would need re-calibrating. A human being would again have to un-pick the html code to separate the content from the data communications to update the sniffer program.
2.11 This human would need to be an intelligent and experienced IT professional who understands code and the nature of data. It is unlikely that such people would be interested in such boring and unsatisfying work.

3. Financial detriment to small business and therefore economic damage

3.1 The bill mentions the implementation cost being £1.8bn and the benefits being £5bn to 6.2bn. I couldn't find any itemisation of these costs and benefits which is what I would expect from any professionally written investment project proposal.
3.2 Given the spectacular failure of the ID card database IT project; where a mal-conceived project was allowed to spend public money unfettered before collapsing, the state needs to ensure the setting up of proper budgetary control into its proposals. Which also means sincere and transparent attempts to quantify their estimates.
3.3 The omission of these details points either to an unwillingness to share the real detail or, just as worryingly, that the Home Office cannot estimate these costs and benefits scientifically because it doesn't know how it will implement the project.
3.4 But even our concern of these unknown costs, in itself, is not the major problem here. The crippling effect of the pushing of that cost burden onto the small ISPs is the problem.
3.5 With Deep Packet Inspection sniffer capability demand high, and capable IT talent supply low, then there could be a large fee uplift demanded by the IT developers that can do this work. Small ISPs would either have to cave in to high consulting costs or be beholden to some kind of software or hardware solution offered up by the big players which they would still need to manage. They would still end up paying, either through expensive training, or expensive maintenance contracts.
3.6 A barrier to entry would be created, keeping hosting start-ups out. The hosting industry would become increasingly vulnerable to the large hosting companies.
3.7 Large companies tend to consume talent rather nurture it. They concentrate on consolidating their commercial position rather than directing creative energy that conversely, abounds in a small business.
3.8 If small businesses are eradicated from the industry in this way, the multinationals will be free to restructure operations via their favourite tax havens (e.g. similar to what large internet firms now do in Ireland), thereby denying the exchequer rightful tax revenues from operations in the UK, and create another market failure here in the UK.

August 2012

Joe Corrall

General:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?
   No. There has been a large degree of deflection when asked direct questions about the scope and focus of the bill.
2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?
   No. The Government has not provided strong evidence that existing warrant powers are ineffective and that this level of tracking and surveillance will be positive, rather than oppressive.
3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?
   To my perspective, while EU laws and other organisations seek to protect or enforce privacy for the individual (particularly the recent dropping of the ACTA proposal as an example), this is odds with that climate by enabling greater loss of privacy.
4. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?
   Have you considered not spying on your own citizens?

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

   Removal of one liberty eroding measure should not be considered as acceptable to trade for another. Would you replace one dictator with another?

Costs:
9. Is the estimated cost of £1.8bn over 10 years realistic?

Absolutely not. Given the massive overspend on every significant government project for the last 10 years the odds of hitting this projected target 10 years in the future is virtually nil. Given the costs required in storing the amount of data aimed to be collected alone would rack up bills in the millions per year.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?

Absolutely not. This is a generalised figure plucked from mid-air based on nothing but assumptions. Storing data and tracking every digital citizen of this nation cannot possibly save money, only cost. I'm amazed this figure has been quoted as it shows a complete negligence and perhaps ignorance for the basic tenants of commerce.

Scope:
12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

In the event of this bill passing, only police enforcement should have any access to its data. Political parties should have no access, and no effect, over its contents. Should such a database be compiled I would trust professional law enforcement officials over an MP with an art history major to be handling it.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

Given the Government's current attitude to extradition requests from the USA I would say you stand about as much chance as a snowball in hell of successfully pursuing any organisation abroad for breach of duty.

Use of Communications Data:

15. Is the proposed 12 month period for the retention of data too long or too short?

Drastically too long. If the crown prosecution service is unable to formulate a case within 12 months of the crime taking place I would argue that they are wasting tax payer time and money. Given that no database is ever secure (I'm a software tester, trust me on this) storing any such data for any length of time is only increasing the security risk of this data being taken for malicious purposes.

Safeguards:
17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

If the bill should pass, a warrant should be vital for preventing abuse and unnecessary intrusion into the public's private life. While the additional demand on judges would be noticeable, a smoother warrant application process, and the knowledge that such measures are a last, not a first, resort should minimise this.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

No. We are in a climate of austerity where an increasing percentage of the public struggles to afford day-to-day living, and you want the creation of two new high paying commissioner roles for one aspect of policy that could be easily handled by the current judicial authority? I don't think that's going to be an easy sell.

Enforcement:
21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

It should amount to an offence. Mis-use of public office. Mis-use of private data. Mis-use of power. Take your pick.

Technical:
22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

No. This bill completely neglects to examine the use of proxies and VPN systems which would place all activity beyond the tracking ability of any ISP. Any serious criminal activity (the type this bill is supposed to target) would be operated over these publicly available services and you simply wouldn't get the log you desire. It seems this bill would only apply to the stupid or the innocent.

23. How safely can communications data be stored?

It can't. As a lead software tester I can reliably inform you that no system is secure, and not database doubly so. Given that you will want this database internet accessible for different departments to use it's a matter of when, not if, it gets hacked and details made publicly available.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

No. While you claim to record only data headers of internet communication, it's impossible to receive this without also receiving the content of the transaction.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?

Very easy. A quick Google search will give you a lost of proxy servers publicly available that you cannot track activity over.

26. Are there concerns about the consequences of decryption?

Yes. If you decrypt an encrypted transaction, you add a token to that transaction which indicates that the action was decrypted. This will render a number of financial communications invalid as it would appear the communication has been tampered with.

I doubt very much you've performed a feasibility study of this action?

July 2012

Simon Cramp

I think just like to make the following point which may be further questions and concerned I have

In the draft bill it seems to make clear it would be if enacted as the communications data act 2012. but what I can't find in the draft bill is any consultation with the department of culture media and Olympics and sport and business and innovation and skills who are the sponsoring department of ofcom the telecommications regulation as set up under the office for communication act 2002 and then provided and carry out its powers under the communication act 2003 and with a view recently by the secretary of state for dcms in amending it with a new white paper later this year in the form of the draft communications bill why is the home office seem to be acting alone in the draft bill when it seem s there has been no discussion between government department I may be wrong .

Two Ofcom asked for data already for television and other thing on a voluntary basis for motioning things why does not say in the draft bill that perhaps certain numbers of people either via ofcom or the security service are ventied

It just seems to come from the wrong way that it just the home office that is the only government department to be the sponsoring department

The other think I was going to say I am concerned re if some accedeintly click on a website they shouldn't and then consquesies happening say if they have a learning disability or a mental health problem will it be treated with symphy and sentively. Although I accept it can work the other as well

August 2012

Patrick Cunningham

1. The bill is not required. There are more than adequate options in place for government agencies to access the private information, both physical and electronic, of people suspected of crimes or terrorist acts. These are well tried and tested, are subject to proper scrutiny by the courts and by parliament, and have suitable checks and balances in place to ensure fair dealing and reasonable recourse for individuals who feel aggrieved or unjustly treated.

2. The powers envisaged in the bill will not only remove the opportunity for individuals to challenge unfair treatment at the hands of the police, the intelligence services and other government agencies, it will remove even their right to know that certain acts have been carried out and data collected and retained. This flies in the face of our long history of respect for individual human rights and the right for individuals to know what data is being held about them by government agencies.

3. The argument that the information gathered will only be used for benign and legitimate purposes presupposes that the currently prevailing political, public order and military conditions will continue. This is a fallacious argument; a future dictatorial government or police state would use the information and information gathering channels which the bill will establish for its own purposes.

4. Even the present regimes of police and intelligence have been shown to indulge in cover-ups, illegal activities and contraventions of human rights. Miscarriages of justice because of the illegal and unjust actions of members of the police and intelligence services have been, and continue to be, uncovered on a depressingly frequent basis. This bill will make it much harder for individual citizens to uncover such failings, shortcomings and illegal activities, and make it easier for those perpetrating them to do so without fear of discovery.

5. The 'War on Terror' has resulted in the removal of many personal liberties already – unnecessarily and far in excess of what is required to maintain an adequate level of public safety. Instead of spending millions on enhancing our security services the government should be making real and effective attempts to negotiate a proper settlement of the underlying global issues – Palestine, human rights, cultural respect, fair trade and mutual support. The 'War on Terror' will never be 'won', because it is not a war, it is not a fight against an oppressor, but an unstable situation arising out of deep-seated injustices. These injustices are capable of being resolved; all we lack is the political will to resolve them.

6 Our democracy relies on respect for the three powers – the executive, parliament and the courts – to maintain a proper balance, avoid the unacceptable exercise of power by one element and maintain the balance between the rights of the individual and the needs of the government. This bill fundamentally undermines that balance. The requirement for government agencies to obtain consent from the judiciary for a range of activities is one of the most fundamental expressions of our commitment to the balance of the three powers, and one which has stood the test of time and permitted our system of policing by consent. If this balance is shifted further in the direction it is already going, the government, the intelligence services and the police run the risk of losing the consent of the people, and this will result in a rapid breakdown of our unique society. This is already happening; instead of responding to it with increasing authoritarianism, the government should be striving to redress the balance and to regain the trust and consent of the British people.

7. I note from your consultation document http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/news/call-for-evidence/ that "The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn" and "the estimated cost [is] £1.8bn over 10 years". What are the 'benefits' referred to and how have this figure been arrived at? It worries me that these

'benefits' will include commercial advantage derived from the government's proposed surveillance, something which is not supposedly an intention of the bill and something which would be wholly immoral, unjustifiable and abhorrent if it were to become fact. I cannot envisage how the country could benefit to the tune of £5-6bn purely from the use of the data collected within the terms of reference so far disclosed.

8. The Bill envisages the establishment of another whole layer of publicly-funded posts; an Interception of Communications Commissioner and an Information Commissioner, along with their offices, staff and establishments. These posts are unnecessary; we already have a well-established courts system in place which undertakes many of the duties these posts would fulfil, and does so effectively and cost-effectively in a balanced way which holds the rights and responsibilities of both citizens and officials in equal regard. The officials appointed to these new posts would be political appointees and would not be directly answerable to the electorate or the general public. They would be subject to political pressure and would not therefore adequately fulfil the role of guardians of the rights of the public. They would also represent an unnecessary expense.

9. I object to the tone of your consultation paper (linked to above). It appears to accept that the bill will be enacted in some form and asks questions designed to 'fine tune' the bill. It does not address the fundamental issue of whether such a bill is needed. I do not accept that the bill is needed. It should be abandoned forthwith, and the government should instead draft a bill outlining the safeguards needed to avoid unauthorised access to electronic data, in order to bring legislation into line with the electronic age, with the same criteria as a starting point that are already incorporated into our legislation protecting traditional methods of communication – postal services and telephony, for example. This should cover unauthorised access by individuals and by government agencies. The new bill should also clarify the limits which the courts should impose on the various surveillance and law enforcement agencies, and enshrine the requirement for a court order to be in place before any surveillance is carried out, with robust requirements for evidence to justify the order. Further, the concept of there being some system of bargaining over legislation outlined in your item 7. is abhorrent. It will never be acceptable to trade one area of personal liberty for another. Personal liberty is a starting point, and any erosion must be backed up by overarching arguments of necessity in every case. It can never be valid to exchange one area of civil liberty for another; if it might be acceptable under these circumstances to scrap an infringement of liberty which already exists, then that infringement should be scrapped anyway because it is clearly not necessary at the most fundamental level required to justify it in the first place.

In conclusion, this government scrapped the ill-conceived and anti-libertarian proposal of the previous government to build a national database and impose identity cards, and for that I am grateful. It is very strange that the same government is now intent on imposing undemocratic and unaccountable powers to interfere with our personal communications. Please think again. Of course there are many occasions when it will be justified for our enforcement agencies to access the personal communications of individuals involved in terrorism or crime, but the right to do so is one which should be exercised with restraint and proper care, and only in exceptional circumstances. This bill if enacted would open the floodgates and result in innumerable officials demanding the right to know what we are saying to whom and when, on the most untenable grounds. It goes against our fundamental human rights as citizens of the United Kingdom, and should be dropped.

September 2012

Chris Davey

Has the Home Office made it clear what it hopes to achieve through the draft Bill?
No, there seems to be several high level objectives along the lines of (National security, crime prevention and detection) but none seem to have detailed analysis into how this bill will specifically address these objectives.
Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?
The bill adds a presumption to guilt onto every person in this country. No member of parliament would agree to have all of their physical mail or all of their face to face conversations monitored and recorded as it would be against their civil liberties. The same should be true of every form of communication. If there is suspicion of wrong doing then let the courts decide if monitoring is an adequate response instead of monitoring the majority of people who are doing nothing wrong.
It also presumes that the people who are communicating about things of interested be they criminal or of national importance won't be encrypting the content or adjusting the details of what is being sent to who. It's the same mentality as internet providers blocking direct access to piracy sites, this only stops people who wouldn't be using them accessing them. Anyone who wants to use them knows how to access them via other means. In the same way this is only going to capture information on people who don't want to be talking via secure means.
How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?
The bill is clearly highly intrusive. The vast majority of people do nothing wrong and yet you want to capture data on all of them. How can this be posed as a reasonable response to crime or national security.
Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?
Yes, let the courts decide on a case by case basis what can be captured depending on the risk involved in the case.
The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5 6bn. Is this figure realistic?
Where is the evidence that supports this? The police can request access to this information at present so how is storing it for longer periods of time going to provide any form of positive financial benefit?
Safeguards:
Given the governments form on keeping data secure it is unlikely any amount of safeguards can make the bill worthwhile. There have also been a number of high profile failures of communication providers to properly secure information much of which has largely been leaked directly onto the internet by hacking groups. Has any analysis been put into the cost to the UK economy of all communication records being potentially publicly available?

August 2012

The Direct Marketing Association

Introduction

The Direct Marketing Association (UK) Limited (DMA) is Europe's largest trade association in the marketing and communications sector, with approximately 900 corporate members and positioned in the top 5% of UK trade associations by income. The total value of direct marketing to the UK economy was estimated to be £9.1 billion in 2011. This comprises three separate figures; £4.3 billion on expenditure on direct marketing media and activities, £1.1 billion on goods and services brought in by companies to enable the undertaking of direct marketing activity and £3.7 billion on the spending of people employed in the industry as consumers (Putting a Price on Direct Marketing The DMA July 2012). The DMA represents both advertisers, who market their products using direct marketing techniques, and specialist suppliers of direct marketing services to those advertisers - for example, advertising agencies, outsourced contact centres etc. The DMA also administers the Mailing Preference Service, the Telephone Preference Service and the Fax Preference Service. On behalf of its membership, the DMA promotes best practice, through its Direct Marketing Code of Practice, in order to maintain and enhance consumers' trust and confidence in the direct marketing industry. The Direct Marketing Commission is an independent body that monitors industry compliance. Please visit our website www.dma.org.uk for further information about us.

The DMA welcomes the opportunity to respond to this inquiry by the Joint Committee on the draft Communications Data Bill.

1. General Comments.

The DMA welcomes the Government's plan to revise the framework under the Regulation of Investigatory Powers Act 2000. However we have a major concern over the application of the draft Communications Data Bill to postal services.

2. Postal Services.

We are particularly concerned over Clause 25 of the draft Bill which extends the application of Parts 1 and 2 to postal operators and postal services. We are not aware that any postal operator currently has the technology to record the relevant details such as where a letter with a particular address on it was posted or entered the postal operator's system. The cost of installing such a system would be immense and we doubt whether the benefits would be proportionate to the cost of installing such a system.

We note that in Clause 26 of the draft Bill there is a provision requiring the Government to make arrangements to ensure that postal operators receive an appropriate contribution toward their costs of compliance with Parts 1 and 2. However, we believe that the costs of compliance would be far more than any likely contribution.

August 2012

Mark Drury

1. I submit that the draft Bill is wrong in principle because it seeks to turn the entire UK population into crime suspects.

2. If I am suspected of a crime the police should investigate me, and obtain an order from a judge if they feel the need to break into my home or intercept my communications. If I am not suspected of a crime then the police should leave me alone to go about my business.

3. The presumed logic of the government securocrats appears to be:

"No actual crime has yet been committed, but it might be in future, and by anyone.
Therefore we need to put the entire population under surveillance."

4. This is a further extension of the state collecting, trawling and retaining data about people's everyday activities 'just in case' – ANPR is another example. This is inconsistent with British values as it violates both the idea of being 'innocent until proven guilty' and that 'an Englishman's home is his castle'.

5. Her Majesty's Government is happy to point the finger at other countries which routinely spy on their citizens. But the East European STASI could only have dreamt of the surveillance capability modern technology and this draft bill would have given them. It is completely inappropriate for a parliamentary democracy.

6. In conclusion, as I am not a crime suspect, the state has no business knowing who I am talking to (freedom of assembly and association), what I am reading (respect for my private and family life, home and correspondence) or what I am saying (freedom of expression).

July 2012

Keith Edkins

1.3 This submission relates to technical considerations regarding communications over the internet. (Let other pens dwell on cost and privacy.) Sections 2 to 4 of this submission relate to telecommunications operators providing telecommunication systems. Sections 5 and 6 relate to the provision of services, and section 7 to authorised disclosure and the Request Filter. Finally in section 8 I refer to the committee's questions 11, 13, 24 & 25 and proffer my own answers.

1.4 Some of my comments are phrased in terms that implementing all the requirements which are theoretically provided for by the Bill would place disproportionate burdens on persons and companies. If it is not envisaged that certain theoretical requirements would ever be implemented by order, these comments may alternatively be read to indicate that the non-implementation leaves gaps in coverage which individuals or organisations could exploit to circumvent the intentions of the Bill.

2. Domestic Computer Systems, and General Observations
2.1 In general, it appears to me that the provisions in the Draft Bill relating to computer communications are too deeply rooted in an assumption that computer usage is much like landline telephone usage. Under this model, the computer user sits at home in front of a computer connected by cable or fibre-optics to a respectable British telecommunications operator, who is entirely responsible for his internet and e-mail communications and therefore able to separate the data from the content. He has signed a written contract with his telecommunications operator (which I shall sometimes abbreviate as TO), who therefore "knows where he lives".

2.2 Even in this simple case there are uncertainties in the Bill. The Explanatory Introduction states that the Bill will not "require the collection of all internet data" but it is unclear what this means, and the Bill does not clarify. Does it require the collection of all internet traffic data, viz. the address of every web page visited, but not the contents of the pages? Or will it require only one record for each domain (as "www.official-documents.gov.uk") visited within some time period, perhaps with a count of how many pages were accessed? I assume this will be clarified in the section 1 orders, but it is regrettable that it is not possible to comment on it at this stage. I will, for now, point out that many web pages contain advertisements, for it is the advertising revenue which funds "free" web content. A sample page on The Independent newspaper's web site, for example, invoked images and other content from no less than 15 domains, and a telecommunications operator is unlikely to be able to distinguish this additional traffic from that which the user consciously initiated. It would seem that, whatever the level of communications data intended to be held, the amount of it that would be generated is considerably more than might at first sight be expected, and over 90% of it may be irrelevant to the user's intended activity.

2.3 It is likely that the user will be connected to the internet through a domestic Router or Hub device which also provides connectivity for other members of his household, including wireless connectivity to other rooms. Is a householder who operates such a device regarded as a "telecommunications operator" with regard to other members of the household? - it would seem that he satisfies the definition of "controlling or providing a telecommunication system". Is a gentleman to be required to store communications data in relation to computer usage by his children, his wife, or his servants? It is probably not the intention that a section 1 order would be made or a notice issued in an instance such as this; but suppose the "household" is a college, or an entire apartment block, connected to the internet by fairly sophisticated routing equipment – would it be required that the operators of this equipment record communications data, over and above those records kept by the external telecommunications operator, in order to determine which communications data relates to which individual computer user?

2.4 If a company (such as BT Retail) provides a full internet service for some customers and physical connection to third party internet suppliers for other customers, can orders made under the Bill be so phrased as to place different responsibilities on it with regard to the two classes of customer? And if, for

example, BT Retail is in turn buying system or service capacity from BT Wholesale, are they both TOs, and if so can orders be so phrased as to avoid compelling double collection of communications data?

2.5 Will all notices made under section 1(2)(b) be published; if not will the existence and contents of notices be obtainable from the Secretary of State under Freedom of Information legislation? Can an order impose requirements or restrictions directly, without recourse to a notice, as the wording of sections 1(2)(b) and 4(1)(a)(ii) appears to allow but for which 8(1)(b) does not impose a duty of compliance? Can a notice ever be cancelled?

2.6 How is the Secretary of State to identify persons who are telecommunications operators who need to be made the subject of an order and a notice? There is no requirement on persons who think they might be regarded as TOs to proactively declare themselves.

2.7 In section 28 "person" includes "any association or combination of persons", while in section 7(1) a notice of the Secretary of State must "specify the person to whom it is given". How shall the Secretary of State specify an association or combination of persons which is not an organisation with a recognised corporate name? If this is to be done by naming severally all the individuals associated or combined, would the notice be void for inaccuracy, or lapse upon any change in the association or combination? Further, what constitutes "publication" in 7(1)(c)? – it is neither defined here nor in the Interpretation Act 1978. Are we to suppose that the London Gazette is normal reading matter for telecommunications operators? "Writing" is defined (in the Interpretation Act) as including a mechanically produced visible forms of words. Does this mean it is impossible to serve a notice by electronic communication, or on a blind telecommunications operator? (Other sections of the Bill have the option of "in a form which produces a record of it having been given".)

2.8 Will telecommunications operators be permitted to notify their customers as to what, if any, communications data they are holding?

3. Public Wi-Fi Connections

3.1 The simple domestic model described in 2.1 above is not the only way in which our computer user can connect to the internet. He can take his laptop computer to a location offering Wi-Fi connectivity. Such Wi-Fi "hotspots" may be found, inter alia, in cafés, on trains and long-distance coaches, and in hotels, and at present may or may not involve payment or registration. Connection to the internet may be through two connected systems, one being provided by the location and one run by a telecommunications operator contracted by the location.

3.2 Is the operator of a Wi-Fi hotspot (café, train operating company, etc.) to be regarded as a "telecommunications operator"? Will he be required to obtain personal identification before allowing computer users to connect to the internet via his system (which he may not need to do for business reasons), and to retain this information; or at least to record some unique identifier of the computer, such as its Media Access Control (MAC) address? Alternatively, if the hotspot is connected to the internet through a separate telecommunications operator, will that TO be required to obtain and retain user or computer information additional to that required when providing service to a domestic user, for the purpose of identifying the individual who used the systems?

4. Public Computers

4.1 A person may make use of a computer which is not his own, but is provided as a public or commercial service. Public libraries are a typical location where such computers may be found, as are Internet Cafés.

4.2 Is the operator of access computers (library authority, Internet Café, etc.) to be regarded as a "telecommunications operator"? Will that operator be expected to obtain personal identification, as asked in 3.2 above? Would schools allowing pupils to use computers be required to keep data on this use? Would a similar requirement extend to employers providing computers for the use of their employees – would this depend on whether or not the employer permits a degree of private use of the computers?
5. Webmail services, and International considerations

5.1 Moving on from the systems to the services aspect of telecommunications provision, the computer user may choose not to use the email service of the company providing his internet connection, but instead to use a web-based email service such as the popular one provided by Google Mail, currently branded as Gmail.

5.2 (Digression) Since Google is based in Mountain View, California, USA, this is a convenient moment for some remarks on international aspects of the Draft Bill. Section 33(4) states that "this Act extends to England and Wales, Scotland and Northern Ireland" (that is, the entire United Kingdom). This is standard phraseology for an Act of Parliament, and is overridden in the Draft Bill only by the definition in section 28 of a telecommunication system existing "in the United Kingdom or elsewhere"; but fails to address the fact that we are dealing with a World Wide Web. For example, again in the definition section 28, "communication" includes "signals serving either for the impartation of anything between persons, between a person and a thing or between things". Are we then to read this as meaning impartation between two persons or things both of whom are in the United Kingdom? It seems very unlikely that this is actually the intention. Is it, then, supposed to mean impartation between two persons or things at least one of whom is in the United Kingdom? Possibly, although this would seem to be the most strained reading possible of section 28, and a difficult objective for a TO to achieve. It would seem that once a TO is made subject to a notice of the Secretary of State, they can only practically obey it by retaining all communications data which comes their way, through any part of their telecommunication system. If the lawfulness of this, possibly excessive, retention is questioned in other jurisdictions, they must argue that this is conduct in pursuance of the requirement of which they have been notified, under section 8(3)(b). Further, sections 5 & 6 define requirements with regard to the safeguarding and the timely destruction of communications data held in accordance with the Bill; however it would appear that these clauses would not be contravened by data disclosure or overlong retention occurring outside the United Kingdom, particularly if the data was initially collected outside the UK.

5.3 As further digressions, with regards to section 5 (and perhaps 6), should not the Bill provide that the Secretary of State may by Order permit that communications data held to satisfy UK legislation may also be retained and used to satisfy specified parallel, suitably safeguarded, legislation of other nations (to avoid the necessity of TOs having to retain a separate copy of their communications data for each nation they operate in)? Further, with regards to section 8(1)(a) as it bears on section 5, is an application for injunctive relief really an effective means of enforcing a provision (viz. prohibition of disclosure) where the breach of the provision will only become apparent to the Secretary of State after the breach, and any ensuing damage, has already occurred? With regard to the definition in section 28 of a telecommunication system existing "wholly or partly in the United Kingdom or elsewhere", this appears to include the case "wholly elsewhere" – is that really the intention or should the "or elsewhere" be removed?

5.4 Returning to webmail, is an overseas company, such as Google in respect of Gmail, to be regarded as a telecommunications operator on whom a notice can be served under section 1(2)(b)? In the light of section 33(4) I would argue not, even by the Bill's own phrasing, let alone the practical limits of the powers of our Parliament. I contend that in section 28 "telecommunications operator" means a person in the United Kingdom (regardless of where their system exists), and that "person" includes an organisation in the United Kingdom; and that in section 7(1)(c) the notice of the Secretary of State must be given in the United Kingdom. Further that even if a notice were considered served, under section 8(2) the duty is only enforceable by civil proceedings in the United Kingdom, where the Courts would have trouble establishing jurisdiction over a company based overseas. In section 9(3)(d) an authorised officer could only issue a notice in the United Kingdom to require a telecommunications operator to disclose data. Sections 5 and 6

on limits of access and data destruction would not apply at all to a TO outside the United Kingdom. Numerous other limitations could be evinced; for the moment I will conclude by asserting that under section 26(6) cost contribution payments would be eligible to be made out of money provided by Parliament only when paid to TOs in the United Kingdom.

5.5 In the case of a UK based webmail operator on whom a notice could be served, is section 1(2)(a)(i) expected to be used to require such operator to obtain a core set of "Subscriber data" which he may not require for his business purposes, such as real name, address and perhaps date of birth of the user? At present, as an example, the sign-up for Gmail requests only name and date of birth, and it seems no attempt is made to verify even these. It is therefore extremely easy to obtain multiple email accounts, or accounts in bogus names, from such companies, as Explanatory Note 73 points out (and registrations for many other services are only "checked" by requiring a response to an email, which is really no check at all). Would the operator be required to take steps to validate the subscriber data, e.g. by demanding acknowledgment of a postal communication sent to the purported address (which, quite aside from its ludicrous low-tech nature and delay wouldn't actually prove the name)? If the operator is required to obtain such data, would he then be required to attempt to keep the address up to date, given that many computer users will change address quite often? Would he be required to obtain this data retrospectively from users who signed up before the passage of the Bill into an Act? It seems likely that imposing a more onerous sign-up procedure on TOs subject to notice than that used by other operators would drive users to choose one of the other operators for mere convenience, even if they have no active reason to conceal their identities.

5.6 Does the definition of telecommunications operators extend to persons for whom provision of a telecommunications service is incidental to their principal activity? What I have in mind is collaborative projects which provide a means for collaborators to contact one another without publicly divulging email addresses (and thereby exposing them to the activity of "spammers"). I myself sometimes receive email through three such projects: Geograph Britain and Ireland, Project Gutenberg Distributed Proofreaders, and Open Street Mapping, to which I contribute. It is of no importance to the collaborators whether these are based overseas (PGDP is based in New Jersey) or in the UK (as the other two are). Registration for these projects typically only requires one to give a name (which isn't validated) and an email address (which as we have said before can easily be obtained without validation). As far as the email stage of the communication goes, the projects are indeed acting as telecommunications operators, but in the email header the sender appears to be the project, not the originating user, whose (purported) name appears only as content of the email. To obtain subscriber data (for what it is worth) it would be necessary to capture information at an earlier stage in the process, at the point where a web conversation is used to generate an email.

6. Social Media

6.1 The space of this submission is not going to permit me to address comprehensively the question of messages sent through modern social media systems, which do not utilise email at all. I will merely make some observations with regards to traffic data and Twitter, the system with which I am most familiar (ignoring for the moment the complication that Twitter is based in San Francisco).

6.2 Twitter messages ("tweets") can reach recipients in at least 3 ways. The "classic" method is that a tweet is not explicitly addressed, but is routed to those other users who are "following" the tweeter. The list of followers can be extremely long for a popular account: the official account for singer Adele has over 8 million followers (this number appears to be increasing by some 15-20 per minute and will therefore be approaching 9 million by the closure date for submissions to your Committee. I believe this is the greatest number of followers for any British person, and that many of the follow links are automatically generated rather than deliberately lodged by the followers.) Can the definition of Traffic Data "logically associated with a communication" be stretched to cover this follower list? Well, perhaps, although I would say it is logically associated with the account rather than the message. In any case there is the question of the practicality of storing the sheer volume; because as each person's list of followers may change between

successive tweets, the current list of followers will have to be stored separately for each tweet. It seems quite possible for the communications data associated with a tweet to be a million times larger than the tweet contents! And in any case, Twitter do not hold validated subscriber data, only a purported name or pseudonym, and an email address which may have been created for a bogus name, for each Twitter account.

6.3 The second method is for a tweet to be explicitly addressed to another user by including their user tag in the message, as "@keithedkins" (in which case the tweet will also be seen by your followers; although if you reply to an incoming tweet the reply is only seen by those of your followers who also follow the sender. Are you still with me?). This tag no doubt qualifies as "Traffic data", being information identifying the recipient comprised in the communication, and Twitter must have to extract it for operational purposes, so presumably would be able to retain it. Such extraction would however conflict with the statement in the Explanatory Introduction (and variants to the same effect in the explanations but not so clear-cut in the Bill) that "communications data is very different from communications content", for such a tag is both data and content. A popular form of tweet is a recommendation of accounts worth following, which consists almost entirely of @ tags, and therefore the traffic data required to be stored would comprise almost the entire content of the message.

6.4 Thirdly, tweets can be retrieved by users to whom they are not directly addressed, and who are not following the sender, by searching on the contents. The sender may facilitate this by including a "hash tag", thus "#TellDaveEverything" - although with the current Twitter software any word or words in the tweet may be searched for. The use of hash tags enables spontaneously formed interest groups to communicate in a manner which escapes the clutches of the Draft Bill, as the receipt of messages is entirely based on content which could not plausibly be regarded as traffic data.

6.5 Other ways of communicating without email are too numerous for me even to list fully, let alone consider in detail. Amongst them are other social media sites such as Facebook and LinkedIn, discussion forums, "have your say" boxes on news sites, weblogs or "blogs" which allow responses to be posted, direct communications with websites such as e-banking and e-commerce, and collaboratively edited sites such as Wikipedia. A frequent feature in such systems is that the distinction between communications data and communications content is obscure, or that communications are available to be read by persons not connected to the message by communications data in any way.

7. Disclosure & the Request Filter

7.1 I will now make some observations on sections 14-16 regarding Request Filtering, with some comments on authorised disclosure in general. As a lead-in, section 9(1)(b)(ii), relating to the obtaining of communications data for the purposes of testing or developing systems, while clearly very necessary, appears to be something of an afterthought - this purpose is not followed through in section 9(6). Is judicial approval under section 11 required for a local authority to obtain data with which to develop or test its systems? Does 9(5)(b), which forbids the disclosure of Part 2 data to any person other than an authorised officer, permit it to be disclosed to the system programmers for testing purposes, given that these may be employed by external contractors and even based overseas? A parallel provision 16(5)(a) regarding testing of systems used for filtering would appear to require the Secretary of State to obtain operational communications data for the purpose of testing. This purpose is followed through in 16(2)(b) and 16(3), although somewhat cumbersomely requiring every individual who may "read, obtain or process" the data to be authorised by the Secretary of State; but there does not appear to be any defined procedure for the Secretary of State to obtain this data, on her own behalf, by some form of notice which falls short of being an authorisation.

7.2 The Explanatory Notes (84) appear to envisage the operation of the Request Filter, potentially correlating several streams of raw data to produce the limited data requested by the designated senior officer a public authority, as a purely automated process. This strikes me as wholly unrealistic. I would have expected each investigation for which recourse is needed to the Request Filter to be unique in character and need to be undertaken in an interactive manner in which sentient human beings attempt data extractions,

view the results, and refine their attempts accordingly (frankly, I doubt whether it can be made to work at all, but I will leave others to discuss this). I would expect these human operators to need a mixture of detective skills (such as one might hope to find in the very police & security forces which the Request Filter is serving to keep at arm's length from the data) and database manipulation skills (which would most likely be found in external contractors); and indeed section 16(1)(a) provides for the Secretary of State to authorise individuals to carry out these activities. I wonder quite who these paragons of virtue are, who can be trusted to handle data which the police and security services cannot. I also feel it is likely that when the data is delivered up to the designated senior officer concerned it will prove to be not quite what he wanted, especially if he is only able to make his requirements known through the original authorisation in writing (or other means leaving a record); and if he has then to issue an amended authorisation to tell the Filter what he really, really, wants, the interests of justice will not be well served if the basic data has already been destroyed in such a way that it can never be retrieved.

7.3 With regard to disclosure, this term does not seem to be defined in the Bill. I suggest it should be made clear that merely passing computer media from person to person containing files of communications data, in circumstances in which it cannot be reasonably anticipated that they will be read or processed by unauthorised persons, does not constitute disclosure. Such passing would include placing back-up tapes in secure depositories, and the conveyance of authorisation data on dismountable media (DVDs, say) by Royal Mail or other carriers. There probably also needs to be provision, connected to section 13(1), to provide that authorisation data must be disclosed in a convenient form, to avoid the possibility of a recalcitrant TO "disclosing" the data in the form of a truck load of paper print-out or on a million floppy disks (and then adding insult to injury by reclaiming the cost).

7.4 Explanatory note 9 states that "Communications data can be used as evidence in court". Will the Secretary of State retain expert witnesses to explain how the Request Filter works in general and how it was applied in a specific case, and what level of credence can be placed in its output? Will it not cause adverse comment in court if the Counsel for the Prosecution states that the evidence he is presenting has been "processed" and "filtered", and that moreover the original evidence has been destroyed "in such a way that it can never be retrieved"? How far back into the Request Filter process will the requirement of disclosure under the Criminal Procedure and Investigations Act 1996 extend, if at all?

8. Conclusion

8.1 Finally I will proffer answers to four of the Committee's Questions. My response to Question 11. "Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?"
"No. They are too broadly phrased to be implemented, the requirement on internet data is not even clear. Conversely, what can actually be implemented will be significantly incomplete."

8.2 My response to Question 13. "How robust are the plans to place requirements on communications service providers based overseas?"
"About as robust as a chocolate teapot."

8.3 My response to Question 24. "Are the proposals for the filtering arrangements clear, appropriate and technically feasible? "
"No; unanswerable because of the other sections of this response; probably not."

8.4 My response to Question 25. "How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?"
"As easy as obtaining an untraceable webmail account. About 2 minutes work."

July 2012

Bruce Elliot

The draft bill troubles me deeply and I do not believe that it should be passed in its current form.

The nature of the intrusion concerned with collecting and analysing communications data

I start from the observation that the collection of communications data which the bill seeks to facilitate is extremely intrusive. A comprehensive set of such data relating to a person or persons would enable the owner of the data to draw firm conclusions about:

- The sexual preferences of the people monitored and their actual practices
- The religious and political beliefs of the people monitored and their membership of political organisations
- The social contacts of the people monitored, including any extra-marital affairs
- Any actual or suspected health conditions for the people monitored

It seems quite clear that the collection of such data is a significant invasion of privacy, of similar magnitude to the searching of a private residence. If anyone is in doubt about such a statement, they might like to consider the (hopefully) hypothetical possibility that such data might fall into the hands of the less scrupulous parts of the media.

The safeguards against misuse

I accept that there are occasions, in attempting to prevent and detect great crimes, where such an invasion may be justified. It seems to me that the safeguards against abuse should be of similar strength to those against abuse of the power to search private residences. It therefore seems to me this data should only be collected under that authority of a warrant issued by a judge. It also seems to me that additional safeguards should include the following as a minimum:

There should be a requirement, except in very limited cases where public safety might be compromised, that subjects of data collection should be informed that the data has been collected on them within a period of time from the collection. After all, one cannot have one's home searched without knowing about it.

There should be a requirement for communications data collected to be deleted within a limited period unless it is being used in an active investigation and procedural safeguards that that exception is not used as a loophole

There should be a requirement on government agencies collecting communications data to publish statistics on how many people are the subject of such collection, both as a matter of principle and to reassure the public that the powers are not being misused.

I am not an expert on the ECHR but it seems to me that the spirit of the convention would require safeguards of this sort of strength, if the UK is to claim compliance.

The need to avoid inadvertently criminalising those who use communications providers outside the UK

As a separate point, it seems to me that those drafting the bill should take great care not to do so in a way which criminalises those who use communications providers outside the UK by placing obligations upon them personally to retain communications data, which in practice, the great majority of individuals will be unable to comply with.

August 2012

Equality & Human Rights Commission

Scope of this submission

1. This submission sets out the Equality and Human Rights Commission's ('the Commission's') analysis of the draft Communications Data Bill; specifically, how proposals align with equality and human rights law.

2. This relates to the Commission's statutory duty to monitor and advise on equality and human rights enactments and advise on the likely effect of a proposed change of law[141].

3. In particular, proposals for this draft bill have been assessed in relation to Article 8 of the Human Rights Act:

Article 8: Right to respect for private and family life

(1) Everyone has the right for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

4. In considering how the legislative framework for communications data should be reformed, the Commission has drawn on its research study published in 2011, 'Protecting information privacy'[142]. A summary of this is set out below.

Introduction

5. One of the most important duties of a state is to protect the security of its citizens, especially by enabling criminal justice agencies to prevent and detect crime. In extreme cases, this may engage Article 2 of the Human Rights Act: the right to life[143]. The Commission recognises that discharging this obligation while still protecting fundamental civil liberties, such as the right to privacy, presents significant difficulties in modern times.

---

[141] Equality Act 2006, section 11.

[142] 'Protecting information privacy', Raab, C. And Goold, B., Equality and Human Rights Commission 2011 http://www.equalityhumanrights.com/uploaded_files/research/rr69.pdf

[143] Article 2: Right to Life, Human Rights Act 1998

(1) Everyone's right to life shall be protected by law. No one shall be deprived of his life intentionally save in the execution of a sentence of a court following his conviction of a crime for which the penalty is provided by law.

(2) Deprivation of life shall not be regarded as inflicted in contravention of this Article when it results from the use of force which is no more than absolutely necessary- (a) in defence of any person from unlawful violence;

(b) in order to effect a lawful arrest or to prevent the escape of a person lawfully detained;

(c) in action lawfully taken for the purpose of quelling a riot or insurrection.

6. Technological changes, particularly over the last decade, have created new problems in gathering intelligence to prevent and detect crime. People are communicating in an increasing variety of new ways and in greater numbers. Data generated through electronic communications is already vast and will continue to grow.

7. Developments in electronic communications have also altered public perceptions of what is or is not in the private domain. The concept of information privacy is struggling to evolve in line with the pace of technological advances. This draft bill provides an opportunity to address this and to re-consider and reach consensus on what information privacy means.

8. Most will agree the current legislation, particularly Regulation of Investigatory Powers Act 2000 (RIPA), has become outdated, so reform is required to modernise the law, but there are other good reasons to change the law too.

9. Devising a workable regime that can plug the intelligence capability gap without creating a state surveillance regime amounting to a snoopers' charter (by default) is the difficult task that the government and legislators face.

10. The human rights legal framework provides the basis to find the right balance between competing considerations, such as security and privacy. The central question from a human rights perspective is whether the measures in the bill are a proportionate intrusion on the right to privacy and also other human rights that could also be engaged.

The Commission's evidence

11. In 2011, the Commission published a report on information privacy, examining threats, particularly related to the activities of the state, which have emerged in recent years144.

12. The central finding of this report was that the existing approach to the protection of information privacy in the UK is fundamentally flawed, and that there is a pressing need for widespread legislative reform in order to ensure that the rights contained in Article 8[145] are respected.

13. The report argues for the establishment of a number of key 'privacy principles' that can be used to guide future legal reforms and the development of sector-specific regulation. It identifies two principal areas of concern: the state's handling of personal data and the use of surveillance by public bodies

Key findings

14. The privacy landscape has been transformed in recent years by a series of landmark legislative reforms, including the Human Rights Act, the Data Protection Acts of 1984 and 1998, and RIPA.

---

[144] 'Protecting information privacy', Raab, C. And Goold, B., Equality and Human Rights Commission 2011 http://www.equalityhumanrights.com/uploaded_files/research/rr69.pdf

[145] Article 8: Right to respect for private and family life, Human Rights Act 1998

15. There has also been a dramatic increase in the amount of personal information held by the public sector, due to technological developments and a steady expansion of the role of the state.

16. The current system has a weak, fractured and piecemeal approach to the protection of human rights to privacy. Acts such as the DPA and RIPA are riddled with gaps and contradictions, and are also interpreted, administered and overseen by a range of separate regulators, independent tribunals, and courts. As a consequence, it has become very difficult for individuals to understand what happens to their personal information, or what they should do when that information is misused. The current system has failed to protect privacy rights in a number of cases.

17. The problem is likely to become more acute. The state's demands for personal information will continue to grow in relation to national security, law enforcement and citizens' access to public services. So far, this expansion has been accompanied by only a relatively small increase in the powers or resources available to regulatory authorities such as the Information Commissioner's Office or the various Commissioners in the field of surveillance.

18. A more comprehensive approach to privacy is needed, based on a firm commitment to implementation of Article 8 of the ECHR. This involves reforming the law and the regulatory system to create a comprehensive privacy protection regime to supersede the piecemeal inventory of measures or 'tools' implemented in a disjointed fashion by various agents. The relevant regulatory agencies need to be strengthened.

19. Law is essential: without legal specification of privacy rights, other instruments are likely to be incapable of providing the remedies that individuals may need. The law needs to be flexible enough to respond to the many and varied threats to privacy.

20. The principles written into law or underpinning it must be reflected in the specification of other instruments. These are seen as reinforcements and complements to the law and not as substitutes for, or weaker versions of, privacy laws.

21. There are many ways of protecting privacy in addition to legal provisions, including self-regulatory approaches, 'privacy-enhancing technologies', 'privacy by design', and public awareness and education. Such complementary, non-legal approaches to the protection of information privacy have an important part to play in upholding information privacy rights.

Recommendations

22. This report makes four main recommendations:

23. A clear set of 'privacy principles' should be developed based on the HRA provisions and used as the basis for future legislation, and to guide the decisions of regulators and government agencies concerned with information privacy and data collection in different contexts.

24. Existing legislation that touches on privacy should be reformed to ensure that it is consistent with the privacy principles recommended earlier. At minimum, such reform should consolidate and improve the existing RIPA and data protection regimes in relation to information privacy and surveillance.

25. Greater regulatory coherence should be promoted. There should be an effort to rationalise and consolidate the current approach to the regulation of surveillance and data collection in the UK, with particular attention paid to the relationship between the various statutory Commissioners responsible for protecting information privacy.

26. Improved technological, organisational, and other means of protection should play an integral part in information privacy protection. The development and use of technological and non-legal solutions to the problem of information privacy protection should be encouraged by government, and more resources devoted to public education and awareness around privacy.

27. The right to privacy is at risk of being eroded by the growing demand for information by government and the private sector. Unless we start to reform the law and build a regulatory system capable of protecting information privacy, we may soon find that it is a thing of the past.

The Commission's analysis

28. Responding to the joint committee's call for evidence, the Commission will set out an analysis of the human rights issues pertaining to the Draft Communications Data Bill, based on our expert perspective as a United Nations accredited 'A-status' National Human Rights Institution (NHRI).

29. In summary, the proposals in the draft bill to collect and store all forms of electronic communications in the UK for 12 months - which some public authorities can then access, based on a number of broadly defined purposes - appear to be too vague and will interfere with the right to privacy. Consequently, the measures will need to be clearly justified and thoroughly scrutinised. Currently, based on the information presented, our analysis is that a cogent and compelling case for the proposed measures has not been made.

30. Everyone concerned about their security wishes to see the police given justifiable powers to investigate crimes. However, since the nature and extent of the problems the police have experienced resulting from the intelligence capability gap are not known, it is difficult to answer questions relevant to assessing the proportionality of the measures. The Commission would advise that it may be useful for the joint committee to be presented with further evidence, from the Home Office and/or the relevant public authorities who would like to have these powers, to enable better consideration of the effectiveness of the proposed measures and investigation of alternatives.

31. It is clear that sensitive information concerning the reasons for the diminishing intelligence capability gap cannot be disclosed publicly because this could compromise existing crime prevention and investigation capabilities. Nevertheless, the important democratic task of parliamentary legislative scrutiny must be properly supported by the government and relevant public authorities in relation to this bill.

32. The Commission's analysis would further suggest RIPA is unlikely to be the best vehicle for the new legislation. The Commission's analysis of RIPA and the right to privacy are set out fully in the

research report 'Protecting information privacy'[146]. This would suggest a better starting point than RIPA for the proposals is required.

33. Despite assurances from the government and the police, valid concerns with human rights implications still remain concerning:

- what 'communications data' actually is and whether content can really be separated,
- the breadth of purposes for which data is to be collected and stored,
- the number of public authorities who will have access to such data, and
- the nature and quality of safeguards to prevent misuse and protect important individual rights, including the right to privacy.

34. The Commission's analysis would suggest substantial improvements to the draft bill can be made in these areas. Otherwise, there are significant risks that the measures in the draft bill could compromise human rights safeguards and result in greater opportunities for hacking, identifying whistleblowers, compromising the work of investigative journalists and intruding on the lawyer/client relationship. Consequently, we believe greater scrutiny of the measures and improved safeguards are required.

35. For most public authorities, apart from local authorities, the authorisation process to access communications data is dependent only on internal decision-makers. The present authorisation system is perceived to lack independence and it is probably not the best process to balance and safeguard individual rights.

36. External oversight and regulation in this area is currently covered by a number of bodies, including the Information Commissioner, the Interception of Communications Commissioner and the Investigatory Powers Tribunal. Concerns about the complexity and lack of effectiveness of this regime are real and need to be addressed.

37. Preventing misuse is preferable to acting after it has occurred. Effective regulation may not be possible after the event, if undertaken by a regulator responsible for probing upwards of half a million data access requests on a 'case by case' basis. This is not a sufficient safeguard in relation to the proposals contained in the draft bill, and significant improvements are needed in this regard.

38. Lack of knowledge about data being accessed hinders individual rights to seek redress through regulators or courts and tribunals. Again, the Commission's analysis suggests reliance on this current system is not a sufficient safeguard in relation to the proposals contained in the draft bill. Significant improvements are also needed in this regard.

39. Finally, a lot of the detail in relation to the draft bill is left to the Secretary of State to devise through delegated order-making powers. Notwithstanding the fact that Parliament has a role in authorising these orders, the Commission would suggest it is preferable to have as much detail on the face of the draft bill as possible, rather than in separate orders. Ultimately, this increases democratic scrutiny, aids understanding and reduces complexity for all concerned.

---

[146] 'Protecting information privacy', Raab, C. And Goold, B., Equality and Human Rights Commission 2011 http://www.equalityhumanrights.com/uploaded_files/research/rr69.pdf

Improved safeguards

40. In this submission, the Commission has set out its analysis of how the draft Communications Data Bill aligns with human rights legislation, drawing on the findings of its research report, 'Protecting information privacy'[147]. Based on this, the following improvements may be necessary and proportionate to improve the draft bill and thereby strengthen compliance with the requirements of the Human Rights Act 1998:

41. It is positive that a commitment has been made to incorporate 'Privacy by design' and 'Privacy enhancing technology' into the technology that will be constructed. However, as a starting point, the draft bill requires clear principles - perhaps based on those in Schedule 1 of the Data Protection Act 1998.

42. The legislation needs to be much clearer and less complex, so everyone can understand their rights and responsibilities without having to resort to lawyers and/or to courts and tribunals.

43. What amounts to data content should be defined on the face of the draft bill, as should those bodies permitted to access data. The purposes should be restricted to those permitted under the HRA. Clause 5(1)(b) should state what in fact is already authorised by law.

44. Independent authorisation of data access requests (by the judiciary or other independent body) should be the norm, especially for more intrusive information beyond basic subscriber details. This should complement internal approval processes. A workable system is required for urgent requests, perhaps with retrospective scrutiny.

45. The threshold to access data should be set at a high level in the legislation to prevent trivial and other disproportionate requests. Clause 9(6) is too broad in permitting data requests for a number of reasons that do not necessarily fall within limitations set out in Article 8 HRA.

46. There is a lack of transparency in the present proposals in terms notifying innocent people at an appropriate point in time that their data has been accessed and destroyed. Individuals (as well as regulators) should receive notification at an appropriate point in time, subject to other considerations - for example, not compromising an ongoing investigation. This will act as a deterrent against misuse and aid accountability.

---

[147] Ibid.

47. A legal requirement to have a system comprehensively recording what data has been accessed, by whom, when, for what purpose(s) and when the data has been destroyed should also be required on the face of the draft bill.

48. Sanctions for misuse have to be set at a level that provides a real deterrent. Consideration should be given to imposing criminal sanctions, including breaches of Section 55 of the Data Protection Act 1998 and breaches of a relevant code of practice.

49. The Secretary of State's delegated powers under the bill should be considerably reduced; further changes including additional powers, should require primary legislation that can be thoroughly debated and scrutinised by Parliament.

50. A legal requirement to monitor, review and report on the operation of the legislation should be placed not only on regulators, but also on government and relevant public authorities.

August 2012

The foundation for Information Policy Research

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

We would like to make the following comments and recommendations to the Joint Committee on the draft Communications Data Bill. A member of our Advisory Council, Professor Peter Sommer, has submitted a response discussing technical details, which we will not repeat here; in this response we focus on the strategic aspects.

1. A state that can watch anybody, or a state that can watch everybody?

In democratic countries we have historically limited our capacity for government surveillance in various ways, while despots try to watch the whole population. In the past this may have been partly a matter of priorities; citizens who can vote opt for schools and hospitals, not secret policemen. But as technology slashes the cost of surveillance, it might just be possible to have schools and hospitals, and watch everyone too. Should democratic governments give in to this temptation, or take a more principled position? The Bill may be the one real opportunity for this Parliament to consider this question.

Britain should remain one of the states that can watch anybody, but not everybody. We understand that BT already has the DPI capacity (installed for the purposes of interception) to monitor about 100,000 Internet subscribers. The other big ISPs presumably have as much again, and GCHQ no doubt has further capacity on backbone links. Rather than accepting the Home Office bid for a massive expansion of this already substantial capability, the Committee should instead recommend a policy of selective data preservation: communications data would be collected only for targeted individuals, such as serious criminals released on license, or on the sex offenders' register. In any case, we recommend that collection should be subject to an overall volume limit (say 100,000 subscribers) to compel the police and intelligence agencies to prioritise. It should be subject to judicial oversight.

2. Communications data only, or interception too?

In the draft bill and its testimony to the Committee, the Government has been vague about what it intends to do with the new powers. It has been much less vague in its work on the European Telecommunications Standards Institute Technical Committee on Lawful Interception (ETSI TC LI), a standards body staffed by people from intelligence agencies, telcos, ministries and switchgear suppliers, with a very strong British contingent. ETSI TC LI drew up the technical standards for government access to mobile phone location, traffic data and content, and has now decided to extend its standards to the facilities that Google, Facebook and other cloud service providers will be ordered to offer the police and the intelligence agencies. We strongly urge the Committee to study the document ETSI DTR 101 567 "Lawful Interception (LI) Cloud/Virtual Services (CLI)", which we incorporate herein by reference[148]. This makes clear that the agencies' goal is not just access to communications data, but interception too – as with the previous Government's 'Interception Modernisation Programme'.

The Communications Data Bill will give the Secretary of State the power to compel service providers to install interception equipment of the government's choice, by secret order. Although the Bill claims that it does not empower interception, nothing in it prevents its being used to direct the installation of equipment

[148] http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_LI/2012_45_Bratislava/SA3LI12_044.doc

which is then used for interception under other laws. The DPI equipment that can be used to collect traffic data can equally be used for interception; this is just a matter of its instructions.

We recommend that the Committee amend the Bill so that equipment installed under its powers cannot be used for interception. If the Home Office will not accept this, then the Committee will have at least achieved clarity about government intentions.

3. Should cloud service access be automated?

At present, cloud service providers such as Google, Yahoo and Facebook screen law enforcement access requests manually. One reason is that can be very hard to tell whether a police force or intelligence agency has jurisdiction.

Imagine that a future British minister or diplomat passes through Cairo International Airport en route to South Sudan on an official visit. She opens her laptop to check her gmail. The local intelligence service notices, and invokes its law-enforcement interface to her gmail account. Suppose that the Communications Data Bill passed in its present form, whereupon the UK compelled all cloud service providers to build an interface for access to webmail. Other countries then demanded access too; even if the providers limit access to democracies in which they have employees, it is hard to see how they can deny access to France, Italy, and Egypt.

Now consider: how much should the Mukhabarat be able to get? Only those mail items she sent, received or viewed while on Egyptian soil? Everything she got in the last 14 days? Everything she'll send and receive in the next 14 days too? All of her inbox? Her Google docs and her calendar too? The agencies will grab the lot if they can. But what is proportionate and necessary, and how can systems be built that respect jurisdiction? It is not clear to us even how to specify such systems, let alone build them.

Designing a law enforcement interface that will give automatic access but respect users' rights is made even harder by the fact that targets of investigation use cloud systems in nonstandard ways. For example, a number of terrorist groups have used webmail dead drops, where they communicate by sharing the username and password to a webmail account, and leaving messges in the drafts folder rather than sending them as formal emails. So traffic data may not really be, or mean, what it ostensibly says; indeed the agencies can redefine traffic data by describing a new modus operandi (real or imagined).

In the absence of a clear and detailed explanation of how to prevent such an interface being abused by foreign intelligence services to the detriment of the UK's critical interests, the UK should not be pushing for it to be built. (The Committee might note that CESG, which does protection, is a subsidiary of GCHQ, whose primary mission is offensive, so offence may be favoured over defence in policy advice.)

In any case, we recommend that law enforcement access to cloud services should by default involve manual scrutiny by the service provider; and to ensure that the scrutiny is careful, no new law should indemnify the provider against providing information contrary to other laws. It is quite right and proper that cloud service company executives should face litigation or even prosecution if they violate users' rights by handing over private UK information to a foreign intelligence agency (or for that matter to a newspaper or a criminal gang that bribes an employee of a government).

4. If some access is automated, what should the scope be?

What law-enforcement interfaces should be automated? Existing systems give automated access to phone records and handle tens of thousands of requests a month. This is possible because phone records are simple; the question of jurisdiction doesn't arise. Cloud services are complex, and jurisdiction is not the only factor: there are more than forty ways for two Facebook users to communicate with each other, and new mechanisms are introduced constantly. A requirement for automated eavesdropping would impair innovation, as a team developing a new feature would have to think through all the aspects of interception

including jurisdiction and liability before the feature could ship.

Complexity can also be an emergent property, and in this respect we are concerned about the draft bill's provisions on filtering. The idea is to enable an investigator to make complex queries on simple data held in multiple different systems. Suppose for example that an opposition MP, or a journalist, were leaked a sensitive policy document to which only twelve civil servants had access. At present investigating such a leak might involve interrogating the twelve suspects, or even arresting the MP. In future, an investigator would be able to query the hundreds of different CSPs saying "tell us all the people with whom these thirteen targets communicated in the last eighteen days". These contact lists would be combined at GCHQ, who might spot that official number nine phoned an academic critical of government policy, and half an hour later the academic called the MP's mobile phone. That, at least, is the theory. The filtering provisions open up the door to large-scale data mining of the Internet; what Google did for the citizen searching for stuff, the Bill will do for investigators searching for villains.

In practice there are serious obstacles. First, the individual communications service providers would have no way of assessing whether any particular request for data is proportionate, necessary or otherwise lawful, so if such requests can be made automatically to cloud service providers they would raise the issues already discussed. Second, as Professor Sommer pointed out, the boundary between traffic data and content is changing constantly, and has some hard cases. A good example is your diary. Many firms nowadays run on corporate calendaring systems, which can be a valuable resource for investigators: an FSA official investigating insider trading would love to trawl all the staff diaries of the target bank. But is this traffic or content? No doubt agencies will argue the former; but bankers may well be unrelaxed about the idea that their internal and client contacts could be traced automatically via surreptitious intelligence-service access to their corporate calendaring system. Third, The way the Bill is currently drafted, it will catch all sorts of machine-to-machine transactions such as ATMs and card transactions in shops, security webcams, wireless dorbells, insurance car tracking systems, and even set-top boxes that track what you watch; these pose further problems of content versus traffic. Finally, it's proposed that the filtering requests would include requests for content as well as traffic data, which GCHQ would filter so as to pass on only relevant traffic data to a requesting police force. So the filtering provisions of the Bill appear to authorise GCHQ to collect arbitrary data (including content) from any CSP. It's worth noting that in NSA/GCHQ terminology, "interception" is what happens when content is scrutinised by a human analyst; if it's just scraped up into a database for future use that's called "collection." The Committee should be careful about terminology!

We recommend that the filtering provisions be removed entirely from the Bill and that the definition of traffic data be made completely explicit in order to prevent mission creep.

5. Will the Bill impair competition?

If communications service providers are compelled to install enough DPI equipment to monitor all subscriber connections, this will be easier for relatively centralised CSPs such as BT than for many of its competitors. If CSPs are required to have staff with security clearances to maintain the DPI equipment, this could be difficult for small providers and impossible for most startups.

If cloud service providers are required to provide law-enforcement interfaces on the same basis as traditional telcos, they will suffer substantially higher costs because of their more complex service offerings and because of the uncertainties in jurisdiction discussed above. A legal requirement for all new communications services to be intercept-ready could impose a very high cost on startups; sensible entrepreneurs would go elsewhere. This would be even worse if any IT startup required someone with a clearance (a large number of tech startups involve foreign nationals). The Bill as proposed might be welcomed by BT, which might rebuild its network at taxpayer expense, but its effects on innovation could be severe. There must be a level playing field, so the proposal that the Home Secretary acquire the power to give secret orders to CSPs is unacceptable. We recommend that any interception requirement imposed on

firms be applied to all firms equally, and be subject to public consultation followed by a vote in Parliament.

6. Should the state be able to compel treachery?

The Bill will empower the Home Secretary to order companies or individuals to build back doors into their systems: in effect, to double-cross their customers or employers. The writer declares an interest, as one of my postdocs is a maintainer of Tor, an anonymous communication system used by citizens in countries like Iran and China to circumvent Internet censorship. If the current Bill were to become law, the Home Secretary could serve us with a secret order compelling us to modify the software to create undocumented logs and mail them to GCHQ. We would probably safeguard Tor's integrity by posting a monthly declaration under oath on our website that we have not been placed under compulsion. Should this fail to appear, our colleagues elsewhere will know that no more software from the UK should be trusted.

The impact on business of a power to compel staff to be silently disloyal might be far-reaching. A prudent US software firm might decide not to locate any developers in the UK, for example. But the implications are not restricted to software. Part 3 of the Regulation of Investigatory Powers Act permitted a Chief Constable to seize a cryptographic key; even though such notices have to be served on directors, their very existence has led at least one international bank to remove key material from the control of London staff, which in turn led to its audit function for Europe moving from London to Switzerland. Legalised treachery is bad for business, and the Bill must not enable ministers to compel it.

7. Which agency should do the watching?

For many years, much of the civil-liberties community has considered GCHQ's interception operations to be a low priority, because most of their surveillance activities were directed outside Britain and because the product was very closely held. But the world appears to be changing.

The US National Security Agency moved to internal surveillance after 9/11, turning its resources against US citizens in ways that broke US law (albeit retrospectively legalised by Congress in 2008). Now the NSA is GCHQ's mentor; it not only leads the Five Eyes intelligence-sharing agreement but spends much more than the UK, Canada, Australia and New Zealand put together. So the NSA sets doctrine and standards across allied governments for communications intelligence and information security. As the USA is the largest buyer, and the dominant player in the Wassennaar Arrangement which coordinates export controls, it also shapes the market for interception equipment. Even such minor aspects of US policy as the sponsorship of academic centres of excellence in information security have been imported into the UK.

So it is not surprising to note that the Bill will greatly expand GCHQ's domestic surveillance capabilities. But Parliament should think hard about the prospect of GCHQ transforming itself from an essentially military agency, tasked with uncontroversial jobs such as deciphering Hitler's telegrams or tapping Chairman Mao's phone, into an internal police agency with broad scope and no effective oversight. It simply has the wrong culture. The can-do approach adopted for dealing with enemies in wartime (or during the Cold War) is not right for internal use in a nation at peace and with the lowest recorded crime rates ever. A central comms data facility driven by intelligence agencies might also be of little use to the police; they would not have the security clearance to know what it contained. If the UK needs an internal technical surveillance agency it should be more like the FBI than the NSA; it must be a body that shares the police ethos and is subject to democratic accountability.

We therefore recommend that any central functions relating to the collection and processing of communications data should be under the control of the proposed new National Crime Agency, or the Metropolitan Police, or the NPIA, rather than GCHQ or the Security Service.

8. Who shall watch the watchers?

The Interception Commissioner and his colleagues have failed to win much confidence. There is a tendency

for regulators to be captured; a regulated industry usually knows much more than they do about what's going on. It should surprise no-one to see this in the interception business because of the highly technical nature of the activity.

Britain is almost alone in the world in not permitting intercept product to be used in evidence. Officials who argue that the sky would fall if policy were to change can never explain why the sky has not fallen in so many other countries such as the USA and the Netherlands. But once intercept product is usable in evidence it will be tested in the courts; this transparency will do more to prevent abuse than any regulator could. Also, as noted above and explained by Professor Sommer, the distinction between content and traffic data is becoming increasingly problematic. We therefore recommend that the law be changed to allow intercept product in evidence, and furthermore that targets of surveillance who are not prosecuted should eventually be notified of the surveillance. Sunlight is the best disinfectant.

9. The human-rights test

It is extremely doubtful that mass surveillance without warrant or even suspicion could comply with human-rights law, specifically section 8 of the European Convention on Human Rights. The Data Retention Directive was much less draconian, yet the two supreme courts that examined local implementations (in Germany and Romania) found them non-compliant. Even if the Human Rights Act were repealed, its replacement would surely reimplement ECHR so long as Britain remains in the Council of Europe. The ECHR was reflects both Europe's and Britain's deepest values.

The fact that the Bill ostensibly only facilitates access to communications data does not really mitigate the problem. Such data can rapidly disclose the most sentitive aspects of a citizen's life; communication with a psychiatrist, a minority-interest dating site or a service such as Narcotics Anonymous can be profoundly revealing. Yet, as we noted above, the Bill appears on careful study to facilitate interception as well.

We therefore recommend that the Committee commission independent legal advice on what amendments may be required to the draft Bill to ensure human-rights compliance.

Summary

We make the following recommendations:

1. Collection should be subject to an overall volume limit (say 100,000 subscribers) to compel the police and intelligence agencies to prioritise, and should be subject to judicial oversight.
2. The Committee should amend the Bill so that equipment installed under its powers cannot be used for interception.
3. Law enforcement access to cloud services should by default involve manual scrutiny by the service provider; and to ensure that the scrutiny is careful, no new law should indemnify the provider against providing information contrary to other laws.
4. The filtering provisions must be removed entirely from the Bill and the definition of traffic data made completely explicit in order to prevent mission creep.
5. Any interception requirement imposed on firms must be applied to all firms equally, and be subject to public consultation followed by a vote in Parliament.
6. The Bill must not empower ministers to compel treachery.
7. Any central functions relating to the collection and processing of communications data should be under the control of the proposed new National Crime Agency, or the Metropolitan Police, or the NPIA, rather than GCHQ or the Security Service.
8. The law should be changed to allow intercept product in evidence, and targets of surveillance who are not prosecuted should eventually be notified of the surveillance.

9. The Committee should commission independent legal advice on what amendments may be required to the draft Bill to ensure human-rights compliance.

August 2012

The Financial Services Authority

1. We welcome the opportunity to submit this memorandum to the Joint Committee on the draft Communications Data Bill. In this memorandum, we set out:

    a. the FSA's role and responsibilities, and the extent and nature of our interest in communications data;

    b. our access to communications data;

    c. our use of communications data;

    d. the specific measures we use to safeguard communications data;

    e. the impact that a warranting system would have on our ability to reduce financial crime and tackle market abuse; and

    f. the role of the Interception of Communications Commissioner's Office (IOCCO).

Executive summary

2. We welcome the draft Communications Data Bill, which would consolidate and update powers essential to our enforcement work.

3. We are alert to the sensitivities of using communications data, and have mechanisms in place to ensure that such information is used appropriately and securely.

4. We recognise that there must be a balance between the safeguards in the process to acquire communications data and the efficiency of that process. We consider that the draft Bill gets this balance right and we ask the Committee to consider carefully any possible changes to the draft Bill that would have a detrimental impact on our ability to reduce financial crime and counter market abuse.

FSA role and responsibilities

5. The FSA is the single statutory regulator for the great majority of financial services in the UK. Our powers are conferred primarily by the Financial Services and Markets Act 2000 (FSMA).

6. FSMA requires the FSA to pursue four objectives:

    a. market confidence – maintaining confidence in the UK financial system;

    b. financial stability – contributing to the protection and enhancement of stability of the UK financial system;

    c. consumer protection – securing the appropriate degree of protection for consumers; and

    d. the reduction of financial crime – reducing the extent to which it is possible for a regulated business to be used for a purpose connected with financial crime.

7. The Financial Services Bill currently going through Parliament introduces a new regulatory environment, splitting the FSA into the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA). The FSA's financial crime objective will move to the new FCA. As the Bill

stands, the FCA will have an operational objective to protect and enhance the integrity of the UK financial system. The 'integrity' of the UK financial system includes:

a. its soundness, stability and resilience;

b. its not being used for a purpose connected with financial crime;

c. its not being affected by behaviour that amounts to market abuse;

d. the orderly operation of the financial markets; and

e. the transparency of the price formation process in those markets. [Financial Services Bill, cl. 5(1)]

8. We currently have powers under the Regulation of Investigatory Powers Act to acquire communications data for the purposes of criminal investigations. Under the European Market Abuse Directive, the FSA must also have powers to obtain communications data for civil market abuse cases – these powers are currently provided under FSMA, but would be consolidated into the Communications Data Bill.

Access to communications data

9. It is of vital importance to the FSA, and going forward the FCA, that we retain our ability to access communications data.

10. We are not one of the 'core' authorities (such as police forces or HMRC) mentioned in the draft Communications Data Bill. As a non-core authority we need to be dealt with by an Order by the Secretary of State. We have no concerns about this as the Bill stands. However, if the Bill is amended to distinguish between core and non-core authorities, we would consider our substantive position to be the same as the core authorities, and would recommend appearing on the face of the Bill.

11. Our processes to safeguard communications data are practically the same as the core authorities. We would therefore have serious concerns about the impact on our ability to investigate cases as a result of any additional requirements on us.

Using communications data

12. Legislation needs to keep pace with developing technologies as we are seeing increasing sophistication by criminals seeking to evade detection. We welcome measures in the Bill that will ensure communications data is available.

13. Our use of communications data regularly supports and underpins successful criminal prosecutions. Communications data is intrinsic to our ability to investigate effectively and prosecute many of the criminal offences we deal with. It has played a key evidential role in 121 criminal enquiries since February 2009. These comprised: 96 enquiries into allegations of insider dealing contrary to s52 Criminal Justice Act 1993; 14 enquiries into allegations of unauthorised business contrary to s19 of FSMA; and 11 enquiries into allegations of market manipulation contrary to s397 FSMA. Some of these enquiries have resulted in criminal prosecutions and/or the disruption of serious financial crime and have enabled us to achieve convictions against individuals resulting in significant custodial sentences and confiscation proceedings.

14. Communications data frequently provides critical evidence in preventing, detecting and prosecuting market abuse (criminal and civil) and unauthorised business (criminal) cases. The communications data provides initial investigatory leads that enable us to identify those involved in alleged criminality

and also to evidence directly communications between suspects. Without this evidence it would be impossible to prosecute the majority of the cases we deal with.

15. Market abuse cases involving insider dealing are often referred to as an 'information crime', as the action underlying the offence is that of passing information between parties. Intrinsically the ability to demonstrate contact between parties is a key element in the evidence required to prove insider dealing has occurred. Without communications data it would be impossible to prosecute most of these offences.

16. We investigate a wide range of serious criminal offences. Recently, communications data was used in an investigation into an illegal investment scheme to successfully locate the suspects' office premises. Typically, given the criminal nature of their activity, suspects move office location every few weeks. Finding the current location of the office allowed us to apply to the Court for a search warrant and execute a search at the premises before it moved again.

Retention period

17. Inevitably, any cut-off point for retaining data means that it will not be possible to investigate some leads. We appreciate the need for balance and the proposed 12-month period for retaining communications data is proportionate in the current regulatory environment.

18. However, the retention period may need to be reviewed if a warranting system is introduced due to the anticipated delays this would cause. In these circumstances it is likely that an unacceptable amount of relevant communications data would be lost as a result of it falling outside the retention period and we would request a longer retention period to take account of this. We note, however, that even a longer retention period would not mitigate the diversion of resources and delay in investigations if a warranting system was to be introduced.

Safeguards

19. We believe our processes provide a robust level of scrutiny to communications data requests. Below we set out our procedures to ensure data is used appropriately and securely.

20. Our application process is identical to that used by Law Enforcement, SOCA, HMRC and the Intelligence Services. We use a Home Office approved application form that we supplement with additional guidance and advice to applicants about the information required to satisfy the application thresholds.

21. In accordance with IOCCO guidance, any FSA applicant requesting authorisation to access communications must be employed within a relevant area and have completed our approved training programme.

22. Our Designated Persons must be employed as a Head of Department in the Enforcement Division. No one of a lower rank is authorised to approve an application for any form of communications data.

23. The Applicant can only submit a request for authorisation to obtain communications data from a Head of Department who is not responsible for the investigation, ensuring the independence of the Designated Person.

24. Our Single Point of Contact consists of two accredited officers who are stationed in a secure area within the FSA. They are the only two FSA employees able to access the secure sites and download communications data which they do through the Government Secure Intranet. The data is downloaded

from this separate IT system and is transferred to us using government approved secure USB drives. These USB drives are kept at all times within the secure area at the FSA.

25. Applications for communications data and the resulting data are encrypted and held securely on our server. Only our two accredited officers have the necessary digital keys and passwords to access the information we hold.

Impact of a potential warranting system

26. We do not consider a warranting system to be appropriate for our obtaining communications data. The cases that we prosecute are very technical in nature. To understand the offence, explanation of the type of trading, method of trading and the nature of the financial markets is required. If we were to request a warrant for communications data then the background information in support of our application would require technical market or trading explanations. We are concerned that this will have an impact on any such application, causing delay and costs to both ourselves and Her Majesty's Court Service, reducing both the number of leads we are able to follow and the number of cases we can prosecute.

27. We currently maintain a system that is well balanced between the safeguards outlined above and an efficient system that allows us to frequently approve or refuse requests within 24 hours and maintain the pace of investigations. We currently assign the same Designated Person to deal with requests under RIPA for communications data that may arise during an investigation. This Designated Person is able to read the background of the case from the outset and is well placed to consider and deal with requests for data throughout the lifespan of the investigation. This avoids the need for numerous individuals to read the background material before determining an application, which in turn enables requests to be dealt with efficiently and effectively.

28. Even if the Court was able dedicate resources to a similar process of assigning a single judge to each investigation, we would anticipate significant delay. There are some comparisons with the arrangements we have in place to apply to a Magistrates Court to obtain search warrants for premises under the Police and Criminal Evidence Act 1984. We are often asked to give our applications in advance to the Magistrates Court so that they can be assigned to an experienced District Judge, rather than a magistrate. The judge often considers the papers in advance before our application. As a result these applications understandably take some time for the Courts to deal with.

29. Other than in exceptional circumstances, applications for communications data would not be dealt with by the courts as urgently as search warrants are. Delays would reduce the number of leads we could investigate and therefore cases we can prosecute.

30. In addition we apply for a relatively low number of search warrants annually. By comparison, in 2011 we made 2,325 requests for communications data. If we continue reducing financial crime and countering market abuse effectively, we will need to make multiple applications to Court every working day, with a detrimental effect on both FSA and Court resources.

Role of the Interception of Communications Commissioner's Office (IOCCO)

31. We believe IOCCO plays an important role providing a complete independent review of our procedures.

32. When IOCCO attend our office they log-in to our system as our Single Point of Contact. This gives them unfettered access to all our computer folders and they have complete access to every application made by us. They test at random and dip sample our cases, giving them an open and accurate ability to review our applications.

33. We have received consistently positive reports from IOCCO following inspections. IOCCO stated in its latest report '*the FSA emerged well from this inspection. The inspector was satisfied that the public authority is acquiring communications data lawfully and for a correct statutory purpose. Overall the public authority has a good level of compliance with the Act and CoP. A very good standard of application is being produced and the principles of necessity, proportionality and collateral intrusion are well justified.*'

34. These reports from IOCCO are indicative of the fact that we take our obligations in relation to communication data very seriously.

August 2012

Mike Gerbrais

GENERAL OBSERVATIONS

Clarity and specificity are more essential than usual in the present draft. Laws originally drafted because of overriding need in one area are at times abused or misused in others in ways the original drafters had not anticipated.

Before commenting on this draft, it is instructive to consider the Regulatory of Investigatory Powers. There is nothing inherently questionable about having close to 700 public bodies added to the RIPA, until put in the context that the original drafters listed just 32 and may have wished in retrospect to control the additions more tightly. There is nothing wrong with legislative power to monitor for terrorism, until put in the context of councils using powers granted for terrorism crises, to ticket for dog fouling. It is also sobering to consider the disproportionate uses that good intentions can leave - in the past this has seen laws in the Criminal Justice Act 2003 intended to reduce extremely violent photographs used to prosecute a cartoon of Tony the Tiger, anti-terrorism laws used for littering, and an autistic citizen under extradition. In the United States and the 2011 SOPA markup hearing, legislators proposed measures of great harm to the internet, referring to world-class experts in security derisively as “nerds”. The risk is present.

Technology and surveillance laws perhaps beyond all others, have the scope to be abused this way. Safeguards need to be correspondingly more rigorous than usual. Scrutiny, good definitions, and clarity of unintended or uncontrolled uses, can ensure that future SI's and usage remains broadly as parliament planned.

While the goal is laudable, I fear for the actual outcome. Key clauses and definitions in this law are so open as to allow (almost) anything to be applied to (almost) anyone. In a few years determined criminals will be more data literate; serious criminals will cover their tracks even in data communications while a bill like the present will be used for crimes which are trivial, on the grounds the power exists and the matters are crimes, however small – regardless of the risk to societal structure, privacy and “chilling” of free speech.

Law-makers are deeply urged to consider the scope for good intentions to be abused, lessons of history, to not be complacent or dismissive of the fears and risks inherent in a bill like this, and apply the greatest degree of caution and rigour, if indeed they decide to press ahead.

We can live with occasional crime, however severe. We cannot live well with loss of the right to speak and associate freely that such draconian broad and open controls define for us.

THE DRAFT

(1)
The Sec of State may by order (after consultation) "impose requirements or restrictions on telecommunications operators or other persons" What “other persons”? As it stands, this allows imposition on any business, type of organisation, or natural person not being telecommunications operators. There is only obligation to “consult”.

> **Severity:** Huge potential for concern.
> **Action:** Delete [other persons], or add [upon some form of parliamentary consent]. If a threat is so serious to add an entire class of people, or persons who are in no way “telecoms operators”, it is serious enough that parliamentary control is better.

"Requirements" is very open. This can mandate that industry and individuals adopt measures that are outdated, deemed less secure or competitive, or deter cutting edge “best practices” beyond the norm such as

advanced data security measures, restrict storage locations or backups, prevent upgrades, and generally disrupt British business as a world leader. Data security moves very fast and operators may need to migrate or update faster than they can obtain consent to update. It is generally better to specify an interface or standard by creating where needed a mandatory specification to be met or exceeded, then leaving the rest to the open market.

(3)
"A telecommunications operator who holds communications data by virtue of this Part must—(a) secure that the data is of the same quality and subject to the same security and protection as the data on any system from which it is derived" – data is communicated from and via many systems. How on earth does the drafter contemplate an operator will know what system data is "derived" from, much less be able to ensure the same security and quality? This is a requirement that cannot reasonably be imposed as drafted. **Action –** Perhaps what is meant: "… who holds communications data must secure that the data held by them, or on their behalf, is of the same quality and subject to the same security and protection as any system under their control from which it was derived"?

> **QUESTION:** Is there a duty to retain control, or to not remove data outside the UK? It is not beyond contemplation that a company may change, be acquired, have systems moved overseas by a parent, or outsource to a third party (not a telecoms operator) so that in some circumstances data may cease to be under their practical control. *"Must secure that the data remains under their control and (etc)"?*

(5)
"The operator must put in place adequate security systems (including management checks and controls) governing access to the data in order to protect against any disclosure"
This is routinely done poorly in most industries. Even major bodies such as the Ministry of Defence, Department of Work and Pensions, Google, Microsoft, Sony, have had serious data theft or loss. Medium telecoms operators will not meet or exceed the security capabilities of multi-billion organisations. This clause is toothless. In any loss of data it is almost impossible to show culpability of a responsible individual unless actions can be measured against a clear statement of required criteria. **ACTION –** "A telecoms operator shall designate one or more directors or equivalent to be each responsible for ensuring compliance with this requirement".

It is easy - and correct - to claim "no system is perfect". The single best practical control is not technical, but a strict duty of vigilance, by which the responsible officer is required to at least identify weaknesses. There is no justification for lack of vigilance, and a duty to be watchful as well as secure creates the single best defence of any expectation of security. **ACTION –** Individual offences related to failure to either (i) take necessary steps for the identification of weaknesses, or (ii) maintain systems in a secure state.

(7)
"Board have to "consider" any issues and the Sec of State "consider" likewise."
Can we have some specific grounds or criteria stated for appeal? Otherwise this is no safeguard and toothless.

(9)
THIS SECTION HAS SERIOUS FLAWS – PERHAPS THE MOST SEVERE IN ANY SECTION
This section as it stands is the whole "terrorism law used for dog fouling" problem all over. (a) There is no "de minimis" level of infraction on any category, although nobody would expect this to be used for dog fouling. (b) Categories are so vague as to be "whatever one wishes them to mean". (c) The controls over proportionality and correct use are very weakly drafted. (d) There is no allowance for the possibility that an authorised person may not know the best way to achieve their purpose or that the operator may have an equally valid preference that reduces cost or damage. (e) The Secretary of State may authorise any person and any conduct without restriction or reasonableness. (f) There is no obligation to state the purpose to the

operator, even in terms such as "to obtain the following data…" or "data pertaining to…" so an operator cannot know if the authorisation is abused or more is done than should be. (g) If a wide range of actions are authorised in some matter out of abundance of caution (as may be expected) there is no control that an authorised person shall minimise the data or activities undertaken or look at the minimum data compatible with the purpose, if they discover that less invasiveness than authorised will suffice. (h) There is no test of reasonableness in any matter.

For example

> **De minimis:** An additional clause to be added, that for each category of purpose states a level of severity or specific actions that is as "de minimis" for that category, in order to ring-fence less severe matters or actions that are generally not intended to become "purposes". For example for crime, one might specify a crime capable of imprisonment for a certain time. **Action –** Add to (9)(6) "…subject in each case to a de minimis requirement set out [by SI or similar]" and append to (9)(7) "...and their de minimis requirements"
>
> **Stronger safeguard on conduct:** (9)(1)(c) and (9)(2) "conduct authorised is proportionate to what is sought to be achieved" are unwieldy because they first state the authorisation is proportionate, then appear to reverse that by authorising "any conduct" unlimited. Also what may be necessary is often less than what is (out of abundance of caution) authorised. Since (9)(2) can only apply if (9)(1)(c) has already applied, amend (9)(2) to read "to engage in conduct that is (i) not in excess of the authorised conduct and (ii) no more than that reasonably required in order to ensure the achievement of [or procure] the purpose"
>
> **Absolute course of action:** It may be that an "authorised person" is not sufficiently (or falsely believes themselves to be) knowledgeable about the system, data or implications of the conduct concerned, or there are more than one acceptable way to procure the purpose and the operator considers one way to be preferable to, or less disruptive than, another. There is no safeguard.
>
> By way of example - it may be that in some circumstances, an authorised course of conduct would (for technical reasons unappreciated or dismissed by the authorised person) cause risk of some loss or damage, of needless operator hardship, for example if their proposed activity would fail due to a backup or cause data inconsistency. An authorised person has absolute authority to do an action themselves, or require its doing by another person, and may press on. **Action** - This section should contemplate technical issues known to the operator that may cause damage or disruption, and take steps to minimise them. They may have significance to the authoriser, the operator, or both.
>
> **Valid purposes:** These are unreasonably wide. To cite a few:
> NATIONAL SECURITY. Putin and the recent "show trial"? China?
> DETECTION OF CRIME. All crime? Dog fouling?
> INTERESTS OF ECONOMIC WELLBEING. Any demand coerced by any substantial overseas power? If the United States playing "hard ball" says they will (hypothetically) only allow favourable terms on a trade matter if we agree in principle to pass some kinds of communications data to them, is that what is meant? Are there any safeguards or strong restrictions related to data being passed overseas?
> PUBLIC SAFETY. Dog fouling?
> ANY TAX. Any amount to any department of any kind?

(10)
Statement of purpose:
There is no requirement to state the purpose. The purpose of access is to obtain data pertaining to a matter, or of a specific type, or of specific currency, recency or the like. In some cases the purpose may be secret, but the nature of data sought will often not be, as the operator's co-operation is required. A given conduct may be used in any manner, reasonably or otherwise. If an authorisation states the purpose, then it becomes

much easier to prevent, identify and address conduct not well related to the purpose or used for other purposes.

(A summary of applicable law approved by the Secretary of State should be required to be included or annexed with any authorisation, for reference of the person executing the authorisation, and person(s) presented with it)

(13)
Reasonableness clause: the stated duty is to "comply", not to "reasonably" comply. If compliance would cause loss or damage, then this could be a problem.
(13)(3) append:

> "...or may cause disproportionate damage (including loss or risk of loss of data), disruption, or cost."
> "Such an operator or person is required instead to provide good cause and to use all reasonable efforts to procure the achievement of the purpose by another means as may be agreed by the authorised person."

(14)
THIS SECTION ALSO NEEDS MORE SAFEGUARDS
There are no restrictions - essentially this seems to say the Secretary of State may access and examine all data to find anything that may possibly be any kind of item (broadly interpreted) in 9(6)". This is a charter so wide as to overturn any privacy restrictions, if not safeguarded.

At a minimum, filtering generally is of two types:

(a) specific targeted filtering in which all data is *scanned on demand* for specific words, communications, patterns or other data likely to be of value in a specific incident or investigation;
(b) general untargeted filtering in which all or some category of data is *indiscriminately and routinely scanned*, without prior knowledge of any specific matter, in order to identify such matters or their possible occurrence.

General untargeted filtering is the one requiring restriction, because it looks at everyone and every action of any citizen, and provides a means of data access and "data mining" that is at the heart of widespread public apprehension. The appropriate restrictions are that by design of the relevant systems, communications data should mandatorily not be readily accessible (directly or otherwise) or provided to any person or other system, except in a few circumstances. Especially:

- General untargeted filtering shall not be performed on systems that by design, minimise exposure of details of persons and communications data, other than (a) for testing purposes or (b) encountering data that it is intended to notify and report as potentially significant.

- Other than these exceptions, systems used for general untargeted filtering shall be designed to minimize and prevent unauthorised review of data, data mining, or privacy breach by any person or persons, or transmission or delivery of the same to any person or system outside the approved filtering process.

(And (15)(4) also requires reflection of a de minimis)

(16) through (21)
Confusing term “authorisation data” doesn’t intuitively make sense. Can this be replaced by “authorised communications data”?

(28)
The definition of "communication data" itself is strange, see (a)(i). A visual image is not by its nature a communication (if I scan an image of a picture or keep an audio recording of a book on my computer is this a "communication". The clause (a)(i) is also redundant because saved data, images etc are already "documents". The real sense of a "communication" is captured by (ii) anyway.
Concern – Unclear as to need for (a)(i) which also appears to make this act encompass an undesirably huge range of non communications.
Action –

1. remove (a)(i), if needed merging its contents into the definition of "document";
2. if at any point the term "communication" needs to encompass the deleted meaning of (a)(i), then amend to state "communications or document" which is clearer.

August 2012

The Global Network Initiative

1. The Global Network Initiative (GNI) welcomes the opportunity to provide written evidence to the Communications Data Bill Joint Scrutiny Committee. We have three specific concerns that we detail in our submission:

a) Broadening the collection and retention of new data on anyone in the UK using communications services;
b) The assertion of jurisdiction over non-UK based communications service providers when services are accessed in the UK;
c) A reserve power that would empower the Home Secretary to require UK providers to capture and retain data (specifically and only for law enforcement purposes) if requirements to capture and retain data cannot be directly imposed on a non-UK provider.

2. GNI is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics, who have created a collaborative approach to protect and advance freedom of expression and privacy in the Information Communications and Technology (ICT) sector. GNI has developed a set of Principles and Implementation Guidelines to guide responsible company action when facing requests from governments around the world that could impact on the freedom of expression and privacy rights of users. These Principles and Implementation Guidelines are based on international human rights standards and are attached to this written evidence in Appendix A. Appendix B has a full list of participants and observers of GNI.

3. It is the duty of governments to respect, protect, promote and fulfil human rights, including to ensure that national laws, regulations and policies are consistent with international human rights laws standards. GNI acknowledges the duty of a government to protect its citizens and public safety. It is right that governments consider how the changing communications landscape impacts policing operations and efforts to protect national security. However, the approach taken must reflect the few and limited circumstances within the Universal Declaration of Human Rights that provide for the limitation of these rights. Finding the right approach is not easy, particularly in the global, complex, and constantly evolving ICT sector.

4. No other democratic nation has proposed the approach set out in this Bill. The UK plays an important leadership role in the development of international legal standards and has far reaching influences on policy thinking generally. This includes the development of policy and legal frameworks relating to communications technology and the protection of human rights. For example, the UK used its convening power to assemble government, industry and civil society representatives to the London Conference on Cyberspace in October 2011, the first gathering of its kind that brought together the cyber-security community with the human rights community.[149] The UK also engaged early to help form an international coalition of governments now working together on freedom of expression on the Internet.[150]

5. There are very active debates internationally on the future of Internet governance. Several proposals, including one at the UN General Assembly for a code of conduct on information security are indicative of efforts by repressive regimes to exert a greater degree of control over the Internet. This could include placing greater requirements on companies.[151]

---

[149] For more information see http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/.

[150] See "Freedom Online: Joint Action for Free Expression on the Internet", The Hague, 9 December 2011, available at http://www.minbuza.nl/binaries/content/assets/minbuza/en/the_ministry/declaration-final-v-14dec.pdf.

[151] "International Code of Conduct for Information Security" presented to UN General Assembly 12 September 2011, http://news.dot-nxt.com/2011/09/13/china-russia-security-code-of-conduct.

6. Whilst these broader issues are outside the direct scope of the UK Communications Data Bill, they demonstrate the wider international context within which the draft Bill sits. We urge the Committee to consider the global context in its scrutiny of the draft Bill and be mindful of possible unintended consequences that could undermine the UK's ability to support and further freedom of expression and privacy rights internationally. We would suggest it is not in the broader interests of the UK to initiate legislation that could give authoritarian regimes justification for their approach.

Specific comments on the Communications Data Bill

7. **The Bill broadens the collection and retention of new data on anyone in the UK using communications services.** This includes requirements to generate data—not required for business purposes and not routinely collected by providers—specifically and only for the purpose of law enforcement access. This provision goes beyond the existing requirements under the Regulatory and Investigatory Powers Act (RIPA) and the EU's Data Retention Directive.

8. This aspect of the Bill could set a powerful precedent for repressive regimes to follow when seeking to justify surveillance on their own populations. Regimes attempt to claim legitimacy for their actions when they are able to point to similar requirements, even if only in the form of policy statements or draft legislation, in leading democratic nations. An example of exactly this type of reaction came from China in response to statements made in Parliament by the Prime Minister David Cameron in the days following the riots in 2011 around the need to consider placing limits on social networks and allowing greater government access to user communications in certain circumstances.[152]

9. This is an enabling Bill that would require secondary legislation or Notices/Orders to be fully implemented. It is not clear whether secondary legislation or Orders, including those that would specify the data sets to be collected, would be made public. These details should be made available so that stakeholders and Parliament can make proper assessments about proportionality and the impact of the Government's proposals.

10. Technological advances are also blurring the distinction between communications data and content that is at the heart of this Bill. For example, the URL for a web address can provide considerable access to information about the type of content the user is viewing. Stakeholders must be reassured that communications data could be reliably extracted without also disclosing content. Taken alongside the expanded scope of data collection for anyone using communications services in the UK this must be considered when assessing the proportionality of the proposals.

11. **The assertion of jurisdiction over non-UK-based communications service providers when services are accessed in the UK is problematic.** Companies considering the provision of services in markets where free expression and privacy rights may be at risk may consider ways to manage and operate their services to mitigate human rights risks. This is one of the requirements in GNI's Principles. It is also consistent within the UN Protect, Respect and Remedy framework and Guiding Principles.[153] We have seen worrying trends in legislative proposals in a range of countries that hold intermediaries liable for the activities of their users in ways that could have serious implications for free speech. One example is the draft Internet decree by the Government of Vietnam that places requirements on foreign providers not located in Vietnam to collaborate with the government in the filtering of a wide variety of information such as that which could

[152] Global Times, "Riots lead to rethink of Internet freedom", 13 August 2011, available at http://www.globaltimes.cn/NEWS/tabid/99/articleType/ArticleView/articleId/670718/Riots-lead-to-rethink-of-Internet-freedom.aspx.

[5] UN Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", available at http://www.business-humanrights.org/SpecialRepPortal/Home/Protect-Respect-Remedy-Framework/GuidingPrinciples.

"undermine the fine customs and traditions of the nation". Whilst filtering requirements and retention of communications data are not analogous, assertions of jurisdiction are. The draft Bill could provide unintended justification for actions by other governments. The UK Government should consider these consequences, including the impact of laws enacted in other jurisdictions on the privacy rights of UK citizens as it prepares this legislation.

12. Even if other jurisdictions do not enact similar or contrary laws, UK citizens' data could still be at jeopardy. Once other governments become aware of the storage of this additional communications data, law enforcement entities in other jurisdictions will seek to obtain it as well. If ICT companies are required to obtain and retain communications data for UK residents law enforcement entities in other jurisdictions could have a legitimate claim to seek access to it. Non-UK law enforcement entities may either try to obtain it through UK law enforcement or by exerting pressure on companies to release the data without UK cooperation.

13**. A reserve power proposed in the Bill would empower the Home Secretary to require UK providers to capture and retain data (again, specifically and only for law enforcement purposes) if requirements cannot be directly imposed on a non-UK provider.** Setting aside the technical challenges of whether this can be done, there are two specific problems. First, this requirement could have the effect of increasing pressure on non-UK providers to cooperate with law enforcement in informal, voluntary agreements. In contrast, GNI's Implementation Guidelines commit companies to encourage governments to be "specific, transparent and consistent in the demands, laws, and regulations" they issue. Secondly, although we understand the challenge that law enforcement faces in regard to accessing communications data in a timely fashion, proposals to address this issue should begin with existing processes. If processes such as mutual legal assistance treaties (MLATs) are insufficiently fleet of foot, then government should initiate a concerted effort to review and improve them. This would be a far more proportionate response to the legitimate concern that data may not be available by the time a lawful request is served on a provider. In June 2012 a GNI commissioned report recommended that access to data through the MLAT process needs to be made more efficient, with safeguards in place.[154]

Conclusion

14. As it considers this legislation, the committee has an opportunity to guide government on how the legitimate needs of law enforcement can be consistent with international human rights standards. It has the opportunity to develop an approach that would serve as a worthy model for other countries. The draft Bill does not succeed in this respect. We recommend that more time be taken and revisions considered to ensure that the rights of individuals are respected, so as to shape a regime that the UK would be comfortable having copied by other governments.

Global Network Initiative
Written Evidence to the Communications Data Bill Joint Scrutiny Committee
Appendix A: GNI Principles and Implementation Guidelines

Principles on Free Expression and Privacy

1. Preamble
2. Freedom of Expression
3. Privacy
4. Responsible Company Decision Making

---

[154] Ian Brown and Douwe Korff, "Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online", June 2012, available at http://www.globalnetworkinitiative.org/news/new-report-outlines-recommendations-governments-companies-and-others-how-protect-free.

5. Multi-Stakeholder Collaboration
6. Governance, Accountability & Transparency

Annex A: Definitions
Annex B: End Notes

1. Preamble

These Principles on Freedom of Expression and Privacy ("the Principles") have been developed by companies, investors, civil society organizations and academics (collectively "the participants").

These Principles are based on internationally recognized laws and standards for human rights, including the Universal Declaration of Human Rights ("UDHR"), the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights ("ICESCR").[155][156]

All human rights are indivisible, interdependent, and interrelated: the improvement of one right facilitates advancement of the others; the deprivation of one right adversely affects others. Freedom of expression and privacy are an explicit part of this international framework of human rights and are enabling rights that facilitate the meaningful realization of other human rights.[157]

The duty of governments to respect, protect, promote and fulfill human rights is the foundation of this human rights framework. That duty includes ensuring that national laws, regulations and policies are consistent with international human rights laws and standards on freedom of expression and privacy.

Information and Communications Technology (ICT) companies have the responsibility to respect and protect the freedom of expression and privacy rights of their users. ICT has the potential to enable the exchange of ideas and access to information in a way that supports economic opportunity, advances knowledge and improves quality of life.

The collaboration between the ICT industry, investors, civil society organizations, academics and other stakeholders can strengthen efforts to work with governments to advance freedom of expression and privacy globally.

For these reasons, these Principles and their accompanying Implementation Guidelines establish a framework to provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of human rights globally.

The participants have also developed a multi-stakeholder governance structure to ensure accountability for the implementation of these Principles and their continued relevance, effectiveness and impact. This structure incorporates transparency with the public, independent assessment and multi-stakeholder collaboration.

---

[155] It is recognized that other regional human rights instruments address the issues of freedom of expression and privacy, including: The European Convention, implemented by the European Court of Human Rights; the American Convention, implemented by the Inter-American Court of Human Rights and Inter-American Commission; and the Organization of African Unity, implemented by the African Commission on Human and People's Rights.

[156] These Principles have also been drafted with reference to the World Summit on the Information Society Tunis Agenda for the Information Society.

[157] It should be noted that the specific scope of these Principles is limited to freedom of expression and privacy.

The participants will seek to extend the number of organizations from around the world supporting these Principles so that they can take root as a global standard.

2. Freedom of Expression

Freedom of opinion and expression is a human right and guarantor of human dignity. The right to freedom of opinion and expression includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[158]

Freedom of opinion and expression supports an informed citizenry and is vital to ensuring public and private sector accountability. Broad public access to information and the freedom to create and communicate ideas are critical to the advancement of knowledge, economic opportunity and human potential.

The right to freedom of expression should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws or standards.[159] These restrictions should be consistent with international human rights laws and standards, the rule of law and be necessary and proportionate for the relevant purpose.[160] [161]

- Participating companies will respect and protect the freedom of expression of their users by seeking to avoid or minimize the impact of government restrictions on freedom of expression, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication.

- Participating companies will respect and protect the freedom of expression rights of their users when confronted with government[162] demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to information and ideas in a manner inconsistent with internationally recognized laws and standards.

3. Privacy

Privacy is a human right and guarantor of human dignity. Privacy is important to maintaining personal security, protecting identity and promoting freedom of expression in the digital age.

---

[158] Taken from Article 19 of Universal Declaration of Human Rights and Article of 19 of the International Covenant on Civil and Political Rights. It should be noted that these Articles reference the right to "freedom of opinion and expression", and then describe the limited circumstances in which the right to "freedom of expression" (i.e. not opinion) can be restricted. That is the approach taken by these Principles.

[159] The narrowly defined circumstances should be taken from Article 19 of the International Covenant on Civil and Political Rights (ICCPR), namely the actions necessary to preserve national security and public order, protect public health or morals, or safeguard the rights or reputations of others. The scope of permissible restrictions provided in Article 19(3) of the ICCPR is read within the context of further interpretations issued by international human rights bodies, including the Human Rights Committee and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

[160] See Annex A for an illustrative definition of Rule of Law.

[161] These Principles have been drafted with reference to the Johannesburg Principles on National Security, Freedom of Expression and Access to Information. The Johannesburg Principles provide further guidance on how and when restrictions to freedom of expression may be exercised.

[162] Participating companies will also need to address situations where governments may make demands through proxies and other third parties.

Everyone should be free from illegal or arbitrary interference with the right to privacy and should have the right to the protection of the law against such interference or attacks.[163]

The right to privacy should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws and standards. These restrictions should be consistent with international human rights laws and standards, the rule of law and be necessary and proportionate for the relevant purpose.

- Participating companies will employ protections with respect to personal information in all countries where they operate in order to protect the privacy rights of users.

- Participating companies will respect and protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards.

4. Responsible Company Decision Making

The implementation of these Principles by participating companies requires their integration into company decision making and culture through responsible policies, procedures and processes.

- Participating companies will ensure that the company Board, senior officers and others responsible for key decisions that impact freedom of expression and privacy are fully informed of these Principles and how they may be best advanced.

- Participating companies will identify circumstances where freedom of expression and privacy may be jeopardized or advanced and integrate these Principles into their decision making in these circumstances.

- Participating companies will implement these Principles wherever they have operational control. When they do not have operational control, participating companies will use best efforts to ensure that business partners, investments, suppliers, distributors and other relevant related parties follow these Principles.[164] [165] [166]

5. Multi-stakeholder Collaboration

The development of collaborative strategies involving business, industry associations, civil society organizations, investors and academics will be critical to the achievement of these Principles.

---

[163] Taken from Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

[164] "Operational control" means the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity. This may be by contract, ownership of voting stock or representation on the Board of Directors or similar governing body.

[165] See Annex A for a definition of Best Efforts.

[166] It is recognized that the influence of the participating company will vary across different relationships and contractual arrangements. It is also recognized that this principle applies to business partners, suppliers, investments, distributors and other relevant related parties that are involved in the participating company's business in a manner that materially affects the company's role in respecting and protecting privacy and freedom of expression. The participating company should prioritize circumstances where it has greatest influence and/or where the risk to freedom of expression and privacy is at its greatest.

While infringement on freedom of expression and privacy are not new concerns, the violation of these rights in the context of the growing use of ICT is new, global, complex and constantly evolving. For this reason, shared learning, public policy engagement and other multi-stakeholder collaboration will advance these Principles and the enjoyment of these rights.

- Participants will take a collaborative approach to problem solving and explore new ways in which the collective learning from multiple stakeholders can be used to advance freedom of expression and privacy.

- Individually and collectively, participants will engage governments and international institutions to promote the rule of law and the adoption of laws, policies and practices that protect, respect and fulfill freedom of expression and privacy.[167]

6. Governance, Accountability and Tranparency

These Principles require a governance structure that supports their purpose and ensures their long term success.

To ensure the effectiveness of these Principles, participants must be held accountable for their role in the advancement and implementation of these principles.

- Participants will adhere to a collectively determined governance structure that defines the roles and responsibilities of participants, ensures accountability and promotes the advancement of these Principles.

- Participants will be held accountable through a system of (a) transparency with the public and (b) independent assessment and evaluation of the implementation of these Principles.

Annex A: Definitions

Freedom of Expression: Freedom of expression is defined using Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR):

> **UDHR:** Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.
>
> **ICCPR:** 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

---

[167] It is recognized that participants may take different positions on specific public policy proposals or strategies, so long as they are consistent with these Principles.

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

Privacy: Privacy is defined using Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR):

> **UDHR:** No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
>
> **ICCPR:** 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

Rule of Law: A system of transparent, predictable and accessible laws and independent legal institutions and processes which respect, protect, promote and fulfill human rights.

Personal Information: Participants are aware of the range of definitions for "personal information" or "personally identifiable information" and acknowledge that these definitions vary between jurisdictions. These Principles use the term "personal information" and interpret this to mean information that can, alone or in aggregate, be used to identify or locate an individual (such as name, email address or billing information) or information which can be reasonably linked, directly or indirectly, with other information to identify or locate an individual.

User: Any individual using a publicly available electronic communications service, for private or business purposes, with or without having subscribed to this service.

Best Efforts: The participating company will, in good faith, undertake reasonable steps to achieve the best result in the circumstances and carry the process to its logical conclusion.

Annex B: End Notes

Implementation Guidelines for the Principles on Free Expression and Privacy

7. Purpose of this Document
8. Responsible Company Decision Making
9. Freedom of Expression
10. Privacy
11. Multi-Stakeholder Collaboration
12. Governance, Accountability & Transparency

Annex A: Definitions

1. Purpose of this Document

The Principles on Freedom of Expression and Privacy (the "Principles") have been created to provide direction and guidance to the Information and Communications Technology ("ICT") industry and its stakeholders in protecting and advancing the enjoyment of these human rights globally.

These Implementation Guidelines provide further details on how participating companies will put the Principles into practice. The purpose of this document is to:

- Describe a set of actions which constitute compliance with the Principles.

- Provide companies with guidance on how to implement the Principles.

As described in the accompanying Governance, Accountability and Learning Framework, each participating company will be assessed on their progress implementing the Principles after two years and annually thereafter.

The effectiveness of these Implementation Guidelines will be reviewed and assessed as experience in implementation of the Principles grows. The review process will include:

- Removing, revising or adding guidelines as appropriate.

- Considering the development of different versions of the Implementation Guidelines that may be tailored to specific regions or sectors.

2. Responsible Company Decision Making

Board Review, Oversight and Leadership

The Boards of participating companies will incorporate the impact of company operations on freedom of expression and privacy into the Board's review of the business.

The Board will:

- Receive and evaluate regular reports from management on how the commitments laid out in the Principles are being implemented.

- Review freedom of expression and privacy risk within the overall risk management review process.

- Participate in freedom of expression and privacy risk training as part of overall Board education.

Application Guidance: *"Board" could mean a Management Board or Executive Board if these are more appropriate for the participating company's structure.*

Human Rights Impact Assessments

Participating companies will employ human rights impact assessments to identify circumstances when freedom of expression and privacy may be jeopardized or advanced, and develop appropriate risk mitigation strategies when:

- Reviewing and revising internal procedures for responding to government demands for user data or content restrictions in existing markets

- Entering new markets, particularly those where freedom of expression and privacy are not well protected.

- Reviewing the policies, procedures and activities of potential partners, investments, suppliers and other relevant related parties for protecting freedom of expression and privacy as part of its corporate due diligence process.

- Designing and introducing new technologies, products and services.

The human rights impact assessments will be undertaken to different levels of detail and scope depending on the purpose of the impact assessment. However, participating companies should:

- Prioritize the use of human rights impact assessments for markets, products, technologies and services that present the greatest risk to freedom of expression and privacy or where the potential to advance human rights is at its greatest.

- Update human rights impact assessments over time, such as when there are material changes to laws, regulations, markets, products, technologies, or services.

- Draw upon resources from human rights groups, government bodies, international organizations and materials developed as part of this multi-stakeholder process.

- Include a consideration of relevant local laws in each market and whether the domestic legal systems conform to rule of law requirements.

- Utilize learning from real life cases and precedents.

- Focus on potential partners, investments, suppliers and other relevant related parties that are involved in the participating company's business in a manner that materially affects the company's role in respecting and protecting privacy and freedom of expression.

- Incorporate the outputs of human rights impact assessments into other company processes, such as corporate risk assessments and due diligence.

Partners, Suppliers and Distributors

Participating companies will follow these Principles and Implementation Guidelines in all circumstances when they have operational control.

When the participating company does not have operational control it will use best efforts to ensure that business partners, investments, suppliers, distributors and other relevant related parties follow the Principles.

Participating companies should focus their efforts on business partners, investments, suppliers, distributors and other relevant related parties that are involved in the participating company's business in a manner that materially affects the company's role in respecting and protecting freedom of expression and privacy. The participating company should prioritize circumstances where it has the greatest influence and/or where the risk to freedom of expression and privacy is at its greatest.

Application Guidance: *It is assumed that this approach will be taken in all relevant contracts signed after committing to the Principles and to all relevant pre-existing contracts.*

Application Guidance: *"Operational control" means the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity. This may be by contract, ownership of voting stock or representation on the Board of Directors or similar governing body.*

Application Guidance: *It is recognized that the influence of participating companies will vary across different relationships and contractual arrangements. See the definition of "best efforts" provided in Annex A.*

Integration into Business Operations

Participating companies will develop appropriate internal structures and take steps throughout their business operations to ensure that the commitments laid out in the Principles are incorporated into company analysis, decision making and operations.

Over time this will include:

Structure

- The creation of a senior-directed human rights team, including the active participation of senior management, to design, coordinate and lead the implementation of the Principles.

  Application Guidance: *This team may build on existing internal corporate structures, such as corporate social responsibility, policy, privacy or business ethics teams.*

- Ensuring that the procedures related to government demands implicating users' freedom of expression or privacy rights are overseen and signed-off by an appropriate and sufficiently senior member of the company's management and are appropriately documented.

Procedures

- Establishing written procedures that ensure consistent implementation of policies that protect freedom of expression and privacy and documenting compliance with these policies. Documentation of policies and compliance should be sufficiently detailed as to enable later internal and external review.

- Establishing a means of remediation when business practices that are inconsistent with the Principles are identified, including meaningful steps to ensure that such inconsistencies do not recur.

- Incorporating freedom of expression and privacy compliance into assurance processes to ensure compliance with the procedures laid out in the Principles.

- Maintaining a record of requests and demands for government restrictions to freedom of expression and access to personal information.

Employees

- Communicating the Principles to all employees, such as through the company intranet, and integrating the company's commitment to the Principles through employee training or orientation programs.

- Providing more detailed training for those corporate employees who are most likely to face freedom of expression and privacy challenges, based on human rights impact assessments. This may include staff in audit, compliance, legal, marketing, sales and business development areas. Where appropriate and feasible, the orientation and training programs should also be provided to employees of relevant related parties such as partners, suppliers and distributors.

Complaints and Assistance

- Developing escalation procedures for employees seeking guidance in implementing the Principles.

- Providing whistle-blowing mechanisms or other secure channels through which employees and other stakeholders can confidentially or anonymously report violations of the Principles without fear of associated punishment or retribution.

  Note: *For example, each company might appoint or designate an internal ombudsman or auditor to monitor the company's business practices relating to freedom of expression and privacy.*

3. Freedom of Expression

Government Demands, Laws and Regulations

Participating companies will encourage governments to be specific, transparent and consistent in the demands, laws and regulations ("government restrictions") that are issued to restrict freedom of expression online.

Participants will also encourage government demands that are consistent with international laws and standards on freedom of expression. This includes engaging proactively with governments to reach a shared understanding of how government restrictions can be applied in a manner consistent with the Principles.

When required to restrict communications or remove content, participating companies will:

- Require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression.

- Interpret government restrictions and demands so as to minimize the negative effect on freedom of expression.

- Interpret the governmental authority's jurisdiction so as to minimize the negative effect on to freedom of expression.

  Application Guidance: *It is recognized that the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time.*

- Seek clarification or modification from authorized officials when government restrictions appear overbroad, not required by domestic law or appear inconsistent with international human rights laws and standards on freedom of expression.

  Application Guidance: *Overbroad could mean, for example, where more information is restricted than would be reasonably expected based on the asserted purpose of the request.*

- Request clear written communications from the government that explain the legal basis for government restrictions to freedom of expression, including the name of the requesting government entity and the name, title and signature of the authorized official.

  Application Guidance: *Written demands are preferable, although it is recognized that there are certain circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written.*

- Adopt policies and procedures to address how the company will respond in instances when governments fail to provide a written directive or adhere to domestic legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.

- Challenge the government in domestic courts or seek the assistance of relevant government authorities, international human rights bodies or non-governmental organizations when faced with a government restriction that appears inconsistent with domestic law or procedures or international human rights laws and standards on freedom of expression

  Application Guidance: *It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on freedom of expression, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.*

  Application Guidance: *Policies and procedures adopted by participating companies will address situations where governments may make demands through proxies and other third parties to evade domestic legal procedures.*

Communications With Users

Participating companies will seek to operate in a transparent manner when required by government to remove content or otherwise limit access to information and ideas. To achieve this, participating companies will, unless prohibited by law:

- Clearly disclose to users the generally applicable laws and policies which require the participating company to remove or limit access to content or restrict communications.

- Disclose to users in a clear manner the company's policies and procedures for responding to government demands to remove or limit access to content or restrict communications.

- Give clear, prominent and timely notice to users when access to specific content has been removed or blocked by the participating company or when communications have been limited by the participating company due to government restrictions. Notice should include the reason for the action and state on whose authority the action was taken.

4. Privacy

Data Collection

Participating companies will assess the human rights risks associated with the collection, storage, and retention of personal information in the jurisdictions where they operate and develop appropriate mitigation strategies to address these risks

Government Demands, Laws and Regulations

Participating companies will encourage governments to be specific, transparent and consistent in the demands, laws and regulations ("government demands") that are issued regarding privacy online.

Participating companies will also encourage government demands that are consistent with international laws and standards on privacy. This includes engaging proactively with governments to reach a shared

understanding of how government demands can be issued and implemented in a manner consistent with the Principles.

Participating companies will adopt policies and procedures which set out how the company will assess and respond to government demands for disclosure of personal information. When required to provide personal information to governmental authorities, participating companies will:

- Narrowly interpret and implement government demands that compromise privacy.

- Seek clarification or modification from authorized officials when government demands appear overbroad, unlawful, not required by applicable law or inconsistent with international human rights laws and standards on privacy.

  Application Guidance: *Overbroad could mean, for example, where more personal information is requested than would be reasonably expected based on the asserted purpose of the request.*

- Request clear communications, preferably in writing, that explains the legal basis for government demands for personal information including the name of the requesting government entity and the name, title and signature of the authorized official.

  Application Guidance: *Written demands are preferable, although it is recognized that there are certain circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written.*

- Require that governments follow established domestic legal processes when they are seeking access to personal information.

- Adopt policies and procedures to address how the company will respond when government demands do not include a written directive or fail to adhere to established legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.

- Narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that Country.

  Application Guidance: *It is recognized that the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time.*

- Challenge the government in domestic courts or seek the assistance of relevant authorities, international human rights bodies or non-governmental organizations when faced with a government demand that appears inconsistent with domestic law or procedures or international human rights laws and standards on privacy.

  Application Guidance: *It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on privacy, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.*

  Application Guidance: *Policies and procedures adopted by participating companies will address situations where governments may make demands through proxies and other third parties to evade domestic legal procedures.*

Communications with Users

Participating companies will seek to operate in a transparent manner when required to provide personal information to governments. To achieve this, participating companies will:

- Disclose to users in clear language what generally applicable government laws and policies require the participating company to provide personal information to government authorities, unless such disclosure is unlawful.

- Disclose to users in clear language what personal information the participating company collects, and the participating company's policies and procedures for responding to government demands for personal information.

- Assess on an ongoing basis measures to support user transparency, in an effective manner, regarding the company's data collection, storage, and retention practices.

  Application Guidance: *Participating companies will work with the Organization to raise awareness among users regarding their choices for protecting the privacy of their personal information and the importance of company data practices in making those choices.*

5. Multi-stakeholder Collaboration

Engagement in Public Policy

Participants will encourage governments and international institutions to adopt policies, practices and actions that are consistent with and advance the Principles.

Individually or collectively participants will:

- Engage government officials to promote rule of law and the reform of laws, policies and practices that infringe on freedom of expression and privacy.

  Application Guidance: *Promoting rule of law reform could include rule of law training, capacity building with law-related institutions, taking public policy positions or external education.*

- Engage in discussions with home governments to promote understanding of the Principles and to support their implementation.

- Encourage direct government-to-government contacts to support such understanding and implementation.

- Encourage governments, international organizations and entities to call attention to the worst cases of infringement on the human rights of freedom of expression and privacy.

- Acknowledge and recognize the importance of initiatives that seek to identify, prevent and limit access to illegal online activity such as child exploitation. The Principles and Implementation Guidelines do not seek to alter participants' involvement in such initiatives.

Participants will refrain from entering into voluntary agreements that require the participants to limit users' freedom of expression or privacy in a manner inconsistent with the Principles. Voluntary agreements entered into prior to committing to the Principles and which meet this criterion should be revoked within three years of committing to the Principles.

Application Guidance: *It is recognized that participants may take different positions on specific public policy proposals or strategies, so long as they are consistent with these principles.*

Internal Advisory Forum

A confidential multi-stakeholder Advisory Forum will provide guidance to participating companies on emerging challenges and opportunities for the advancement of freedom of expression and privacy.

External Multi-stakeholder Learning Forums

Participants will promote global dialogue and understanding of the Principles and share learning about their implementation. Participants will engage with a broad range of interested companies, industry associations, advocacy NGOs and other civil society organizations, universities, governments and international institutions.

Participants will create a global learning, collaboration and communication program. This program will identify stakeholders, topics and forums for learning, collaboration and communication activities.

Application Guidance: *This could include, for example, the Internet Governance Forum, the International Telecommunications Union, the UN Global Compact and the UN Special Representative of the Secretary General on human rights and transnational corporations and other business enterprises.*

Part of this learning program will be an annual Multi-stakeholder Learning Forum focusing on the rights to freedom of expression and privacy, the specific scenarios in which these rights are affected and other broader issues related to the implementation of the Principles.

Where participants have activities or operations in the same countries they will seek to collaborate on the development of local dialogues on relevant prominent issues and emerging concerns in those localities.

Participants will develop and share innovative tools, resources, processes and information that support the implementation of the Principles.

Included in the learning program will be a consideration of the role that tools such as encryption, anonymizing technologies, security enhancements and proxy technologies can play in enabling users to manage their media experiences and protect freedom of expression and privacy.

6. Governance, Accountability and Transparency

Governance

A multi-stakeholder representative Board will oversee this initiative, described in more detail in the accompanying Governance, Accountability and Learning Framework document.

Reporting on Implementation

There will be three different levels of reporting on the progress being made to implement the Principles, described in more detail in the accompanying Governance, Accountability and Learning Framework document.

Independent Assessment

There will be a system of independent assessment of the implementation of the Principles, described in more detail in the accompanying Governance, Accountability and Learning Framework document.

Annex A: Definitions

Freedom of Expression: Freedom of expression is defined using Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR):

> **UDHR:** Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.
>
> **ICCPR:** 1. Everyone shall have the right to hold opinions without interference.
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Privacy: Privacy is defined using Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR):

> **UDHR:** No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
>
> **ICCPR:** 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

Rule of Law: A system of transparent, predictable and accessible laws and independent legal institutions and processes, which respect, protect, promote and fulfill human rights.

Personal Information: Participants are aware of the range of definitions for "personal information" or "personally identifiable information" and acknowledge that these definitions vary between jurisdictions. These Implementation Guidelines use the term "personal information" and interpret this to mean information that can, alone or in aggregate, be used to identify or locate an individual (such as name, email address or billing information) or information which can be reasonably linked, directly or indirectly, with other information to identify or locate an individual.

User: Any individual using a publicly available electronic communications service, for private or business purposes, with or without having subscribed to this service.

Best Efforts: The participating company will, in good faith, undertake reasonable steps to achieve the best result in the circumstances and carry the process to its logical conclusion.

Global Network Initiative
Written Evidence to the Communications Data Bill Joint Scrutiny Committee
Appendix B: GNI Participants and Observers

Participants

The following organizations are participating in the Global Network Initiative.

- Annenberg School for Communication, University of Southern California
- Christine Bader, Kenan Institute for Ethics at Duke University
- Berkman Center for Internet & Society at Harvard University
- Boston Common Asset Management
- Calvert Group
- Center for Democracy & Technology
- Centre for Internet & Society
- Centro de Estudios en Libertad de Expresión
- Church of Sweden
- Committee to Protect Journalists
- Domini Social Investments LLC
- Electronic Frontier Foundation
- Evoca
- F&C Asset Management
- Folksam
- Google Inc.
- Human Rights First
- Human Rights in China
- Human Rights Watch
- Index on Censorship
- International Media Support (IMS)
- Internews
- Microsoft Corp.
- Movements.org
- Rebecca MacKinnon, New America Foundation
- Research Center for Information Law, University of St. Gallen
- Trillium Asset Management
- University of California, Berkeley School of Information
- Websense
- World Press Freedom Committee
- Yahoo! Inc.

Observers

The following companies currently have observer status with the Global Network Initiative:

- Afilias
- Facebook

William Heath

This Draft Communications Bill is not worth tinkering with; it should be rejected out of hand. The intention for mas data retention is wrong and the approach to solving the problem is wrong.

False premiss

The Government says it is losing access to certain categories of data. The world is indeed changing fast, and people with bad intentions use new tools. But it fails to set out the wider context: there is a flood of highly specific data available to government and to the security agencies. Ask them: do they or do they not routinely have access now to vastly more data about any individual compared with 20 years ago? Why is there no public debate set in this context?

The case this merely restores a capability which has been eroded is at best unproven, at worst deliberately misleading.

Corruption of public servants and of suppliers

Accepting that most public servants are honest and most suppliers to government try to do a good job, nevertheless routinely placing vast amounts of highly revealing data about everyone in the hands of CSPs and accessible to large numbers of public servants creates risk. It further damages people's trust in public servants and institutions. For the largely honest and law-abiding citizen it changes the role of their comms service providers so that instead of where essential doing their lawful duty as required they work routinely for the secret state against the individual's interests.

Human rights; whistleblowers

Others make the argument this is not conformant to our European human-rights obligations. I find this persuasive and it is a serious point. I particularly fear the impact on whistleblowers. CDP is an apparatus for ensuring a Government doing wrong can shoot the messenger.

Govenment IT spend

My previous company tracked with awe and growing concern not just the scale of government IT spend, but the lack of efficacy with which it was done. Worst of all was the profoundly wrong intention behind much of what was done: centralised databases for health, education, children and the National ID Scheme.

This is now starting to be rectified with a totally different, citizen-oriented, design driven, low-cost, agile culture in the new Government Digital Service.

But CDP is old-school: hyperambitious, based on the flawed premiss that shiny technology politicians don't properly understand will nevertheless cure our social ills and keep us safe, prone to massive escalating costs, no credible cost-benefit analysis published. It favours big established service providers over new agile tech businesses by placing overhead, complexity and additional cost on the services they offer.

I think the £1.8bn cost estimate is lowballed to get this through. Anecdotally the usual historic MoD practice was bid low to get projects through Parliament; you multiply that first estimate by pi (3.14) to get the real cost. That may apply here. We simply don't know, because the Home Office is so secretive about its cost estimates (as if the cost of our IT projects were the vital information that renders the UK unsafe).

Some of what is in the draft Bill is so outrageous (eg the general powers granted to the Home Secretary) that

it may be deliberately intended for sacrifice to get the main points through. Dont play along. This should be rejected out of hand.

Instead we need
- a shared "problem statement" on which most informed participants can agree on the facts
- an open consultation or debate which is technically, legally and commercially well-informed
- evaluation of the wider range of options available now and in the future, in the wider context of what the world is becoming
- a formal design process which addresses the core problem in a human and intelligent manner. This country has brilliant service designers who can address themselves to problems of crime and security. There is no sign theu have been near this draft Bill.

This "politicians fallacy" model of solving serious problems by creating massive IT projects through a legislative process has been proven repeatedly to fail, and at great expense. The clearest signal you can send that this is simply not good enough, that times have changed, and things will be done differently is not to tinker with this. Just reject it.

August 2012

Letter from Charles Farr dated 23 August 2012

Thank you for the opportunity to give evidence to the Joint Committee on 10 July. I said we would respond in writing to a number of issues that you raised. We will also merge this content into our wider written evidence, to be submitted in due course.
CD usage

You asked about the use of communications data (CD) by law enforcement and other agencies.

A summary from the initial findings of the recent ACPO survey of crime types for which CD is requested is attached at Annex A. Like a previous survey in 2010 it was conducted over a two week period and includes data from police forces and law enforcement agencies (including SOCA and HMRC) across the UK.

You will see that the four main crime types for which CD was sought were drugs, property offences (including burglary and theft), offences against the person (including kidnap, armed robbery and serious assault) and financial offences (including fraud and money laundering). The survey also indicates that almost 85% of data sought was less than six months old; data older than that was most relevant to investigations into terrorism, sexual and financial crime. While the overall figure relating to terrorism is relatively low, this reflects both the limited time period over which it was conducted, as well as the absence of the intelligence agencies from this survey. In reality, we would expect the proportion of usage for terrorism to be higher. A further breakdown of the results will be provided in due course in our written evidence.

Details of the 2010 survey are also included in Annex A. As we said in our oral evidence, the 2010 survey is less detailed than the survey this year, but does provide a useful indication of the use of CD by law enforcement for that period. The 2010 survey again provided information on the age of data requested in each category: 67.9% of data had been retained for up to six months when it was requested, with the remaining 32.1% retained for over six months, including some data which had been retained for more than 12 months (this data will have been retained by service providers for business purposes). In both surveys, information regarding age only covers service use and traffic data – subscriber data may have been held for business reasons for several years by the company before it was requested.

In his oral evidence to the Committee on 12 July, ACC Gary Beautridge may have given the impression that police forces also provide detailed statistics on their use of communications data directly to the Home Office. These statistics (the number of authorisations and notices issued under the Regulation of Investigatory Powers Act each year) are, in fact, provided by forces to the independent Interception of Communications Commissioner"s Office, not the Home Office. The Commissioner is responsible for determining what information about the use of communications data is published in his annual report.

The latest report from the Commissioner (for 2011) explains which agencies make use of communications data, including law enforcement and intelligence agencies (around 99%), the Financial Services Authority (around 0.48%), Local Authorities (0.4%) and other users (around 0.22%).

During our discussion, you asked whether communications data might be used in future only for investigations in connection with serious crime. I noted that there is no single definition of serious crime. In immigration law, for instance, a person is presumed to have been convicted of a particularly serious crime (and could, therefore, face potential removal from the UK, in spite of being a refugee) if they are sentenced to a period of imprisonment of at least two years or convicted of an offence specified by order of the Secretary of State. In criminal law, the Serious Crime Act 2007 provides a list of serious offences, but also allowing for offences that a court considers sufficiently serious to be treated as if they were contained in that list.

There are other definitions of serious crime based on: the likely sentence a person being investigated might receive; whether the criminal activity involves violence or substantial financial gain; or the minimum penalty (normally a term of imprisonment) that a person could receive if convicted of a particular crime. We will consider the implications of having a serious crime threshold further in our written evidence.

Benefits of CD
You asked about the proportion of cases in which communications data was essential in enabling a prosecution and securing a conviction. This is not straightforward. As the Committee noted in our earlier informal session, it is not possible to know what weight was attached by a jury to a particular piece of evidence. But I understand that the Crown Prosecution Service is collecting some information, in order to inform their own discussions with the Committee, and we are discussing with them what data it might be practical and possible to provide.

The CPS have already indicated that in the ten cases brought to trial by the CPS Organised Crime Division in April 2012, they relied on communications data in eight, including six cases of drug trafficking or conspiracies to supply controlled drugs, and two regarding money laundering. With the other two cases, communications data was used in an initial investigation and in an earlier trial.

As you know, we believe it would be misleading to assess the value of communications data only on the basis of whether it has been used as evidence in prosecutions. Communications data alerts the police and others to the identity of witnesses and other potential suspects to inform their ongoing investigations. Of course, it may also be critical to proving innocence as well as guilt.

Capability gap
You asked about our assessment of the capability gap and the impact that legislation is expected to have on this. We assess the present gap to operational stakeholders to be around 25%. This estimate is based on an assessment of the types of communications technology for which data is not retained at present, requests which cannot currently be met and those requests which are not even made because the police and others know the data will not have been retained.

We assess that this gap will widen without legislation. Use of traditional fixed line and mobile telephony has slowed, while internet use (driven by the predicted rise in smart phone and tablet sales) is expected to continue growing year on year. Over the next two years, without intervention, we estimate that the capability gap is likely to grow to approximately 35%.

I know that the Committee are also keen to understand more about the data that is currently available to public authorities and the data which public authorities are not able to access.

As the Committee knows, there are 3 categories of data – traffic data, service use data and subscriber data – defined in the Regulation of Investigatory Powers Act 2000 (RIPA) and the draft Bill). Under those categories, I have enclosed (at Annex B) an illustrative list of those types of data for which a public authority could submit a request to a current service provider in the UK. I believe your specialist adviser will be well-placed to explain these data types to you, but we would also be happy to do so, if that would be helpful. I should underline that, as agreed with your clerks, specific handling restrictions apply to the annexes marked Confidential.

The proposed legislation does not provide for the retention of new categories of data (as defined in RIPA and the draft Bill), nor does it specifically target a problem with one category of data (eg traffic or subscriber data). It seeks to ensure that this data is available in relation to all those services provided by Communications Service Providers (CSPs) to users in the UK. Not all UK providers currently obtain all the required data, such as weblogs or the data required to resolve an IP address to a particular individual or device. CSPs based overseas may not retain the data we need for 12 months, may not have the systems in place to allow access to this data in the time and format required, and may place limitations on the data they are prepared to provide.

The proposed legislation is intended to enable us to cover these gaps to a greater extent than we are currently able. We are examining whether it might be possible to provide the Committee with more detailed information, on a confidential basis, about the data that we are currently missing.

During the session, we also discussed whether the definition of communications data has changed in this legislation. As I stated, we are not changing the fundamental definitions of CD categories („subscriber", „use" and „traffic"). At present, however, "traffic data" does not expressly include the times at which a communication reaches each stage of its transmission. To fully understand how a message is routed, and its potential significance to an investigation, the times at which a message is sent, delivered and read may all be important. The Bill corrects this anomaly by adding „time" to the definition of traffic data. A minor consequential amendment has also been made to the equivalent definition in RIPA.

Cooperation with overseas providers
You asked about the compliance by overseas CSPs with requests for communications data made by UK public authorities. The picture across overseas providers is mixed. Most who receive disclosure requirements comply to the extent that they are able (and some publish statistics on their disclosures of information). Some do not provide all the data they could; some do not collect the data we require; some collect it, but do not retain it for long enough; some are not able to provide it in the timescales or the form that investigators need; and some are not able to provide a 24/7 service (which is particularly important in threat-to-life situations).

The Single Points of Contact (SPoCs), particularly in the major public authorities using communications data, will generally know what data will be available in a timely and useful manner from the main overseas providers. Where they believe the data will be available, they will make a request and, in most cases, it will be met. Where they do not believe it will be available, they will not usually request the data. There is no central log of the requests made by public authorities but refused by overseas providers. But as we set out in our oral evidence, the challenge we face is less that providers refuse individual requests, than that some requests will not be made by public authorities in the first place because they do not expect that the data to be available at all, or at the speed and quality required.

The value of the Bill in relation to overseas providers consists in helping us increase the availability of data for which requests can be made – for example, by asking an overseas provider to retain data in a suitable format for longer than they currently retain it for business purposes.

Safeguards
I know the Committee is interested in a specific criminal sanction for misuse of data, as well as information on the number of prosecutions and investigations for misuse. We have asked law enforcement agencies for information on any prosecutions and investigations and we will pass this on to you. But the Interception Commissioner"s 2011 report notes that he was satisfied that, where compliance issues were identified, „these occurred due to genuine misunderstandings, rather than any wilful or reckless failure to comply" and he has already been assured that the „necessary corrective action has been taken by these public authorities." Since 2005, we understand that the Commissioner has identified only one case where data was requested that should not have been disclosed as a matter of law under one of RIPA"s statutory purposes.
Where any abuse does take place, there are a number of relevant offences in the Computer Misuse Act and the Data Protection Act. Where abuse takes place inside a public authority, malfeasance in a public office may be relevant.

I know that the Committee is keen to visit a SPoC unit and hope that seeing the process and safeguards in practice will provide you with further context.

Costs and benefits
The Committee were interested in how much money is currently saved by the use of communications data. Benefits from the use of CD take different forms. I understand that Donald Toon gave evidence that CD is worth approximately £800m per annum to Her Majesty"s Revenue and Customs. Alternative investigative techniques, such as the use of covert surveillance teams, are extremely expensive, and will not provide information available from communications data, including historical information required in investigations. These techniques can also be much more intrusive. You have subsequently written with a set of detailed questions on costs and benefits. In our written evidence we will provide further information on the expected benefits and those achieved to date, as well as an explanation of the methodology used to calculate them.

Technical issues
You asked where the deep packet inspection (DPI) 'boxes' are likely to be manufactured. Where practical, CSPs may use their existing suppliers and solutions to collect required CD from their networks. A number of UK and international suppliers provide specialist DPI equipment. We are confident that CSPs and industry can provide a CD collection capability, and will work with them to procure a sustainable network collection capability.

Manufacturers who provide PI equipment to the global telecommunications sector include: Acme Packet Inc; AdaptiveMobile Ltd; Advanced IO Systems; Alcatel-Lucent; Arbor Networks Inc.; BAE Systems Detica; Bivio Networks Inc.; Bridgewater Systems Corp.; Cisco; Cloudshield Technologies; Endace; Huawei; IP Fabrics; Ipoque; Juniper; Niksun; Procera Networks; Radware; Roke Manor; Solera Networks; Symantec; Tilera; Unipier; TRL; and Verint.

Regarding the request filter, you asked whether you can manually check that it had filtered correctly (to ensure that the result is sound) and whether there would be an audit trail of filter requests. Both will be possible. Automated systems, such as the Request Filter, should minimise intrusion and reduce the risk of errors which arise from human error. If, however, a public authority had concerns that the returned results from the Filter were incorrect, a manual check of the audit trail of the Filter request could be undertaken. The Draft Bill includes new obligations on the Secretary of State and the Interception Commissioner to monitor the operation of the filter (including frequent testing), in order to continually demonstrate that it is providing accurate results.

Delegated Legislation

I recognise that the Committee are keen to see draft Orders, particularly with respect to Clause 1 of the Bill. As you will be aware, James Brokenshire told the House on 9 July that we would keep this matter under review. We are keen to provide as much clarity as possible, but do not, at this stage, have a draft Order to share with the Committee. We will, however, work on an indicative list of the type of obligations that might be set out in a draft Order, and how this might be translated into the more specific requirements of a notice issued to a CSP. We will provide this to the Committee shortly.

With regard to the Order that will list the public authorities that can access CD under the Bill, we informed the Committee that we have written to all public authorities listed under the RIPA (Communications Data) Order 2010: they are given in Annex C. We have now started to receive business cases from these public authorities and will provide a summary of these to the Committee in the autumn. No decision has yet been taken on which of these authorities might continue to be able to obtain communications data; I am sure the Committee will express views on this point.

On a separate issue, during the hearing, Lord Armstrong asked about the statutory instrument that would set the level for the designated senior officers (DSO). Lord Armstrong was correct that a statutory instrument that only set this level would be a negative order, but in practice any Order specifying the rank of a DSO will almost certainly also designate relevant public authorities and impose restrictions on the exercise of the Part 2 powers, so will most likely become subject to the affirmative procedure.

Consultation
You asked about consultation on the proposals within the Bill:

A public consultation on CD under the previous Government in 2009 set out the challenges regarding future access to CD. Following the election, the current Government assessed the evidence and, following advice from law enforcement, security and intelligence agencies, discussion with industry and consideration in the National Security Council, developed a new approach to CD collection and access, reflected in this legislation.

A separate public consultation was conducted in 2009 to identity the public authorities that should be able to acquire communications data under RIPA, the types of data they could acquire, and the purposes for which they could acquire it. This resulted in the Regulation of Investigatory Powers (Communications Data) Order 2010. As you know, we are again consulting public authorities to collect and assess their business cases for retaining the power to acquire communications data.

A broad range of Government departments and public bodies have been consulted throughout the development of the draft Bill. Following publication other stakeholders (including public authorities, regulators, academics, interest and pressure groups and public commentators) have been briefed on its content.

There is ongoing engagement with industry on the Draft Bill, through bilateral meetings and well-established stakeholder engagement groups.

The Bill itself also requires the Secretary of State to consult prior to the placing of any obligations with Ofcom and any persons or organisations likely to be subject to such obligations, or their representatives.

The Government believes that this pre-legislative scrutiny process (the work of your Committee and that of the Intelligence and Security Committee) is vital in ensuring that the policy is properly considered before introduction to Parliament.

International Comparisons

A list of retention periods of the 27 EU Member States under the Data Retention Directive is attached at Annex D. More extensive international comparisons regarding wider aspects of CD will follow in our written evidence.
Please do not hesitate to contact me or my officials if you require anything further.

Home Office submission with restricted annexes removed

Summary
Communications data (CD) is the information about a communication: who was communicating; when; from where; and with whom.
We distinguish between CD and communications content. CD does not include the content of a communication.

CD is collected by the communications industry for their own business purposes. Law enforcement, the intelligence agencies and some other public authorities can seek access to it, usually in the investigation of a broad range of crimes. CD is critical to protecting the public. Alternative capabilities (including different forms of surveillance) are often more intrusive and expensive, and may not provide the same information. New internet-based technologies are generating communications data in different ways. Communications service providers (CSPs) may have no business interest in this data and, therefore, the data may not always be retained. As people move to internet-based forms of communication, it becomes much less likely that data (for example, an e-mail address) will be available to the police and others when they need it. This has a direct impact on our ability to investigate and prosecute criminals and terrorists. CD is routinely used as evidence to support prosecutions in court. A recent study by the Crown Prosecution Service Organised Crime Division showed that they used CD as evidence in over 85% of the cases they brought to trial in London, Birmingham and the North between April and June 2012.

Legislation is, therefore, necessary to ensure that CD continues to be available in the future, as it has been in the past. The proposed legislation will enable more of the communications data required by law enforcement and other agencies to be retained by CSPs.

Any public authority, beyond law enforcement and the intelligence agencies, wishing to continue to access communications data will need to make their case and have that access approved by Parliament.

The Bill retains and extends the safeguards and oversight arrangements for the acquisition of CD that exist under current legislation. There are proven safeguards and oversight – and penalties in other legislation – in place to prevent any misuse of these powers. The Bill is specifically designed to comply with Article 8 of the European Convention on Human Rights.

The way we communicate is changing. The Government believes that the capabilities available to law enforcement need to keep pace with these changes. The legislation will help ensure that the internet does not become a safe haven for criminality, and that the police and others can continue to protect the public.
INTRODUCTION
What is Communications Data?
1. Communications data (CD) is the information about a communication. It can include, for example, the time and duration of a phone call, the phone number or email address which has been contacted and the location from which a call has been made. Communications data does not include the content of any phone call or email.
How do law enforcement and intelligence agencies, and public authorities, use communications data?
2. Communications data is used by the police and intelligence agencies in the investigation of a broad range of crimes, including terrorism. It has played a significant role in every major Security Service counter terrorist investigation over the past decade and in 95 per cent of all serious organised crime investigations.
3. Communications data can support each stage of an investigation. At the outset, it can enable the identification of witnesses or suspects. It can then be used to test alibis or support witness statements. In the final stages of an investigation, it can be critical to building the overall case and is regularly used as evidence in court, where it may help build a chronological picture, demonstrate associations and contacts, establish the whereabouts of people involved and corroborate witness statements.

4. Statistics on the use of CD are provided by police forces and others to the independent Interception of Communications Commissioner, who issues an annual report. In 2011, the Commissioner reported that public authorities (primarily the police) submitted 494,078 requests for communications data. About 50% of these requests are to identify the subscriber of a communications device, for example the owner of a mobile phone.
5. The total number of requests does not correspond directly to the number of people being investigated (i.e. 500,000 requests do not relate to 500,000 people). Many requests may be made in relation to the same person because that person may hold and use a large number of communications devices (many criminals habitually change phones on a regular basis to try to evade detection). Nor does the number of requests correspond directly to the number of crimes investigated (i.e. 500,000 requests do not relate to 500,000 crimes). Many requests can be made during an investigation into a single crime; a significant murder, organised crime or counter-terrorism investigation can involve hundreds of communications data requests – many of which would be subscriber checks.
6. A 2-week snapshot survey undertaken by the Association of Chief Police Officers (ACPO) this year demonstrated the range of investigations which communications data can support. The four main crime types for which CD was sought were drugs, property offences (including burglary and theft), financial offences (including fraud and money laundering) and offences against the person (including kidnap, armed robbery and serious assault). Further details of this survey can be found in Annex A.
7. One key finding of this and previous surveys is that communications data is valuable even when it relates to communications which have taken place many months before an investigation begins. The survey indicated that, although the majority of communications data requested relates to recent communications (those that have taken place six months or less prior to law enforcement requesting the data), a significant and important minority of data older than that was used in investigations into terrorism, sexual and financial crime. For example, 52% of communications data used in child abuse investigations in the two week survey related to communications activity more than 6 months prior to the investigation.
8. From April to June 2012, the Crown Prosecution Service Organised Crime Divisions in London, Birmingham and the North used communications data as evidence in 46 of the 53 cases it brought to trial. Communications data was used as evidence in 28 of 31 cases (involving 62 defendants) in London (and in one other case had played a significant part earlier in the law enforcement operation); in 5 of 6 cases in Birmingham; and in 13 of 16 cases prosecuted in the North.
GENERAL
Has the Home Office made it clear what it hopes to achieve through the draft Bill? Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?
9. The purpose of the Bill is to maintain the availability of communications data for public authorities, notably the police, so that these authorities can obtain the data on a case-by-case basis when they are able to demonstrate that they need it. The Bill will replace Part 1 Chapter 2 of the Regulation of Investigatory Powers Act (RIPA), which concerns communications data.
10. At present, the law only requires UK communications service providers to retain communications data that they already generate or process for business reasons. But as technology and business models change, providers may not need to keep data for their own business reasons – for example, service providers may not need to know how many emails have been sent by one of their customers. Although the current Data Retention Regulations (transposing the EU Data Retention Directive) ensure that much of the communications data for domestic communications services is available for 12 months, they do not currently specify retention of all the data types that law enforcement need to identify the „who", „when" and „where" of a communication. In particular, data is not necessarily collected for internet based communications.
11. Moreover, providers of communications services in this country who are based outside of the EU are not covered by our Data Retention Regulations if they do not generate or process data in the UK. There is, at present, no requirement for them to retain communications data relating to their services even though those services may be provided to customers in the UK.
12. The effect of these developments is that communications data is not always available to the police and other public authorities when they require it in the course of an investigation. Data gaps are most apparent in connection with internet communications. For example, the Child Exploitation and Online Protection agency (responsible for the investigation of child exploitation in the UK) is already experiencing significant

problems in obtaining the same level of subscriber information for internet communications as is currently available for traditional telephony. Similar problems are being encountered across all areas of policing.
13. We currently assess that around 25% of the communications data needed by investigators is not currently available to support investigations. This estimate is based on an assessment of the types of communications technology for which data is not retained at present, requests that cannot currently be met and those requests that are not even made because the police and others know the data will not have been retained. Use of traditional fixed line and mobile telephony has slowed, while internet use (driven by the predicted rise in smart phone and tablet sales) is expected to continue growing year on year.
14. The proposed legislation provides powers to enable the Home Secretary to request a communications provider to retain data, even when the provider has no business reason to do so and where they may be offering services in the UK from outside the EU. That data would then be available to public authorities – exactly as data is available at present – where the authority can demonstrate why they need to see it and how it is proportionate for them to do so. The legislation envisages a continued collaborative relationship of the kind that exists at present between Government and providers. The period for which data will be requested to be retained will be as it is at present – 12 months.
15. Over the next two years, without intervention, we estimate that the gap in the availability of data is likely to grow to approximately 35%; and over a longer period, we predict this will degrade further still. The legislation will enable us to halt and then to reverse the decline in the availability of data to public authorities. The range of communications methods that are and will be available, and the challenge in keeping pace with the rate of technological change, means that it is no longer reasonable to expect we could return to 100% coverage. As a result of this Bill, we aim to prevent any further degradation in coverage and get back to around 85% by 2018. A confidential analysis of the modelling used to estimate the availability gap is at Annex B.
16. The proposed legislation does not provide for the retention of new categories of data (as defined in RIPA and the draft Bill), nor does it specifically target a problem with one category of data (such as traffic or subscriber data). It seeks to ensure that this data is available in relation to all those services provided by Communications Service Providers (CSPs) to users in the UK. The proposed legislation makes no changes to the existing framework for public authorities getting access to data. Nor does it make any change to arrangements for the interception of the content of electronic communications. These arrangements are not the subject of this legislation.
How will the Home Office use the powers created in the Bill?
17. Clause 1 of the proposed legislation provides a general power for the Secretary of State to ensure, by Order, that communications data is available to be obtained by public authorities. The Order itself will set out in more detail the requirements that may be placed on a communications service provider. The Order will be debated by Parliament and, if approved, will then enable specific draft notices to be drawn up and discussed with individual providers.
18. We will not place new requirements on every CSP or in relation to all communications services and new requirements will need to be proportionate. They will be subject to detailed discussion with legal, commercial and technical representatives from CSPs. Notices will be approved by Ministers and served on providers. The expectation is that notices will, therefore, be individually tailored to each of the provider's system or service where there is an operational need for communications data to be available. Our fundamental approach will be developing collaborative relationships with providers in order to ensure the continued availability of communications data.
19. In summary, Clause 1, provides the general power; the Order will set out the broad requirements; and the notice will set out the more detailed requirements for a specific CSP.
20. It has been claimed that, under this legislation, the Government is intending to place so-called "black boxes" on all networks in the UK. This is untrue. „Black box" is a misleading term that has been used to describe „Deep Packet Inspection" technology or probes, which can be used to monitor the flow of communications around networks so that network providers can manage or configure the network, in order to improve performance, reliability and the experience of their customers. Probes can be programmed to look for and pull off the network particular protocols or elements of a communication passing across the network, for example, the communications data.

21. Under these proposals, we are not planning to put probes on all UK networks. We will work with industry to determine the best solution, examining services used by people under investigation by the police or other authorised agencies. Probes would only be used when this approach did not provide the communications data required. Any communications data collected by such probes would, as with other data, be stored by industry, not by the Government.

What lessons can be learnt from the approach of other countries to the collection of communications data?

22. Public authorities (mainly policing) in all countries in Europe and most countries outside Europe make regular use of communications data to investigate crime.

23. Across the EU, there is a common minimum requirement for the retention of communications data by communications service providers. This requirement is set out in the Data Retention Directive (DRD). Member States have transposed the Directive consistent with their domestic requirements. EU Member States are also bound by common principles of data protection, including data deletion, as reflected in EU and other international law, and instruments such as the European Convention on Human Rights. This includes the processes for accessing retained data.

24. The DRD has been or is being transposed in all EU Member States with the exception of Germany, where the constitutional court ruled that in transposing the Directive the Government had not provided for appropriate measures to control access to the data retained under the DRD. The court did not rule that the premise of data retention was of itself unconstitutional. Constitutional courts in Romania, the Czech Republic, Bulgaria and more recently Cyprus made similar rulings on their transposition, but all these countries have now transposed or are doing so.

25. Public authority access to CD in the UK is broadly in line with comparable EU countries in terms of the volumes acquired, retention periods, and the purposes for which communications data may be accessed. More specific information on the approach being taken by other countries – including those outside of the EU – is contained in Annex C.

26. Procedures for access to CD vary across the EU according to Member States" criminal justice systems – because a system of magistrate approval exists in other countries does not mean it would be appropriate in the UK. The UK and the Republic of Ireland are common law countries with similar processes for authorising access to CD that has been retained under the DRD; applications for data must demonstrate necessity and proportionality, and are considered by a senior officer in the relevant organisation.

27. In countries such as France an investigating magistrate is responsible for directing the investigation of a crime and for its prosecution. In these countries the investigating magistrate is also responsible for approving applications for communication data. In countries where a judicial authorisation regime is in place, data can be acquired in certain circumstances using an internal authorisation regime similar to the UK (for example, if only subscriber data is required or if the data is for intelligence purposes). As set out at paragraphs 71-75 below, we believe that a process of judicial authorisation for all CD requests would be expensive, present operational risks and represent a significant change to our criminal justice system.

28. The technical and business changes which are having an impact on the availability of communications data in the UK are also having an impact in other countries, though the advanced state of our communications industry and law enforcement methods may mean the impact is felt sooner here than elsewhere. In countries which use intercept as evidence in court, interception of the content of communications will often be used, for example, to demonstrate the linkages between criminals in a network, where in the UK prosecutors would rely on communications data for the same purpose. In the US, law enforcement agencies may not face the same set of challenges as the UK as the dominant providers of internet-based services are the US companies. However, some other countries are also considering changes to domestic legislation or, in the case of some EU countries, taking a broader interpretation of existing data retention legislation to enable them to retain the communications data they require.

Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

29. The Government has considered carefully possible alternatives to the continued use of communications data in the investigation of crime and has concluded that there is no comparable like-for-like alternative. Directed surveillance (i.e. surveillance in a public place) and intrusive surveillance (i.e. surveillance in a private place, such as a home) do not provide essential historical information required in criminal investigations when investigating a crime that has already occurred. Nor would they provide rapid, accurate information of the kind available through communications data. They also involve greater intrusion into

privacy and are much more costly. The estimated maximum cost of the measures proposed in this legislation (£1.8 billion over ten years, or approximately £180m a year), amounts to just 1.3 per cent of the current annual £14bn police spending.

30. The Government has also considered alternative technical solutions. An approach considered by the previous Government would have involved the wider deployment across UK networks of technical probe equipment (as referred to in paragraph 20) to collect large volumes of data about services transiting the network (such as webmail or social media). Although we do not rule out the use of probes where necessary, this Government has reviewed this option and sees no benefit in pursing it.

31. It has been suggested that an alternative to a communications data regime based on data retention would be a regime built around data preservation: rather than requiring providers to retain data in relation to the services they provide on a continuous basis (with data destroyed after 12 months), they would retain data specific to an investigation once they were tasked to do so. It has been suggested that this would be less costly than the arrangements set out here and more proportionate. But a regime built around data preservation would not be consistent with the DRD, which requires data retention. And it would fail to meet the fundamental requirement of the Bill, namely that historic CD should be retrospectively available to investigators in the investigation of the background to a crime when it is necessary and proportionate for them to request it. The European Commission, in its Evaluation Report on the Data Retention Directive (published 18 April 2011), acknowledged the views of most Member States that data preservation could not replace data retention.

The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

32. This Government has committed to legislating better and less. In many cases, the communications data required by public authorities is already generated or processed by CSPs in the course of their business, and retained under the Data Retention Regulations. It is, therefore, not necessary to supersede these Regulations, although it would be possible to do so using the proposed legislation. This legislation will also amend or repeal a variety of other Acts which contain information gathering powers, often with weaker safeguards, which could be used to acquire communications data.

Is the proposed 12 month period for the retention of data too long or too short?

33. We believe that the 12 month proposed period for the retention of data is appropriate.

34. The EU Data Retention Directive provides for retention of communications data for up to 2 years; the UK has implemented a 12 months retention period based on evidence that the majority of data useful to law enforcement is up to 12 months old. A shorter period would risk losing data vital to investigations into serious crimes including terrorism, murder and sexual offences. A longer period would bring only modest additional benefits for investigators, which may not justify the cost and intrusion involved.

35. In June 2012, a 2-week nationwide snapshot survey of communications data requests was carried out by ACPO, including data from police forces and law enforcement agencies (including SOCA and HMRC). This showed that 84% of communications data requested was up to 6 months old, 13% of communications data requested was between 7 – 12 months old and 3% of communications data requests were for data which was more than 12 months old (although a communications service provider does not have to retain data beyond 12 months under the Data Retention Directive obligations, they might retain data for longer for their own business purposes). Further detail of this study is included at Annex A.

36. The age of data requested can vary depending on the type of crime under investigation. The overall statistics do not therefore reflect the importance of older data for particular crimes, such as terrorism, sexual and financial offences. In the snapshot survey half of the data requested in child abuse or bribery and corruption investigations was 6-12 months old: in the case of sexual offences, it may be that an offence is only reported following a period in which the victim comes to terms with the trauma of the event.

Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base? What might be the effect on business?

37. We see little risk that this legislation will make communications providers see the UK as a less attractive base. At present, CSPs are reimbursed by Government for costs incurred in the provision of communications data. These arrangements will continue under the proposed legislation: CSPs will not be

financially disadvantaged. We recognise that CSPs will want to be assured that the law will be applied consistently across providers. We are also committed to using legislation to support a collaborative relationship with industry. We will place obligations upon CSPs only where there is an operational need and it is proportionate to do so. Not all CSPs will be affected. Before placing an obligation, we will consult the CSP to ensure they can deliver what we are asking and will work with them to enable compliance.

How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

38. The approach taken in this Bill is consistent with the Government's wider approach to preserving civil liberties, including the right to privacy, protecting the public and safeguarding national security. The Bill contains significant safeguards to limit the intrusion into individuals" privacy to the minimum necessary and to ensure the consistency of the legislation with our obligations under Article 8 of the ECHR (set out in more detail in the Safeguards section below).

39. This is consistent with measures the Government has introduced or removed elsewhere in order to ensure that individuals" rights to privacy are properly protected. These include: abolishing the intrusive ID cards regime: scrapping the hugely disproportionate ContactPoint database, which would have held the details of every child in the country; restricting the retention of DNA profiles of individuals not convicted of a crime; imposing stricter regulation on CCTV and number plate recognition; restricting the use of Stop and Search, to ensure it is only used where there is reasonable suspicion; reducing the maximum period of pre-charge detention from 28 to 14 days; and restricting the access of Local Authorities to surveillance powers. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

40. The right to life is one of our most important civil liberties. Communications data is an essential tool used by the police and the agencies to investigate crime and bring to justice those who threaten our safety and security. Communications data is also essential in enabling the emergency services to locate vulnerable and missing people who are at risk. Access to communications data is subject to rigorous scrutiny and oversight by Parliament, Ministers and, where necessary, the courts. The Bill contains a wide range of safeguards to ensure that communications data is used lawfully and that any intrusion into individual privacy is proportionate and necessary. We do not, therefore, believe the legislation creates any „imbalance" in civil liberties that needs to be corrected by measures elsewhere.

SCOPE

Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

41. We believe that the definitions contained within the Bill are appropriate, given the need to be able to cover a range of systems, services, providers and categories of data. Any significant gaps in scope of the legislation may be exploited by criminals and terrorists wishing to evade justice.

42. The Bill maintains the three categories of communications data that are defined in RIPA. They are: „Subscriber data": information that private sector communications service providers (CSPs) hold about people to whom they provide a service (e.g. names, addresses, telephone numbers). „Use data": information about the use a person makes of a service (e.g. itemised telephone call records, records of connection to internet services, timing and duration of service usage). „Traffic data": information about a communication and the equipment used in transmitting it (e.g. information about the location of mobile phones, routing information such as IP address allocation).

43. We are not changing these fundamental definitions of CD („subscriber", „use" and „traffic"). At present, however, „traffic data" does not expressly include the times at which a communication reaches each stage of its transmission. To fully understand how a message is routed, and its potential significance to an investigation, the times at which a message is sent, delivered and read may all be important. The Bill corrects this anomaly by adding „time" to the definition of traffic data. A minor consequential amendment has also been made to the equivalent definition in RIPA.

44. The definition of communications data already includes data about websites which have been accessed. It also includes data about communications accessed through a website, including social media websites (such as e-mail and instant messaging). But communications data does not and will not include the content of specific pages that have been browsed within a website. Communications data detailing which websites customers visited (but not the specific pages) has been capable of being retained by communications service providers since 2001, where they have agreed to do so under a Voluntary Code of Practice on the retention

of communications data. This legislation only covers communications data – so it does not, for example, cover the content of any material posted on social media websites.

45. The Bill applies to any person who provides a telecommunications service. This includes a wide range of internet services, including email, messaging and social media services. The Bill also applies to any person who controls or provides a telecommunications system (for example, a mobile network provider). The definitions of systems and services in the legislation do not contain any geographical or territorial limitations, and are not therefore dependent on the location of the provider. In practice, obligations to retain data will relate to those systems or services used by UK nationals or persons within the UK. Further guidance will be provided within the codes of practice.

46. This legislation covers providers of both public and private telecommunications systems and services. This is to ensure that criminals cannot seek to evade detection and investigation by simply communicating through their own private systems. Obligations will only be imposed in relation to private systems and services where a legitimate operational requirement is identified and where it is reasonable to impose such requirements. More detail on these considerations would be set out within the new code of practice.

47. The Bill will also ensure the current powers relating to postal operators and postal services are maintained. In some cases, law enforcement or intelligence agencies might have to obtain communications data relating to a suspect's mail from a postal operator, but we have no plans to impose requirements on public postal operators to retain communications data. As with other services, requirements to obtain and retain communications data relating to postal services would only be imposed if there was reason to believe that these services are being used by terrorists, people engaged in serious crime or other people under investigation by the police or other authorised agencies, and where the required data was not already being retained.

Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

48. The Bill provides for law enforcement and intelligence agencies to have access to communications data. The Government is reviewing other public authorities who currently have access to communications data, in order to determine whether they should be able to continue to obtain it. Only where the Government believes there is a continuing, legitimate case for a public authority to continue to have access will they propose this to Parliament. We have written to all those public authorities who have access at present, asking them to provide a business case for their continued access. A summary of the outcome of this review will be provided separately in due course.

49. The 2011 report of the Interception of Communications Commissioner explains which agencies make use of communications data, including law enforcement and intelligence agencies (around 99%), the Financial Services Authority (around 0.48%), Local Authorities (0.4%) and other users (around 0.22%). A list of those public authorities who can access CD is set out in a consolidated order, last approved by Parliament in April 2010, as per Annex D. This followed a public consultation on which authorities should have access to these powers.

50. The draft legislation permits the Secretary of State, by Order, to add and remove public authorities from the list of those who are allowed to obtain communications data. Once the Government has assessed the case for other public authorities to continue to access communications data, it would in principle be possible to list those authorities in the draft Bill itself. If, however, there were no power in the Bill for the Secretary of State to amend the list of authorities by Order, any future changes would require primary legislation, significantly reducing the flexibility of the legislation. There may be legitimate reasons in future for removing public authorities from the list; or adding them if, for example, new bodies are created or functions are transferred between public authorities. An order-making power, subject to affirmative procedure, should ensure that the list of public authorities with CD powers can be kept up to date while providing Parliamentary scrutiny of any changes.

51. The requests for communications data from public authorities other than law enforcement and intelligence agencies account for around 1% of the total. But many of these organisations regard communications data as vital to meeting their responsibilities in investigating crime and protecting the public.

USE OF COMMUNICATIONS DATA

Are the circumstances under which communications data can be accessed appropriate and proportionate? What kind of crimes should communications data be used to detect?

52. We are confident that the specified circumstances in which requests can be made for communications data are appropriate and proportionate. The police and other authorised public authorities can only access communications data for the permitted purposes that are set out on the face of the Bill, and in any given case only when it is necessary and proportionate to do so. These purposes have to be approved by Parliament and are entirely consistent with Article 8(2) of the European Convention on Human Rights (ECHR). Article 8 of the ECHR is the „Right to respect for private and family life". Article 8(2) states that „There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the pretention of the rights and freedoms of others." Rather than including the broad purpose of the „protection of the rights and freedoms of others" and „the protection of morals", the proposed purposes in the Bill are more specific and tightly defined, whilst remaining consistent with the broader Article 8 purpose.

53. The vast majority of CD requests fall under purposes at clause 9(6)(a) and (b) of the draft Bill – „in the interests of national security" and „for the purpose of preventing or detecting crime or of preventing disorder" – and 99% of requests for communications data are made by the law enforcement and intelligence agencies.

54. An illustration of why requests might be made under the other purposes, and which organisations might make them, is included at Annex E.

55. The Committee has asked whether the use of communications data could be limited, either through reducing the number of statutory purposes, or by limiting those purposes – for example by limiting the „crime" purpose to investigations of „serious crime". It would be challenging to define a threshold for those crimes that are sufficiently serious to merit the use of communications data. There is no standard definition of „serious crime" in UK or EU law – there are a range of definitions based on the likely sentence a person being investigated might receive; whether the criminal activity involves violence or substantial financial gain; or the minimum penalty (normally a term of imprisonment) that a person could receive if convicted of a particular crime.

56. The Government's 2011 review of counter-terrorism powers set a threshold for the use of directed surveillance by Local Authorities in order to prevent the use of these powers for investigations into trivial offences. In that case, the review rejected an approach based on a list of crimes, not least given the challenge of maintaining such a list over time and instead set a restriction based on a custodial threshold (6 months).

57. It would be possible but, in the Government's view, complex and damaging to set a threshold for the use of communications data. A minimum three year custodial sentence, for example, would exclude using communications data in investigations into crimes where there is a legitimate case for doing so, including harassment; intentionally causing harassment, alarm or distress; immigration offences such as illegal entry to the country; supplying firearms or ammunition to a person under 18; and aggravated vehicle taking. Common law offences such as kidnapping or false imprisonment do not have a maximum penalty in statute and would have to be considered when formulating such a threshold. Those offences falling below such a threshold would also include crimes that often cannot be investigated at all without the use of CD, including online fraud, fake ticketing websites and some forms of harassment. Economic crimes may be seen as low-level, but left undetected can have a detrimental impact on consumers and business practice in the UK. Crimes such as harassment may be categorised as "non-serious" but can be extremely distressing for the victim and can escalate into more serious crime.

58. Limiting the use of CD to serious crime (however defined) would therefore impact on investigations into crimes whose impact on victims can be serious and make some investigations effectively impossible to mount. Such limitations would also affect serious investigations. CD is often used at the start of an investigation when the police may not know which specific offence(s) will later be the focus of any prosecution. Investigations into apparently lower level crime can often lead to more serious offences coming to light – without the benefit of access to CD in the initial investigations, these more serious offences may not be investigated.

59. From a legal/human rights perspective, Article 8 of the ECHR does not prescribe a level of seriousness of crime that must be met before the right to a private life can be restricted. The key consideration is whether such interference is necessary for the specified purpose of preventing disorder or crime and proportionate to what is sought to be achieved.

SAFEGUARDS

Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should 'designated senior officer' be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

60. There will be robust – and satisfactory – safeguards at every stage of the communications data process, including data acquisition. These are consistent with Article 8 of the ECHR, in keeping with the existing legislation relating to data acquisition, under the Regulation of Investigatory Powers Act 2000 (RIPA).

61. Part 2 of the proposed legislation preserves the essential elements of Chapter 2 of Part 1 of RIPA, which was enacted in order to provide public authorities with a human rights compliant framework for acquiring communications data. The substantive protections of Article 8 contained in RIPA will continue to be guaranteed by the strict purpose limitation for the acquisition of communications data, the built-in consideration of necessity and proportionality in each case, and numerous other safeguards (as at paragraph 52).

62. Communications data may only be acquired for a specific purpose set out in primary legislation (such as preventing or detecting crime, in the interests of national security or for the purposes of preventing death or injury in the case of an emergency).

63. Communications data may only be acquired by public authorities that have been approved by Parliament. The Bill sets out four categories of public authority – the police, Serious and Organised Crime Agency/National Crime Agency, Her Majesty's Customs and Revenue and the intelligence agencies – to be granted access to communications data. Other public bodies who currently have access to communications data will only continue to do so if they are added by Order, subject to debate and approval by both Houses of Parliament.

64. Each of these public authorities has a strict authorisations process in place for each individual request for communications data – including clearance by a Designated Senior Officer (DSO). The Bill ensures that Parliament will approve which public authorities can access communications data, for what purpose and the authorisation levels required (as they have done for the present regime, approving the Regulation of Investigatory Powers (Communications Data) Order 2010).

65. We anticipate the stipulated ranks of DSO to be the same as under the current Order, given the extensive consultation that contributed to its drafting.

The statutory instrument that will set this level of authorisation would be a negative order, but in practice any Order specifying the rank of a DSO will almost certainly also designate relevant public authorities and impose restrictions on the exercise of the Part 2 powers, so will most likely become subject to the affirmative procedure, as was the case with the 2010 order.

66. The Designated Senior Officer may only authorise a request for communications data if the applicant can demonstrate that the data is necessary for an investigation and the amount of data requested is proportionate to the objective of the investigation. DSOs are trained in considering the Article 8 (right to a private life) impact of acquiring communications data and must balance interference with privacy against the specific benefit to the investigation or operation being undertaken. These considerations are set out in existing legislation and further guidance is provided in the existing Communications Data Code of Practice. Should the Bill be passed, Parliament would have the opportunity to approve a new Code of Practice. The Government believes that the role of the Designated Senior Officer is, and will be, effective in providing scrutiny of communications data applications and that the application process is thorough and comprehensive.

67. Communications data requests approved by Designated Senior Officers are subject to oversight by the Interception of Communications Commissioner, including through inspections of public authorities. He provides a (published) annual report to the Prime Minister. The Commissioner has not to date identified any wilful and reckless abuse of these powers by those in public authorities. The independent Investigatory

Powers Tribunal provides individuals with an avenue for complaint if they think the powers have been used unlawfully. The tribunal has the power to order the destruction of data or award compensation if wrongdoing is found.

68. Under the proposed legislation, the role of the Designated Senior Officer is supported by a proposed Request Filter. The purpose of the Request Filter is to automatically obtain, process and analyse communications data needed to answer more complex data requests where data from different communications services providers might be required. The Request Filter will ensure that, after processing, only the key communications data is passed to a public authority and data irrelevant to the investigation is destroyed. By using the Request Filter to automate the analysis, the amount of data passed to public authorities will be minimised, reducing the levels of intrusion and protecting privacy. Without these filtering arrangements, public authorities are likely to need to make many more requests to CSPs in future and would need to piece the communications data together in-house, with implications for personal privacy and data protection.

69. The Request Filter will also support the Designated Senior Officer in determining whether the data for which an application has been made is likely to be available, and what data is likely to be necessary to answer the request. This will enable a more informed decision about proportionality. If a request is then made, the Request Filter will increase the Designated Senior Officer's ability to assess the Article 8 issues arising from the processing of personal data by the CSP; and it will act to reduce the potential impact on Article 8 of the use of communications data where processing or collation may be required.

70. We would emphasise that the Designated CD Senior Officer is only one part of a complex set of safeguards which govern retention, acquisition and transmission from a CSP to a public authority of CD. Most communications data is personal information and is, therefore, subject to the same general data protection safeguards (such as the Data Protection Act 1998) as any other personal information at any stage of its journey. As at paragraph 17, Parliament will debate and approve the Order stating what kind of obligations may be imposed on communications services. Requirements will then only be imposed following consultation with the company concerned and where it is considered to be reasonable and justified by the expected benefits to public protection. And, as at paragraph 76, statutory oversight will continue to be provided by both the Interception of Communications Commissioner and the Information Commissioner.

Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

71. In UK law, specified law enforcement and security agencies obtain a warrant to intercept the content of a communication. The warrant (providing background to the application) is submitted to the Home Secretary, who must approve the application.

72. In setting the procedures and safeguards in relation to interception and communications data, Parliament has consistently taken the view that interception of the content of a communication is significantly more intrusive than acquiring information about a communication. The European Court of Human Rights has similarly taken the view that communications data is less intrusive than interception. For that reason, a warrant signed by the Secretary of State is required to intercept the content of a communication, but not to obtain communications data. In any case, it would not be logistically possible for a Minister (or Ministers) to approve warrants for communications data, given the number of applications each year and the frequency with which data is used in criminal investigations. This would also have a significant operational impact on the ability of the police and intelligence agencies to operate at the pace demanded by their investigative work.

73. A system of judicial authorisation has been introduced for local authorities in response to specific concerns about their operating practices. But local authority requests for communications data also only constitute about 0.4% of total requests each year. It is, therefore, logistically possible to submit these requests to a magistrate. It would require a major increase in the number of magistrates available across the country, 24/7, to approve CD requests from other authorities. Some magistrates would need to receive security vetting. There would be operational risks in the police and intelligence agencies having to disclose sensitive secret material to local magistrates and there could be implications for operational effectiveness. In some less urgent cases, requests could await magistrate approval for some time with the risk that data could be destroyed before approval was given, particularly if the request was for data approaching 12 months old.

74. The financial costs of such a system would be significant. Based on projected costs for magistrate approval of Local Authority requests, the magistrate costs for other public authorities would be around £60m per annum, not including IT or additional accommodation. Staff from public authorities would be required to present cases for approval. An initial estimate of costs across public authorities for the additional staff required would be at least £10 million, potentially far higher. It may be challenging for public authorities or central Government to meet such costs in a tight resource climate.
75. Introducing judicial authorisation for this power would also represent a significant change to our criminal justice system and the relationship between police, intelligence agencies and the judiciary.
Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?
76. The Government believes that the roles of the two Commissioners in the communications data process are coherent and consistent. The Government also believes that the Commissioners will provide effective oversight of the new communications data regime.
77. The legislation will provide for the Information Commissioner to keep under review the security and integrity of communications data retained by CSPs under the Bill to ensure the data is protected against accidental loss, unlawful destruction, unlawful retention and unauthorised disclosure. The Information Commissioner must also keep under review the specific requirement under the legislation to destroy data when its retention is no longer lawfully authorised (for example, at the end of the maximum retention period of 12 months specified under the new provisions). CSPs and the Secretary of State will be required to keep a sufficient record of things done under the Bill to enable the Commissioner to effectively discharge his functions.
78. The Interception Commissioner will continue to provide independent oversight of the acquisition of communications data by public authorities. The Commissioner's role will be extended to oversee the collection of communications data by communications service providers and the operation of the filtering arrangements. This will include oversight of testing, regular auditing and inspections. The Interception of Communications Commissioner must be a serving or retired senior member of the judiciary. He must report annually to the Prime Minister on how he has carried out his duties. His report is published and laid before Parliament.
79. The Interception of Communications Commissioner is supported by a Chief Inspector and five inspectors, who are all highly trained in the processes and the extent to which communications data may assist public authorities in carrying out their functions. The inspectors undertake a revolving programme of inspection visits to public authorities who are authorised to acquire communications data. The inspections take between one and five days, depending on the level of access the public authority has been granted under the Act, how frequently they are using their powers to acquire communications data and their previous level of compliance.
80. In 2011, 99 individual public authorities were inspected by the inspection team and a further 77 local authorities were inspected during the inspection at the National Anti-Fraud Network (NAFN), which provides a Single Point of Contact service for many local authorities. The findings of the inspections are reported in the Commissioner's Annual Report to the Prime Minister. The Interception of Communications Commissioner will fully investigate how and why the errors occurred and must be satisfied that the CSP or Public Authority has put in place measures to prevent the same errors occurring in the future.
81. The Interception of Communications Commissioner regularly makes recommendations to public authorities where he has identified compliance issues. The Commissioner reports as necessary on the action taken by public authorities in response to recommendations. Where serious issues have been identified, a re-inspection will follow shortly thereafter in order to check compliance. If his concerns are not addressed, the Commissioner could write to the Home Secretary recommending that the powers be withdrawn from that authority by Parliament, but it has never been necessary to take such a step.
PARLIAMENTARY OVERSIGHT
Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?
82. Parliament has a number of routes to conduct oversight of the powers in the draft Bill. In addition to the work of this Committee, Parliament will debate the Bill during the passage of the legislation. Parliament will also approve the secondary legislation delegated under the Bill, including the Order under Clause 1, the

granting of access to CD to any further public bodies, the purposes for which they can acquire CD, and the restrictions and authorisation levels imposed. Clause 1 of the Bill allows for notices to be served, imposing specific requirements on specific CSPs. These notices will be tailored to each system and service, and will describe the data that must be retained; illustrative details of what they may include are outlined at Annex F. Parliament will approve the Code of Practice that will be required to cover the entire Bill under the affirmative procedure.

83. The Interception of Communications Commissioner and the Information Commissioner will lay before Parliament annual reports on the performance of public authorities and CSPs.

84. We would also anticipate that Parliamentary Committees with an interest in these issues (including the Home Affairs Select Committee and the Joint Committee on Human Rights) may monitor the implementation of this legislation over the longer term.

85. There are a number of other delegated powers in the draft legislation. The Delegated Powers memorandum was published with the draft Bill. It identifies the provisions of the Bill that confer powers to make delegated legislation, and explains in each case why the power has been taken and the nature of, and reason for, the procedure selected. The Bill will be subject in the normal way to scrutiny by the Delegated Powers and Regulatory Reform Committee.

ENFORCEMENT

Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

86. The Government believes that the powers in the Bill are sufficient to ensure that CSPs comply with any requirements that are legally placed upon them.

87. Part 1 of the Bill will allow the Home Secretary, when necessary, to require communications service providers to retain CD where they would not otherwise retain it for business reasons. These new requirements will be subject to consultation with Ofcom, any company likely to be affected and the joint Government-industry Technical Advisory Board. The Secretary of State will set out these detailed requirements on a service provider in a notice. It is the duty of a CSP, enforceable by civil proceedings, to comply with a requirement imposed by a notice. Under Part 2 of the Bill, providers are obliged to obtain and disclose communications data to public authorities in pursuance of an authorised notice. It is the CSP"s duty to comply with this requirement unless it is not reasonably practicable to do so. The mechanisms for enforcement are the same as under Part 1. If a communications service provider is concerned about the requirements placed upon them, they can ask the Technical Advisory Board to consider the impact of these obligations. The Board can make recommendations to the Secretary of State following which he or she can modify, maintain or repeal the notice.

88. The Secretary of State may bring civil proceedings for an injunction or other appropriate relief in the event of a provider's non-compliance with obligations placed on it. It is a civil contempt of court to refuse or neglect to do an act required by a judgment or order of the court. A judgment or order against a corporate body may be enforced by an order of committal against the directors or other officers of the corporation. The court may also give leave for the issue of a writ of sequestration against the property of the corporation or any of its directors or officers. This could lead to a fine or imprisonment.

How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

89. We believe the plans are robust and our enforcement mechanisms – which will always be a last resort – are credible. The Bill enables requirements to be placed on overseas providers: the definitions of systems and services in the legislation do not contain any geographical or territorial limitations, so are not dependent on the location of the provider. The enforcement mechanisms for overseas providers in the event of non-compliance with a requirement are, therefore, the same as for domestic. We seek a collaborative approach with overseas providers, who generally have a good understanding of the UK processes and oversight for acquiring CD. The new legislation would facilitate that by allowing us, for instance, to offer cost recovery to overseas CSPs.

90. In the event that an overseas provider was not prepared to co-operate in providing the communications data we need, two options would be open to the Government: a) collecting the required CD from UK networks; or taking enforcement action through UK courts. We believe that a provider with substantial interests in the UK is unlikely to wish to be in contempt of an order of the court.

Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

91. The Code of Practice sets out detailed guidance on the acquisition and disclosure of communications data. Wilful or reckless conduct (as set out below), which also amounts to a breach of the Code, will already constitute an offence. To introduce a new offence for other types of errors made by officers in public authorities while seeking to acquire communications data will criminalise errors made by officers acting in good faith. We do not believe a bespoke offence is necessary, particularly given the lack of evidence that the system is being abused by those with access to CD. It is better to ensure comprehensive and regular training is in place for those acquiring communications data; combined with a rigorous inspection regime that identifies and reports errors, ensuring that they are addressed.

92. Offences exist on the statute books and in the common law to address situations where public officials, and other individuals, abuse access to personal data. In many cases, the obtaining of personal information is likely to be part of a course of conduct involving criminal activity such as misuse of computer systems and hacking, all of which are offences. The relevant offences, depending on the context, include: Unauthorised access to computer material, contrary to Section 1 Computer Misuse Act 1990 which carries a maximum sentence of two years" imprisonment. Unauthorised access with intent to commit another offence, such as fraud, contrary to section 2 Computer Misuse Act 1990 which carries a maximum sentence of five years' imprisonment. Knowingly or recklessly obtaining, disclosing or procuring the disclosure of personal data without the consent of the data controller under Section 55 of the Data Protection Act, which carries a maximum penalty of an unlimited fine. The common law offence of misconduct in public office. It is committed when the office holder wilfully acts (or fails to act) in a way that he knows is wrong and is calculated to injure the public interest. The maximum penalty for this offence is life imprisonment.

93. In addition, there are also a number of offences which may be relevant depending on the context, including offences of bribing another or being bribed contrary to the section 1 or 2 of the Bribery Act 2010. Where the offences were committed prior to the coming into force of the Bribery Act 2010, relevant offences include corruptly accepting money or other advantage contrary to section 1 of the Prevention of Corruption Act 1906 for which the maximum penalty is seven years' imprisonment.

94. The Interception Commissioner's 2011 report notes that he was satisfied that, where compliance issues were identified, „these occurred due to genuine misunderstandings, rather than any wilful or reckless failure to comply" and he has already been assured that the „necessary corrective action has been taken by these public authorities." Since 2005, the Commissioner has identified only one case where data was requested that should not have been disclosed as a matter of law under one of RIPA"s statutory purposes.

95. We know that ACPO has consulted with forces across the country to identify cases of wilful misuse of communications data by police officers and staff. To date, they have identified no additional examples of wilful and reckless misuse, further to the case they outlined in their oral evidence to the Joint Committee on 12 July, where the data had initially been obtained lawfully.

COSTS AND BENEFITS

Is the estimated cost of £1.8bn over 10 years realistic?

97. The estimated cost over the ten years to 2020/21 is taken from the most recent business case for the programme, approved by HM Treasury in June 2011. The business case described what needs to be done to maintain capability to access communications data before and after the introduction of new legislation. Further details on the costs and benefits, including responses to the specific questions posed by the Committee, are given in Annex G.

98. The cost estimates in the 2010/11 business case are based on assumptions about the roles of certain technologies, law enforcement and agency capabilities and the telecommunications market. The main assumptions were informed by independent research and surveys, and best practice across the telecommunications industry: Communications traffic continues to grow year on year and we need to work with more CSPs. The total volume of internet traffic increases by a factor of ten over the 10 year period with storage volume increasing in proportion. CSPs are required to retain communications data for up to 12 months. Per unit data storage costs continue to decrease by 25% per annum. Technology will be upgraded or renewed as appropriate on a five year cycle in line with the telecommunications industry.

99. The estimates in the 2010/11 business case represent a highest cost scenario. It is difficult to estimate costs with precision over the long term. The programme has an incremental approach to developing capabilities, which takes account of changes in technology, the communications market and the investigative capabilities of law enforcement and intelligence agencies.
100. The programme business case is currently undergoing a formal regular review which will produce revised costs and benefits. The revised business case will inform a new Impact Assessment to be published before the Communications Data Bill is introduced formally in the House. Parliament will then have the opportunity to consider again the latest costs and benefits of the programme enabled by the Bill.
101. The technology delivery aspects of the programme have recently been reviewed by the Major Projects Authority in the Cabinet Office who have endorsed the Programme's approach.
102. The Home Office has provided for the programme business case in its spending plans until March 2015, after which it will be subject to further scrutiny as part of the next spending review
The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?
103. As the impact assessment sets out, the estimate of benefits of £5–6 billion over the ten years to 2020/21 relates to the programme and is taken from the programme business case approved by HM Treasury in June 2011. The programme includes a number of areas of work under existing legislation.
104. The approach taken to estimating benefits in the business case is consistent with best-practice HM Treasury „Green Book" methodology1. The Home Office Chief Scientist accepted the methodology, and Home Office economists, with support from statisticians from across government, helped to construct the estimates. The methodology is described in the appendix to Annex G.
105. The estimated benefit of £5 – 6 billion over ten years is the value added by the programme. We regard this as cautious. Only benefits that can be ascribed a monetary value with confidence are considered in the business case. These are revenue loss prevented; assets seized; lives saved; children safeguarded; and paedophile rings disrupted.
106. Other benefits could not be subscribed a monetary value with confidence and therefore were not included in the business case including benefits from illegal drugs seized, terrorism prevented and operational efficiencies through the use of communications data to target law enforcement resources more efficiently.
107. Furthermore, the business case only costed the benefits derived by a representative sample of 13 organisations using communications data and not every organisation that does so. No projections were made or costs added for other organisations
108. Like costs, benefits from the programme will be subject to change and are being reviewed as part of the revised business case.
1 The Green Book is a best practice guide for all central departments and executive agencies, and covers projects of all types and size. It aims to make the appraisal process throughout government more consistent and transparent.
TECHNICAL
Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?
109. CSPs already identify, collect and hold communications data relating to their own services. We are confident that the technology we and CSPs would be using can distinguish between communications data and content. This technology is not new and is already commercially available. Any specific technologies we might use would be thoroughly tested before deployment and monitored carefully afterwards. The purpose of this legislation is not to obtain communications content and it would not be lawful to do so. The technology must understand the data if it is to collect it. It will not do so if, for example, the format of the data means that it is it is not possible to distinguish communications data from content (for instance, if encryption means that parts of the communication cannot be recognised).
110. Where practical, CSPs may use their existing suppliers and solutions to collect required CD from their networks. A number of UK and international suppliers provide specialist DPI equipment. We are confident that CSPs and industry can provide a CD collection capability, and will work with them to procure a sustainable network collection capability. Manufacturers who provide DPI equipment to the global telecommunications sector include: Acme Packet Inc; AdaptiveMobile Ltd; Advanced IO Systems; Alcatel-Lucent; Arbor Networks Inc.; BAE Systems Detica; Bivio Networks Inc.; Bridgewater Systems Corp.; Cisco;

Cloudshield Technologies; Endace; Huawei; IP Fabrics; Ipoque; Juniper; Niksun; Procera Networks; Radware; Roke Manor; Solera Networks; Symantec; Tilera; Unipier; TRL; and Verint.

How safely can communications data be stored?

111. There is a good track record, over a period of nearly a decade, regarding the security of communications data retained by the CSPs, both for business purposes and the Data Retention Directive.

112. As part of their Data Protection Act obligations, CSPs must already protect personal data stored for business purposes from loss, theft or unauthorised disclosure. The Government has worked closely with CSPs to ensure that the process for the retention and disclosure of CD to Public Authorities is secure and over the last 3 years has invested to protect the transmission of communications data. We have, for example, connected UK CSP disclosure systems to secure, accredited Government networks, in order to fully protect the transmission of CD requests and responses. All major network providers strictly manage the security of their networks, routers, switches and management equipment; the CSPs will ensure that any collection equipment deployed on their networks will, as a minimum, be subject to the same security and access controls. The proposed legislation gives the Government the ability to ensure that data is held by CSPs in a manner accredited to our Information Assurance standards, maintaining the high existing standards in place.

Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

113. Internet communications services are technically different from the telephone services of the past. The communications data now needed to understand the „who, how, when and where" of a single communication may no longer be held by a single communications provider. The Filter is intended to enable law enforcement agencies to continue acquiring complex CD in a way that minimises collateral intrusion. We are confident in the availability of technology to process and filter communications data in the way proposed. We believe the provisions relating to the Request Filter are set out clearly on the face of the Bill.

114. It may be helpful to illustrate how we expect the Request Filter would work in practice. During a live terrorist investigation, if a law enforcement agency wanted to identify a suspect who they know was at two separate locations at two specific times, they might currently need to submit separate requests to obtain a full list of all those devices at each location, then compare these lists to see which one was in both locations. Under the proposed arrangements, the agency could submit the request to the filter, which would send requests to all CSPs holding relevant location information. The filter would then automatically analyse these returns without human intervention. Once the analysis had taken place, only the details of devices which were active in both areas at those times would be sent back to the investigating officer. The filter would then delete all the data, merely retaining an audit trail of the request.

115. The Bill makes the Secretary of State responsible for setting up and maintaining any filtering arrangements and provides the power to transfer this to a designated public authority. Day to day operation of the filtering arrangements may be carried out by an approved body.

116. The filtering arrangements will be overseen by the Interception of Communications Commissioner. The Commissioner will audit the operation of the filtering arrangements to ensure: all use is correctly approved by authorised public authorities; that the Filter only acquires necessary authorised data from CSPs; and that once the processing and filtering to answer a request is complete all acquired communications data is immediately destroyed.

117. It will be possible to manually check that the Filter had functioned correctly (to ensure that the result is sound) and there will be an audit trail of filter requests. Automated systems, such as the Request Filter, should minimise intrusion and reduce the risk of errors which arise from human error. If, however, a public authority had concerns that the returned results from the Filter were incorrect, a manual check of the audit trail of the Filter request could be undertaken. The Draft Bill includes new obligations on the Secretary of State and the Interception Commissioner to monitor the operation of the filter (including frequent testing), in order to continually demonstrate that it is providing accurate results.

118. The Request Filter will not separate content from CD. It will only filter CD that has already been retained by CSPs. Nor is it a central database. The legislation makes clear that the Filter can only acquire and process communications data to answer a specific public authority request. Once that request has been answered the Filter will permanently delete all the communications data it acquired.

How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?
119. Criminals and terrorists are always seeking new ways to try to evade detection by the police and others. Law enforcement and intelligence agencies have always had to respond to changes in criminal behaviour. There are obfuscation techniques which can make tracking criminal groups more difficult, and sometimes a combination of capabilities may be required to tackle these effectively. This legislation will put the UK in a good position to manage these challenges. There are inevitably limits to what we can say publicly about the techniques to tackle these problems because to do so could help criminals – including terrorists – evade detection.
Are there concerns about the consequences of decryption?
120. The encryption of communications can have a significant impact on the investigation of all forms of crime and, like other countries, we are constantly developing our response to the challenges which it can pose. The purpose of this legislation is to facilitate closer cooperation and collaboration with CSPs in the UK and overseas, and enable the police and others to access the data they require. Collaboration and access to data are essential if we are to manage the challenge of encryption. This legislation is entirely consistent with work required to deal with encryption and the UK"s cyber-security strategy.
ANNEX D
List of public authorities listed in the Regulation of Investigatory Powers (Communications Data) Order 2010 Ambulance Services Care Quality Commission Charity Commission Child Maintenance and Enforcement Commission Civil Nuclear Constabulary Criminal Cases Review Commission Scottish Criminal Cases Review Commission Department of Agriculture & Rural Development in Northern Ireland Department for Business, Innovation & Skills (BIS) Department for Environment, Food and Rural Affairs Department of the Environment in Northern Ireland (DOENI) Medicines & Healthcare Products Regulatory Agency Department for Transport – Accident Investigation Branches Dept of Transport – Driving Standards Agency Maritime and Coastguard Agency Department for Transport – Vehicle Operators Services Agency Department for Work and Pensions Environment Agency Glasgow City Council (where the majority of Scottish Local authority CD Requests are made.) Scottish Environment Protection Agency Financial Services Authority Fire and Rescue Services Food Standards Agency Gambling Commission Gangmasters Licensing Authority General Pharmaceutical Council (formerly The Royal Pharmaceutical Society of Great Britain) Health and Safety Executive Office for Standards in Education, Children's Services and Skills (Ofsted) UK Border Agency Home Office Immigration Removal Centres Independent Police Complaints Commission Information Commissioner Local Councils – Local Government Regulation Ministry of Justice – National Offender Management Service and Contracted Out Prisons National Anti-Fraud Network (NAFN) NHS Services Northern Ireland Local Government Association Northern Ireland Prison Service Ofcom Office of Fair Trading Pensions Regulator Police Ombudsman for Northern Ireland (PONI) Port of Dover Police Port of Liverpool Police Postal Services Commission Royal Mail Serious Fraud Office Welsh Local Government Association
ANNEX E
Use of Communications Data – Purposes
This annex sets out the purposes for which communications data requests may be made and indicates who might make them. All the organisations mentioned below have been asked to submit business cases to support their continued access to communications data and we will assess whether they have an ongoing requirement in due course.
a) in the interests of national security
The Intelligence agencies protect the UK from threats to national security (including terrorism and espionage) and helps counter proliferation of weapons of mass destruction. They use communications data to enable them to identify, assess and counter these threats.
b) for the purpose of preventing or detecting crime or of preventing disorder
Law enforcement agencies and the police primarily request communications data to support the prevention and detection of crime.
c) for the purpose of preventing or detecting any conduct in respect of which a penalty may be imposed under section 123 or 129 of the Financial Services and Markets Act 2000 (civil penalties for market abuse),
This purpose is required to cover the responsibilities of the Financial Services Authority (FSA). The FSA conducts investigations into criminal and civil offences. The former are covered by purpose b). The latter are currently covered by the Financial Services and Markets Act (FSMA) but the FSA"s power to request

communications data under this Act will be removed by the Communications Data Bill as part of the streamlining of legal bases on which communications data may be acquired. There is a legal obligation to provide such powers. Under the EU Market Abuse Directive the UK is required to ensure that the Financial Regulator (in this case the FSA) has appropriate investigative and enforcement powers in order to carry out its functions, including the right to acquire communications data. Were this not to be provided for, the UK could face infraction proceedings.

d) in the interests of the economic well-being of the United Kingdom

As part of their mission to protect the UK and its interests, the intelligence agencies may request communications data under the purpose of economic well-being. The agencies seek to protect the UK from those who might wish to destabilise the economy in ways which could cause serious harm to the prosperity of the UK.

e) in the interests of public safety

The Air Accident Investigation Branch, the Marine Accident Investigation Branch and the Rail Accident Investigation Branch are all administratively part of the Department for Transport, but function independently in the conduct of their investigations. Their primary purpose is to determine the cause of accidents with a view to preserving life, improving safety and preventing future accidents – not to apportion blame or liability. They may apply for communications data under this purpose because an integral part of their investigations is ascertaining whether the use of telecommunications by drivers, pilots or others played any part in the incident (which may include loss of life).

f) for the purpose of protecting public health

The Health and Safety Executive (HSE) is the enforcement authority for most work-related health and safety legislation. It investigates and prosecutes offences which involve the creation of serious risks to people"s health and safety such as poisonings, explosions from faulty domestic gas installations, major chemical incidents, movement of dangerous goods and construction site injuries etc. The HSE obtains communications data in order to trace and investigate individuals or businesses whose activities may be putting people at risk of serious harm, or where mobile phone use may be among the causes of an incident.

g) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department

HM Revenue and Customs (HMRC) uses communications data in connection with policing/assuring a wide range of UK revenues, taxes and duties, as well as protecting the public at the border by combating the smuggling of prohibited, restricted and duty payable items. This is necessary to tackle the avoidance of millions of pounds of duties and taxes on goods and attacks on the self-assessment and tax credit systems, where organised crime gangs with false identities use multiple claims to obtain large repayments. Although HMRC may make requests for communications data under this purpose, many of their requests may also fall under purpose (b) because of the criminal offences involved.

h) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating an injury or damage to a person's physical or mental health

The Maritime and Coastguard Agency is an on-call emergency organisation responsible for the initiation and co-ordination of all search and rescue operations within the waters for which the UK has responsibility. This includes using communications data to locate and respond to missing vessels at sea, persons either in distress at sea, or to persons at risk of injury or death on the cliffs or shoreline of the UK (where HM Coastguard has a statutory responsibility to co-ordinate a response to save life or prevent injury).

i) to assist investigations into alleged miscarriages of justice

The Criminal Cases Review Commission or Scottish CCRC may make requests for communications data under this purpose to support their investigations into alleged miscarriages of justice. The Criminal Appeal Act 1995 and the Criminal Procedure (Scotland) Act 1995 provide for the Criminal Cases Review Commission and the Scottish Criminal Cases Review Commission respectively to investigate alleged miscarriages of justice. They affirm the safety of convictions, thus reinforcing everyone's right to a fair trial under ECHR and promoting confidence in the effectiveness of the criminal justice system. Communications data enables the Commissions to determine salient facts to support or undermine assertions made by people claiming wrongful conviction. This includes verifying an applicant's location at the time of the crime or proving/disproving that a call was made at the material time.

j) where a person ('P') has died or is unable to identify themselves because of a physical or mental condition—
(i) to assist in identifying P, or
(ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition.
Communications data could be requested under this purpose in order to deal with cases where it is otherwise not possible to identity a person caught up in a natural disaster. Communications data relating to such a person"s mobile phone may be the only means of identifying him/her. Communications data may be requested under this purpose to identify a home address for the victim or the last person they may have been in contact with in order to identify a next of kin. For example, communications data may be requested under this purpose by police forces (including the British Transport Police) and the Serious and Organised Crime Agency (SOCA).

HMRC

HMRC is the UK's tax authority. It is responsible for safeguarding the flow of money to the Exchequer through its collection, compliance and enforcement activities. The department also administers the payment of benefits and credits to those requiring financial support. In 2011/12 HMRC collected £474.2 billion in taxes and paid out over £42 billion in benefits and credits.

The flow of such large sums of money across HMRC's tax and benefits systems inevitably makes the department a target for predatory and sophisticated Organised Crime Groups (OCGs) attracted by the prospect of financial gain.

The threat to the revenue from OCGs applies equally across the full range of tax systems. Examples include sophisticated and sustained attacks against online direct tax regimes such as Income Tax Self Assessment by OCGs operating in the cyber-crime arena; indirect tax frauds such as cigarette and tobacco smuggling, alcohol smuggling (and diversion); hydrocarbon oils smuggling (and laundering) and VAT (including Multi Trader Intra Community - MTIC fraud). To combat this criminal activity HMRC deploys the full range of intelligence gathering capabilities including the acquisition of communications data (CD) which features in the overwhelming majority of our criminal prosecutions.

CD provides intelligence to support operational activity leading to arrests, and seizures of money and contraband. It is also adduced in evidence to support criminal prosecutions.

General:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

Yes. The EU Data Retention Directive does not impose an obligation on UK Communications Service Providers (CSPs) to retain data they otherwise would not retain as part of their normal business processes. This means that certain categories of communications data – particularly in relation to offshore CSPs - are not available to support investigations into criminal activity.

In some cases we are able to obtain this material under the provisions of mutual legal assistance treaties but this is a cumbersome, bureaucratic and, above all, slow process that prevents any real-time investigation of crime and provides no guarantee that the material requested will eventually be made available. The Bill will correct this situation by obliging UK CSPs to retain this data as it passes over their networks. The material will be held for no more than 12 months – in line with current legislation – and law enforcement agencies such as HMRC will only be able to obtain data that relates to a specific investigation as long as it is proportionate and necessary to do so. We fully support the aims of the objectives of the Bill.

A recent investigation highlights the difficulties we are currently experiencing. As part of an investigation into a £600 million Missing Trader VAT fraud chain we could not obtain from an overseas CSP the IP login histories of several key targets. As a consequence we were unable to identify links in the criminal conspiracy and we were unable to use CD to evidence association between conspirators during the subsequent court case.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

Yes. CD is a critical investigative and evidential tool for the law enforcement agencies. A degradation in this capability would put lives at risk and - as far as this Department is concerned – hinder our ability to identify and prosecute criminal gangs and individuals that attack the UK tax system.

Operation Tulipbox was a Missing Trader Intra-Community VAT fraud investigation which highlighted the importance of communications data. CD provided key intelligence to link targets, establish fraudulent trading patterns and rebut defence arguments. The trial concluded with sentences of 15, 14 and 9 years for the three co-conspirators. £10 million worth of assets were identified for confiscation, and we prevented a revenue loss of £91.2 million by identifying and closing down the fraudulent trading network. Perhaps more importantly, the strategic intelligence we gathered whilst conducting the investigation enable the Government to change the rate of VAT on the traded commodity to zero, thereby preventing other organised crime groups from exploiting the potential for fraudulent gain.

We would not have been able to achieve these results without access to CD and therefore maintenance of this capability is critically important to us.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

This Bill provides no new powers to law enforcement agencies. CD requests must be made in the context of a subject's 'Right to Respect for Privacy'. They must be necessary, proportionate and must take into account the degree of collateral intrusion. Furthermore, communications data is probably the least intrusive method of covert investigation. It seems oddly possible that if this Bill should fail, law enforcement agencies may have to rely on more intrusive methods of investigation to compensate for their inability to acquire relevant communications data.

COSTS:

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6 billion. Is this figure realistic?

Placed in the context of HMRC's view that CD was instrumental in protecting some £870 million of revenue in the last financial year then a predicted benefit from the draft Bill of between £5-6 billion spread across the wider law enforcement community over a ten year period seems a reasonable estimate.

All of our most serious crime investigations rely on CD to identify suspects, establish relationships within and between criminal organisations, and direct operational activity to evidence crime, seize contraband and criminal cash and make arrests.

As CD as an investigative tool degrades we may partially fill the gap with more costly and more intrusive forms of surveillance however it is unlikely that we will be able to fully compensate for the decline in the availability of CD without the proposed Bill. This, in turn, will have a significant impact on our ability to meet the challenging Spending Round targets that we have been set by the Government.

USE OF COMMUNICATIONS DATA

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

Yes. We use CD for two purposes only, the prevention and detection of crime and the assessment of tax. We use the former to support investigations into criminal attacks on the UK's tax systems. The latter represents less than 1% our total CD requests and is limited to subscriber checks only (RIPA s21(4)(c)) but is nevertheless a key tool in identifying those who owe substantial sums in tax.

15. Is the 12 month period for the retention of data too long or too short.

We believe the current UK data retention period of twelve months represents a fair balance between the needs of the investigator and the Article 8 rights of the individual. We note that it is in line with the position taken by the majority of our European partners.

SAFEGUARDS

17. Would a warrant system be more appropriate?

We believe that the current system strikes a good balance between the needs of the investigator and the safeguarding of sensitive and private information.

Across HMRC approximately 100 Higher Officers (equivalent to Inspector rank in the police) are accredited to authorise requests for subscriber data (RIPA S21(4)(c)). These so called 'designated persons' (DPs - RIPA Part 1, Chapter 2 Codes of Practice) receive specific training for their role along with continuous professional development in good practice and new guidance. They will be independent of any investigation requiring their authority to acquire subscriber data.

We have three Senior Officers (equivalent to Superintendent rank in the police) who can authorise more sensitive communications data (RIPA S21(4)(a&b)). They are experts in the acquisition of communications data and are ACPO accredited Single Points of Contact able to engage directly with CSPs. They are not attached to any operational team so they can be fully independent of any request they may have to authorise. They provide out of hours support to operations and are also responsible for reviewing the quality of the subscriber data authorisations by the Higher Officers.

A robust inspection programme overseen by the Interception of Communications Commissioner's Office (IOCCO) assures these processes. We are visited once a year by IOCCO who, during a visit usually lasting four to five days, will fully review the end-to-end application process, including the quality of considerations by the DP.

It is hard to envisage a system of judicial authorisation that can match the current level of scrutiny without adversely impacting on the efficiency and effectiveness of the investigation process. We are concerned at the potential for judicial authorisation to be a slower, and possibly less informed, process as well as raising some practical issues.

We would envisage that any hearing in respect of an application for communications would require the presence of the applicant to answer any questions that the magistrate may have.
Any questions in relation to the availability of the data requested, the processes for obtaining it and the potential additional data which could be obtained would require the additional presence of an accredited SPoC in court and possibly a representative of the CSP.
Would courts be prepared to sit at short notice or would there be specified days when courts handled communications data requests?
How would courts handle referrals? That is, those requests where there is a change of CSP or where the original notice was served and has not been complied with and needs to be reissued. Would there be automatic access to the original magistrate?
Would magistrates appropriately trained in CD be readily available to deal with the level of requests? Would such requests be managed geographically or would there be designated magistrates with a national remit?

Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

In our view, the Office of the Interception Commissioner provides effective and proven oversight of the provisions of RIPA Part 1 Chapter 2. The annual inspections are comprehensive and thorough and the

findings are published in the Interception Commissioner's annual report. Where deficiencies in an agency or force are detected, there is a requirement for the agency or force to respond with a detailed action plan to remedy the deficiency.

ENFORCEMENT

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

As the United Kingdom's tax administration, HMRC is keenly aware of the importance of policing access to sensitive information. The S.19 of the Commissioners of Revenue & Customs Act 2005 creates an offence of wrongful disclosure of revenue and customs information and it is a matter of record that we will take firm action against members of staff who acquire and misuse information to which they are not entitled, up to and including dismissal and prosecution.

We would have no objection to the insertion into the Bill of an offence of wrongful access to and/or misuse of communications data, should this reassure the public.

August 2012

ISPA

About ISPA

The Internet Services Providers' Association (ISPA) is the trade association for companies involved in the provision of Internet Services in the UK. ISPA was founded in 1995, and seeks to actively represent and promote the interests of businesses involved in all aspects of the UK Internet industry.

ISPA membership includes small, medium and large Internet service providers (ISPs), cable companies, web design and hosting companies and a variety of other organisations. Our members may be affected by the Communications Data Bill in various ways. ISPA currently has over 215 members, representing more than 95% of the UK Internet access market by volume. ISPA was a founding member of EuroISPA.

We have been involved in the area of communications data for many years, including the development of data retention provisions under both the Anti-Terrorism Crime and Security Act (2001) and the Data Retention (EC Directive) Regulations 2009 and ISPA members have great experience in handling RIPA requests.

Introduction

1. ISPA members accept that law enforcement agencies should have reasonable access to communications data in order to help in the detection and investigation of serious crime and to safeguard national security. However, any communications data regime needs to be workable for the industry and capable of earning user trust, as well as be proportionate and balance the requirements of law enforcement with both the level of intrusion in to users' privacy and the cost and burden placed upon communication service providers (CSPs).

2. We believe that the current regime performs fairly well, in particular the dedicated expertise in the Single Point of Contact System (SPOC), which has provided for an effective means of structuring the relationship between law enforcement authorities (LEAs) and CSPs. The current system also ensures that the costs that CSPs incur when they comply with requests can be reimbursed so that CSPs continued investment in innovation and service development has not, so far, been adversely impacted by data retention requirements. This also acts as a safeguard to ensure that law enforcement to only requests data where the cost can be justified. It is crucial that these elements continue as part of any future communications data regime.

3. As an association representing a variety of CSPs, ISPA has particular experience and knowledge of costs and burdens placed on CSPs. Below we will argue that a great deal of uncertainty surrounds the proposals and the main changes should be viewed as significant extensions to current capabilities. We have grouped our comments according to the themes raised in the Committee's call for evidence.

4. Industry needs clearer and more detailed information on what the proposals will actually mean in practice for different CSPs. They will have a significant impact on how the UK Internet is run and our members need to fully understand how this will affect them. We would urge the Committee to address the points summarised below with Government so that the whole data retention process is clear and proportionate.

Summary of main points

5. We accept that law enforcement should be able to access communications data in a changing communications environment, but this has to balance the requirements of law enforcement, privacy of users and the impact on business. It is not clear if the Draft Bill achieves this.

6. We welcome that cost recovery is included in the Draft Bill as it ensures a more effective system and reflects the fact that our members do not gain from retaining and disclosing communications data.

7. The Draft Bill has the potential to put the UK at a competitive disadvantage and destabilise the market, with the UK seen as a less attractive and more onerous place to do business digitally, affecting both inward investment and services being made available. In challenging economic times we question whether this should be a government priority.

8. In our view the Draft Bill amounts to a significant extension of the current capabilities and should be viewed as such. This is particularly true of the powers to capture and retain third party data and the filtering arrangement.

9. Due in part to the lack of detailed information made available, we are yet to be convinced that the proposals technically possible on the scale envisioned or that foreign CSPs will provide the necessary information to UK law enforcement.

10. The changing definitions of CSP and communications data have the potential to include a wider range of CSPs and data than previously.

11. Far too much discretion is given to the Home Secretary without the necessary Parliamentary oversight to ensure that significant changes proposed are proportionate and necessary. Parliament should be told what data will be retained, for what purposes and make sure that the necessary safeguards are in place to balance the differing interests of law enforcement, users and businesses.

General comments / requirements of law enforcement

12. ISPA members fully understand that the communications landscape is changing and that this warrants a review of the current communications data regime. However, we feel that that the Draft Bill is missing crucial detail, principally because of the number additional requirements that could be introduced by order, notice and regulations. A great deal more work needs to be done to explain what the current proposals will mean in practice. Whilst we understand that concerns about security and confidentiality may limit what can be revealed publicly and what can and cannot be written on the face of the Draft Bill, we feel that the current level of information makes it hard to undertake an adequate, in-depth assessment of the proposals. To help us fully understand the implications of what is being proposed, we would urge the Committee to seek as clear information from the Home Office as possible on what the Draft Bill will mean in practice for all involved.

13. The Home Office argues for law enforcement to be able to 'maintain' access to communications data as technology and ways of communicating evolve. However, it is not clear that the proposals in the Draft Bill merely maintain current capabilities in a changing environment. For example, the obligation to generate data that is not required for business purposes, the requirement to capture and retain data of a third party and the extended definition of CSP represent significant changes. We question whether such extensive additional powers are proportionate and necessary and whether less intrusive alternatives might be more appropriate.

14. On this basis, we believe that the Draft Bill would in fact extend existing capabilities in that it would require CSPs to retain data that they would otherwise not retain for business purposes and capture and retain data about services they do not own or operate. This could create a capability to track

relationships and interactions between individuals in multiple contexts and across multiple online environments where they meet.

15. In comparison with other Western countries the proposals are far reaching and beyond current norms. It could set a precedent for similar legislation elsewhere so it is important that the Draft Bill is fully scrutinised and explained as clearly as possible. How the proposals fit with the Government's wider goals of making the UK a digital hub to help boost growth and its support of the Internet freedom agenda is unclear.

Costs

16. It is currently difficult to determine with any accuracy the costs of the proposals to ISPA members but we note that the Home Office's cost estimates and risk assessments are made on the basis of optimistic assumptions. We would encourage the Committee to test these assumptions. There appear to be three key elements:
    1) costs incurred by CSPs;
    2) ability to bring overseas providers into the retention regime; and
    3) the continuing development of communications services.

Costs incurred by CSPs

17. The costs that will be incurred by CSPs could be significant but there is insufficient detail to determine whether the Home Office's assessment of £859 million is correct. ISPA believes, however, that the key costs related to the retention element of the proposals will be due to the Home Office and not CSPs. This is because the final costs will primarily be dependent on the retention notices issued by the Home Office to CSPs, which will specify the technology that CSPs will be required to deploy and the amount of data they are requested to retain.

18. We strongly welcome the Home Office's commitment to maintaining the current system of cost recovery for CSPs. CSPs do not gain from retaining and disclosing communications data. It is for this reason that we hope that the Committee endorses Parliament's support for the cost recovery system and we encourage Committee members to go further and ensure that the cost recovery for CSPs is guaranteed on the face of the Bill. This would provide a long-term guarantee that would bar future Governments from transferring retention costs to CSPs and thereby jeopardising investment of CSPs in network infrastructure and services.

19. The requirement to capture and retain data types which are not required for business purposes or to collect data relating to third party services is likely to impact the way CSPs build and operate their businesses. This is not why ISPs run their networks and is technically very complex. This obligation could force our members to redesign their networks based on the obligation to retain, rather than on commercial interest or economic effectiveness. Furthermore, there is a concern for small and start-up tech companies that they may be brought into the regime at any moment. This could severely impact on innovation, affect current and new business models and divert resources away from business investment and discourage international companies from choosing to base themselves in the UK. The Home Office should be able to offer certainty to CSPs about who and what is in scope and how the process may come about.

20. The estimated costs seem to be based on a number of assumptions. In the interests of transparency, and to enable Parliament and the wider public to understand the whole process, further detail should be provided on how the figure of £859 million was calculated. The accuracy of these estimates is important to an assessment of the overall proportionality of the Draft Bill. Not only must the costs be accurately assessed but industry must be assured that the costs of complying with the eventual obligations can be fully recovered. We therefore query whether contingency plans are in place for a situation where it becomes clear that the money that has been allocated turns out to be insufficient (e.g. because the need to retain third party data exceeds expectations).

Ability to bring overseas' providers into the retention regime

21. Two of the key elements of the new proposals are the extension of retention requirements to providers outside the UK and the ability to require UK CSPs to retain data of third party providers. According to comments made by the Home Office, these two proposals are closely interlinked as the third party data retention requirement would only be used if overseas providers were unwilling to comply with an order to retain data in the first instance. The ability to bring overseas providers into the retention regime will therefore have a significant impact on overall costs as the capturing of the relevant overseas data via UK providers would be the least cost efficient solution.

22. There is a concern over how these requirements will be viewed in other countries and possibly copied. Asserting UK jurisdiction on overseas providers is a significant step and it is not clear that this is a proportionate, necessary or realistic policy step. We do not feel that the Home Office has provided a compelling case for such sweeping powers and it is not clear that less radical alternatives (such as reforming Mutual Legal Assistance Treaties) have been fully explored. We would encourage the Committee to explore this further.

The continuing development of the communications industry

23. At present Government estimates that there is a 35% gap in communications data availability which, if the proposals are introduced, could be reduced to 25%. It is unclear how the baseline (i.e. 100% of data) for this assessment has been derived, how it will develop with new forms of communications and whether it will stay at the currently estimated level. It is not certain whether the data contained in this gap is not already available to LEAs but is not currently requested properly. We further question whether the proposals are justified and represent value for money for only a 10% increase in current capabilities. Developments in the communications industry are difficult to predict and there is little explanation in the consultation document of how the Government has taken account of this in the estimation of costs.

Level of intrusion into users' privacy

24. ISPA members believe that any intrusion into users' privacy should be kept to a minimum and be proportionate and necessary in order to avoid a situation where average users feel inclined to change their online behaviour in response to the proposals. The Draft Bill should be viewed within the wider debate around privacy and use of data online, which is based on a system of trust and a trend towards greater transparency. The level of intrusion is actually not fully explained or understood because a great deal of the detail remains unclear.

25. The filtering capabilities that the Draft Bill includes could present additional risks to privacy. As an additional third party is being included in the disclosure of private data, it could become an additional attack vector for malicious agents looking to obtain information about individuals. There also exists

the possibility for legal representations being made by other parties via the courts to access data retained for the purposes of civil cases or as defence material in other cases.

26. Questions of intrusion, proportionality and necessity arise in relation to the retention of and access to data. The scope, definitions and also the presence of appropriate safeguards proposed by the Draft Bill will play an important part in determining the answer to these questions.

Scope & Definitions

27. Whilst the Draft Bill appears to make only a minor change to the definition of 'communications data' it potentially has a substantial impact. The introduction of the new term 'telecommunications operator' and the inclusion of overseas providers effectively makes a significant change compared to the established definitions of 'public communications providers' under the Regulation of Investigatory Powers Act 2000 (RIPA) or 'communications providers' under the Anti-Terrorism Crime and Security Act 2001 (ACTSA).

28. The Draft Bill's term 'telecommunications operator' refers to a person who controls or provides a telecommunications system, or provides a telecommunications service and will thus cover, among other things, social networking providers, webmail and instant messaging.

29. If the definition of communications data is applied to these wider areas, for example, then it becomes clear that these providers will not only be required to retain new types of data (compared to a 'traditional' CSP) but that these data types also have the potential to be far more revealing and intrusive than the data that is currently being retained for law enforcement purposes. For example, the draft Bill defines 'subscriber data' as "information (other than traffic data or use data) held or obtained by a person providing a telecommunications service about those to whom the service is provided by that person." Social networks often ask their users for information about their gender, religion, relationship status etc. which should not only be considered as very personal information but is also information that is currently not retained for law enforcement purposes.

30. A further challenge of definition is determining what within a communication application constitutes communications data and, as such, would need to be retained, as opposed to data that would need to be collected through lawful intercept. Within communications applications such as social networking services or online gaming, the differentials between what would traditionally constitute Internet 'traffic' and 'content' become less distinct. The Committee should consider whether communications data can be reliably extracted from content data in this scenario.

31. In addition to changing definitions, the Draft Bill extends the scope geographically by requiring overseas providers to retain data or by making this data accessible via UK CSPs. The Home Office says that these new retention requirements only cover data relating to UK citizens or people staying within the UK during the time for which the data is requested, yet the requirement provides access to a wider data set than this. The Committee should consider whether such a broad power is necessary and proportionate if the policing need is much narrower.

32. The precise data types as well as the proportionality and feasibility of the proposed extension to the scope of the data retention regime merit further investigation by the Committee. Until this is known, the impact of the proposals cannot be accurately quantified by Parliament or CSPs.

Safeguards and Enforcement

33. Higher levels of intrusion would warrant the introduction of new safeguards and additional oversight mechanisms. As we argued earlier, this should be applied to both the retention of and the access to communications data. As others may focus more on access to data, we will focus on the retention of data.

34. Oversight of data retention should take place on multiple levels. Parliament plays a key role in this and we welcome that the Committee has been given the opportunity to scrutinise the current proposals in the form of a Draft Bill. We are concerned, however, that numerous requirements in addition to those on the face of the Draft Bill could be introduced by orders, notices and secondary legislation, i.e. with limited parliamentary oversight. For example, the data types that CSPs would have to retain would only be specified in notices by the Secretary of State, without further scrutiny. As currently drafted, the current Draft Bill would put a great deal of power into the hands of the Home Secretary and to ensure that the retention of data is proportionate, Parliamentary oversight needs to be robust.

35. It is proposed that oversight would be provided by the Interception of Communications Commissioner's Office (IoCCO) and the Information Commissioner's Office (ICO). The proposals of the Draft Bill lead to a situation in which CSPs would be required to retain much larger volumes of commercially sensitive data with a corresponding increase in burdens to store and manage it appropriately, including securing and restricting access to it, for law enforcement purposes authorised by the Draft Bill. The Committee must be satisfied that, whatever proposals are passed by parliament the IoCCO and ICO are sufficiently resourced to address these issues. They must also have the necessary powers and access to information they would need to perform their oversight roles effectively. We would also welcome clarification on what proposed role Ofcom will have in the process.

36. The Committee will be aware that the EU Data Retention Directive (EUDRD) is under review, and there is a potential for the period of retention to be reduced. Any reform or changes to the wider communications data landscape should be flexible and allow for developments in Europe to be reflected in the UK.

Technical aspects of the Draft Communications Data Bill

37. The Draft Bill raises serious concerns about technical feasibility which have yet to be explored in detail.

38. Requiring companies to generate data specifically and only for law enforcement purposes or to capture and retain data about third party services sounds simple but they are technically very complex and difficult propositions. We would like to dispel the idea that existing equipment can be easily reconfigured to capture and retain third party data. DPI and such technology can be used by ISPs for legitimate traffic management processes, but it does not follow it could be repurposed to fulfil the requirements set out in the Draft Bill. We are yet to be convinced that current hardware can handle the volume of traffic that moves across service provider networks at this level.

39. There is a further concern that the in-line devices that would be placed into the network are vulnerable to hackers and criminals and prone to cause single points of failure. Since the Draft Bill and the backstop powers rely heavily on such complex technical solutions, we would encourage the Committee to consider whether this approach could be technically feasible or cost effective to implement.

40. The Draft Bill contains powers for law enforcement to use a filtering arrangement to match individual's various communications across different platforms. Again, we feel more information is required to better understand what this will mean in practice and whether more safeguards need to be put in place to safeguard privacy. By extending the value chain and analysing data from multiple sources rather than from the source itself, as the filter is expected to do, the reliability of the data could be compromised and its evidential and intelligence value lost.

41. In terms of the utility of capabilities proposed, ISPA is concerned that they would be evaded not only because users will increasingly turn to encrypting traffic, but also by the prospect that it will become the norm and be built in as standard by third parties, i.e. even where users haven't specifically decided to encrypt. This would impair the ability of CSPs to manage traffic on their networks, as it would all appear as a stream of different encrypted communications streams with no easy way to differentiate the content within those streams. In addition, we are yet to be convinced how third party data could be reliably extracted from encrypted traffic.

August 2012

Dr Dominic Jackson

- I am a private individual representing no-one but myself. I am a technology enthusiast and keen student of the workings of the Internet however I am also a person who guards my privacy jealously.

- In summary, the draft communications data bill is an abhorrent piece of legislation. It does far more than merely "updating existing powers" and seeks to give broad powers to spy on all UK Internet users for no good reason. It is a classic "solution in search of a problem" and should be rejected at the earliest opportunity.

- The Government has made no convincing case of the need for the powers proposed in this Bill. The only vague justifications are hand-waving hypothetical scare stories about terrorists using the Internet, social media and the like to communicate and plan atrocities. The improved convenience to law enforcement of the powers sought is nowhere near enough justification for seeking to record who communicates with what or whom, in every Internet operation carried out in the UK.

- It is disappointing to see a Government, which campaigned on the basis of repealing some of the Labour administration's excesses such as the Identity Cards Act, introduce such legislation. The draft Communications Bill shares many of the fundamental failings of the Identity Cards Act, such as lack of clear description of the problems to be solved, appeals to fears, scaremongering and paranoia about terrorism and costs that will almost certainly spiral out of control at a time when the country can ill afford such wastefulness. Moreover, if passed, the powers in the Bill will almost certainly be subject to demands from others, such as the media industry looking to prosecute copyright infringers.

- I am concerned that the UK's approach will act as a "green light" and a template for other countries to introduce similar legislation. Canada attempted to introduce data mining powers which were rebuffed only after a massive outcry (and arguably, incompetence from senior Canadian government figures during the debate and controversial "guerilla tactics" from those opposed to the plans). Australia has also proposed similar plans, apparently modelled on the UK approach.

- The intersection of the draft Communications Data Bill with data retention powers is of deep concern to me. Data retention in Europe was passed because of a classic piece of "policy laundering" by the Blair government during the mid-2000s at a time when terrorism scaremongering was an everyday occurrence in Government rhetoric. Having tried unsuccessfully to get such legislation passed domestically, the Blair government moved to Europe and managed to obtain an EU Directive to mandate that which they could not achieve at home. Data retention has already been rejected in some EU states (notably, Germany and Romania) as unconstitutional. The remains of this power in the UK, together with vague representations about what "communications data" should be collected, represent a massive infringement of civil liberties, again for no good reason (see previous comments about Government terrorism hype). The question of if 12 months' retention is too long or too short is emphatically answered with "too long" but the correct period should be either nothing or next to nothing (e.g. 24 or 48 hours). The period of data retention also obviously has a bearing on the costs of the proposal given the storage capacity needed to retain the data.

- I am deeply sceptical about the costs and benefits quoted for this Bill. Government IT projects such as this ALWAYS over-run in terms of timings and costs. They are inevitably subject to "feature creep" as the private sector contractors involved "gorge their faces" on lucrative Government contracts. This has been seen with countless previous Government IT projects such as NHS Spine and indeed the Identity Cards Act. I see no justification for the benefits quoted for the Bill and suggest that the money allocated, if it needs to be spent at all, should be directed towards better

policing.

- The notion that "communications data" (such as who is communicating with whom and the date and time of the communications) can be separated from the content of the communication itself, is a complete fallacy in Internet terms. If it is recorded that I visited www.example.com then it is obviously trivial to replay my visit and probably inspect the content of the communication even though this was not originally stored. The draft Bill is also worryingly silent on whether only the fact that I visited www.example.com will be recorded, or whether the individual pages within that site (some possibly with custom URLs arising from personal information such as a user login that I pass to the site) will be recorded. This fallacy is a key underlying assumption of the draft Bill and that it is demonstrably false does not instil confidence in the rest of the Bill. The Bill also fails to appreciate that, with modern technology, it is perfectly feasible for "communications data" to consist of a five minute Amazon EC2 instance that talked to a web application that momentarily existed in some other cloud somewhere and then vanished. The data collected on such ephemeral, virtual communications is, for all practical purposes, useless.

- Likewise, the questions raised about security of the data once collected ignore the "elephant in the room" of the human factor. That is to say, any database security is only as strong as its weakest link, and above a certain level of basic computer security this weak link will inevitably be the human operators of the database. Even if they are not inherently corrupt then they can be corrupted through blackmail, extortion and the like. We have seen from the recent News International scandals how this kind of influence can be brought to bear on civil servants and other figures entrusted with private data. Given that the day-to-day running of the powers proposed by the draft Bill would almost certainly be outsourced to "minimum wage slaves" employed by G4S and the like, it is not hard to imagine the motives for corruption, nor the opportunity, which just leaves the means which isn't hard to imagine either.

- The second major fallacy of the draft Bill is that storing the data collected in a number of separate databases will somehow be safer than if it was all stored in one centralised database. Again this betrays a lack of understanding of modern technology; it is just as trivial with modern computing power to index and thus search across a multitude of data sources as it is to search just one. Google's branching out into image and video searching with just one search term should be treated as an example of this. It will be trivial to assemble a complete picture of people's lives from the various data sources this Bill contemplates creating which represents a massive invasion of privacy.

- The measures proposed in the Bill could be easily circumvented either by use of encryption and Virtual Private Networks, deliberately using non-UK providers or by switching to offline communications. The serious terrorist will doubtless adopt these measures, leading to the Bill only affecting the "incompetent amateur" and the law-abiding citizen. The suggestion made in Government circles that encryption could be broken for the purposes of this Bill do not bear thinking about: strong encryption underlies many of the positive aspects of 21st century life such as online banking, e-commerce and online servicing of utility accounts and convenient interaction with the State (such as updating the electoral register and paying council tax online).

- The "unintended consequences" of this draft Bill do not require much thought. Investigative journalists might unintentionally reveal their sources, CEOs of commercial organisations logged as communicating with one another might unintentionally reveal takeover plans, abused women in hiding might have their cover blown. The notional application of the powers in the draft Bill to identifying terrorist cells would be equally applicable to identifying members of other cells of civil society (such as Greenpeace, digital rights campaigners, Occupy). The same objections apply as to the Identity Cards Act: today's governments might consider themselves benign towards such movements but what of tomorrow's BNP government? Once handed over to the State the

information can never be erased from the State's logs and this alone should be reason to scrap the draft Bill.

- The evidence proffered in favour of the proposed powers is weak and consists of hand-waving "What if" scenarios. More people are killed in road accidents than in terrorist attacks each year in the UK. Terrorists doubtless use "offline" communications methods such as meeting in pubs, restaurants and other public places. Does this mean the proprietors of such establishments should be required to record who enters their premises and who they talk to, and pass this on to the State? Of course not – common sense revolts at the idea! Taken to its logical conclusion, everyone should be locked up in prison until they can prove they are not a terrorist, but logistics aside, a civilised society again finds this idea repulsive.

- Ultimately, preventing terrorist atrocities is a matter for highly skilled human intelligence workers. It is a classic "needle in a haystack" problem; after the event it is often easy (with hindsight) to identify the links between the perpetrators and then to show that, actually, the authorities had all this information already and could have "joined the dots" and thus stopped the attack. However, before the event, the problem is to identify the relevant "dots" in amongst the "sea of other dots" and of "joining the [relevant] dots" before it is too late. From this context, throwing more hay onto the stack on the offchance that it contains another needle, is clearly a waste of effort. One would use sophisticated techniques to narrow down the area of the haystack that needs searching, for example using metal detectors or asking where a needle was last seen.

- To conclude the themes of the previous paragraph, presuming it is a real threat and not just hype and paranoia (which is in itself debatable), the problems of serious crime and terrorism will be addressed by clever police and detective work; identifying likely perpetrators and concentrating on THEM ALONE to identify their network of contacts, then use undercover officers to infiltrate the gangs, prevent them obtaining explosives and weapons and gathered evidence to bring the members to justice. There is ample evidence from global news reports that intelligence agencies across the world are having some success with these tactics. There is no evidence that warrant-less, unjustified mass surveillance of the population is achieving or will achieve the same results.

- The oft-quoted maxim is "If you've nothing to hide, you've nothing to fear!" This is highly disingenuous. I DO have something to hide, namely my personal privacy and desire to proceed with my daily life free of interruption or harassment by the State. Every single person has this same factor; our own reasonable expectations of privacy and therefore, by implication, the converse of the clichéd maxim must be true. We ALL have something to hide and so we ALL have something to fear from legislation such as this.

- The draft Bill has no solid underlying foundation in fact or reality, it is the latest in a series of "terrorist paranoia" pieces of legislation. I ask the Committee and Parliament as a whole to please bury the ideas it contains back in the ground where they came from, ideally with a stake through the heart and salting the earth above them to prevent the concepts rising from the dead, as they have done in this latest rehash of the Labour government's discredited Intercept Modernisation Programme.

August 2012

Andrew James

General:
1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?
It has but the problem is it hasn't outlined *how* it will do this.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?
No, the argument is not convincing. The argument is fundamentally flawed in that any legislation would never be flexible enough to provide for the very problem it is intended to solve – the rapid change in communications.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?
The wider landscape is changing at such a rapid rate, that even the most recent legislative instruments can be argued as quickly becoming out dated. But more to the point, communications data now describes one's personal life to a much deeper level (shopping transactions for example can be argued as a communications data whereas previously it would not be communication data, a result of our changing behaviours utilising the internet).

4. What lessons can be learnt from the approach of other countries to the collection of communications data?
The UK is entirely unique in terms of historic context and the relationship between the telecommunication industry and the policing/intelligence arena. It would be misleading to look at other countries in terms of strategic lessons.

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?
Yes, the government should take a risk based approach to identifying application based communications (Skype, MSN, Facebook, FaceTime etc.) and ascertain how the managing companies (Microsoft, Google, Apple) can provide meaningful communications data on a needs driven basis. The obligation should be drawn away from the communication provider/ISP and towards the application layer. This is where the trend is heading. The response must be much more agile (in technical and legal terms) than what the government is currently proposing or it will be money unwisely spent.

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

The EU-DRD is a high level guideline that offers no clarity on exactly how CD would be collected and managed in the UK, nor does it offer any relevance, specifically, for the law enforcement landscape in the UK.

Of course it would, but the government is pushing this through as an urgent legislation and EU requirements would not allow for a change in the harmonisation policy requiring an EU regulation in this area so this is a moot question.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?
The legislation provides for powers which can be interpreted in a number of ways, it is not clear at all, how the Home Office intends to utilise these new powers, whether it would maintain a register of all communications data, or ask operators to do that.

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

For SMEs, the answer will be – of course it will be less attractive. The rates involved in storing and being able to provide communications data is a huge administrative burden.

Costs:
9. Is the estimated cost of £1.8bn over 10 years realistic?

No way. Firstly, how can something so unpredictable as the communications market be predicted with any reliability for 10 years away (we are in this position because we didn't predict where we are now would happen!). Secondly, over 85% of defence and security programmes (major projects) have been seriously under estimated in the last 20 years. This is simply a finger in the air guess. The government has already spent hundreds of millions on this since 2005 and has not yet delivered anything.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?

Again – there are no robust quantitative assessments that could possibly make this figure realistic. It is a rough estimate at best and is based on conjecture and opinion of the agencies who stand to benefit, the figure ought to be properly assessed by the NAO as should the entire cost basis of the programme.

Scope:
11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

No. The definition of communication data is based on the former definition of CD from RIPA. It makes no distinction to new communication data. For example, how does one define the limit between the communication data and the content for – an amazon transaction for a book on counter terrorism, or a conversation on Skype? How would the legislation be secured enough to not allow for 'catch all' interpretation to the actual real life mechanisms that will be developed to capture CD? The definitions and scope are confused and misguided.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?
The list should be determined on a risk based approach, with immediate threat to life being first and so on.

13. How robust are the plans to place requirements on communications service providers based overseas?
Many UK companies are based abroad and regulated by British law. As long as a company operates here they are exposed to British regulation – Santander in Spain etc. However the detail of the regulation of overseas third part data must be addressed in tighter detail in the plans. The problem here is that it is incredibly easy for someone in the UK to turn on their computer and communicate via a method that has no legal base in the UK – this is a major problem in the legislation that is again not addressed. E.g. If an app company creates an app such as WhatsApp, say in Russia, and I communicate on that using my laptop, is it the operator (my broadband provider) or What'sApp that provides the communication data. Techically, the operator has no access to the communication data, and legally, the WhatApp owners are based in Russia so have no obligation to provide that data to the UK operator. If this can't be answered the whole point of this programme of legislation is entirely flawed.

Use of Communications Data:
14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

15. Is the proposed 12 month period for the retention of data too long or too short?

It is too short for complex and high profile investigations. It is too long for civil liberties purposes.

Safeguards:
16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

How would this work in a threat to life situation? The resource implications are massive.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

Yes.

Parliamentary Oversight:
19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

They are better than 2 years ago!

Enforcement:
20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

There are no penalties described in the draft Bill. The draft Bill refers to the Financial Services and Markets Act 2000 only.

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

Technical:
22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

Technology exist to store any sort of data as long as that data is defined and the process is authorised. Communications data and content definitions are far from clear and are variable across types of communication, so the answer to this question is no.

23. How safely can communications data be stored?

Dependent on multiple variables, very or not at all. The question is pointless without given context.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

No.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?

Any organisation who can argue the greyness of the clauses in this draft Bill will be able to circumvent compliance. Any individual with a 4 year old's technical ability could communicate with anyone else without being exposed to the mechanisms intended by this draft Bill.

26. Are there concerns about the consequences of decryption?

I think there are bigger concerns here than decryption. A criminal is not going to use encryption when they can simply use a number of communication apps in sequence (GChat, WhatApp, iMessage, MyMessage) etc.

The communications environment in the last 10 years has moved on from telephones and post, to a world where I can and do use over 10 types of IP based application and non-application layer communications per day. The government is trying to match this human-evolution and society-evolution led rapid change with a piece of legislation and a costly technological solution designed now and for the next 10 years. The logic to the approach is flawed. It won't work, it will only cost the tax payer billions and move us in the wrong direction in the delicate balance of liberty and security.

August 2012

JANET

1. This is the submission of the JNT Association, trading as Janet, to the Joint Committee on the draft Communications Data Bill.[168] Janet is the UK's National Research and Education Network, a high-speed private data network that connects all universities, colleges, research organisations and schools networks to each other and to the public Internet.

2. We are concerned that the draft Bill will, perhaps unintentionally, affect a much wider range of networks, data and users in the UK than the current Data Retention Regulations (Q1, 2, 11), and that it could damage the reliability of, and confidence in, computers and networks that is essential if the UK is to achieve the social and economic benefits of an information society (Q9, 26). We also believe that the possibility of many new processes for obtaining communications data will lead to confusion and create new opportunities for unauthorised access to that data (Q16, 23, 26).

Q1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

Q2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

3. The draft Bill would give the Secretary of State the power to order the collection of communications data from any "telecommunications operator"; this is defined in clause 28(1) of the draft Bill so as to include public and private networks both inside and outside every organisation in the UK as well as a high proportion of domestic properties. Current data retention requirements only apply to the much smaller number of public communications providers, as defined in Regulation 2(e) of the *Data Retention (EC Directive) Regulations 2009*, deriving from s.151 of the *Communications Act 2009*.

4. The Home Office's case for the Bill does not mention nor justify this significant increase in the networks, organisations and users that may be subject to data retention requirements, nor can we see any need for it to achieve the Bill's stated purpose. We therefore recommend that the scope of the Clause 1 power be reduced to "public communications providers" as under the current data retention regime.

Q9. Is the estimated cost of £1.8bn over 10 years realistic?

5. The financial costs largely depend on how, and how often, the powers created by the Bill are exercised, so cannot be estimated from the information that has been published.

6. However we note that the powers may also impose non-financial costs on telecommunications operators and their services. Many networks, including Janet, have been designed to ensure that a single failure does not cause loss of connectivity. A side effect of this improved resilience through the provision of multiple paths is to make it harder to collect communications data as there is no longer any single point where all data can be collected. The Bill appears to give the Secretary of State the power to order such resilience to be removed to facilitate the availability of communications data, even though this would make the network unsuitable for the growing range of teaching, research and operational purposes that depend on highly-reliable networks. An order to add new monitoring devices into a network, or to alter the normal traffic routing, could also have an unpredictable effect on its reliability and performance.

---

[168] http://www.parliament.uk/documents/joint-committees/communications-data/commsdataCfE.pdf

7. The Bill may also require telecommunications providers to install and manage new systems to collect communications data, and will require them to keep collected data secure. This will require continuing effort by expert network and security engineers and privacy specialists. Organisations that have such specialists will forgo part of their contribution to the development and operation of products and services; organisations that do not currently have such skills will need to recruit them in areas subject to skills shortages.

Q11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

8. The draft Bill does not use the term "communications service provider", which only appears in the Notes. The draft Bill instead defines and uses the term "telecommunications operator". We do not consider that either the definition of "telecommunications operator" or "communications data" (in clause 28(1)-(5)) is appropriate.

9. As in our response to Q1 & 2 above, we do not believe that "telecommunications operator", as defined in clause 28(1) of the Bill is the appropriate scope for the clause 1 power.

10. The definition of "communications data" in clauses 28(1) to 28(5) will extend much wider than the normal meaning of that term (and the stated intention of the draft Bill) when it is applied to organisations such as universities, webmail and social network services, all of which appear to be included in the current definition of "telecommunications operator".

11. This is because "communications data" is defined in clause 28(1) as the aggregate of "use data", "traffic data" and "subscriber data". Clause 28(5) then defines "subscriber data" as "information (other than traffic data or use data) held or obtained by a person providing a telecommunications service about those to whom the service is provided by that person". In other words "communications data" will comprise all information held by the service provider about the individuals who use the service. In the case of a university or social network this would cover much more than is normally considered subscriber or communications data: for example it would include a student's academic record or a member of staff's personnel file. Indeed since, unlike clause 28(4) defining use data, clause 28(5) does not exclude the content of communications, it appears that communications data would also include the content of all the user's messages that were held by the telecommunications operator.

12. To remove this problem the draft Bill's definition of "subscriber data" should be replaced by a definition that states what subscriber data **is**, rather than what it is not.

Q16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

13. The current *Regulation of Investigatory Powers Act* Part 1 Chapter II (RIPA) regime establishes a single, well-defined, process for accessing communications data. This has allowed communications providers to develop their own processes for handling RIPA notices through a single point of contact, ensuring that all

disclosures of communications data are prompt, lawful and efficient. To promote such efficiency, the Home Office Code of Practice[169] prohibits any use of other powers to obtain communications data.

14. Clause 9(2) of the draft Bill would reverse this approach by permitting "any conduct" to be used to request or order the disclosure of communications data. Communications providers would no longer be able to adopt standard processes, since they might receive valid requests or instructions through any process and in any form that any designated senior officer considers necessary and proportionate. This will inevitably slow down the process of access to communications data and increase its costs. As discussed in our response to Q 23 & 25 below, we believe it will also increase the opportunity for fraudulent access to stored information.

15. Clause 9(3) encourages alternatives to the standard RIPA process (which is described in clause 9(3)(d)), by giving examples of "asking any person" – apparently including within a communications provider – who may be able to obtain communications data to do so; Clause 9(4) would then authorise "obtaining or disclosure... or any other conduct" by such a person, even if it would otherwise be a criminal offence for example under s.55 of the *Data Protection Act 1998*. Indeed clause 9(2) appears to allow such a person to be required, rather than just asked, to obtain and disclose data, which would make the RIPA process redundant. The existing RIPA process was designed to promote the interests of law enforcement, communications providers and users. We do not consider that creating alternative processes under clause 9(2) will be satisfactory for any of those interests.

Q23. How safely can communications data be stored?

Q25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?

16. It is highly unlikely that communications data (or indeed any other data) can be stored completely safely: there are examples of information being obtained without authorisation from both police[170] and ISP[171] databases. Successful attacks can use both technical and human weaknesses, as discussed in the Information Commissioner's reports "What Price Privacy"[172] and "What Price Privacy Now".[173]

17. We are especially concerned that allowing multiple processes for obtaining communications data under Clause 9(2) – particularly since these processes can be less formal than the current RIPA one – will make it much easier for "blaggers" to obtain communications data by fraudulent impersonation. Telecommunications providers and others with access to communications data will be required by that Clause to respond to new and varied forms of legitimate request and order, making it much easier for a blagger to explain why his request varies from those that have been seen before. Protecting against this risk will require scrupulous checks by the recipients of all requests under Clause 9(2), thus delaying lawful access to data and increasing the workload for both providers and the designated senior officers with whom they will have to verify every new process.

---

[169] http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition

[170] http://news.bbc.co.uk/1/hi/uk/7033935.stm

[171] http://www.theaustralian.com.au/australian-it/telecommunications/anonymous-hackers-dump-stolen-data-belonging-to-australian-firm-aapt/story-fn4iyzsr-1226437681976

[172] http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf

[173] http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico-wppnow-0602.pdf

18. The data collection and storage systems envisaged by the Home Office will represent attractive targets for those who wish to obtain data about users. Even if only local communications data is stored this will be in larger quantities than at present. However the Home Office have also indicated that it will be possible to obtain data about communications using third party providers; this can only be done by examining the content of communications and extracting communications data from it. Such systems will be a particularly valuable target for attack, since access (either through a human or technological attack) to such a system could provide the ability to read all the communications content that passes through it, as is reported to have happened to Vodaphone-Panaphon's systems in Greece.[174]

Q26. Are there concerns about the consequences of decryption?

19. Our concerns that data storage and collection systems will be an attractive target for unauthorised access would be increased if those systems were storing or accessing the plaintext of information or communications that are currently encrypted. As well as the harm resulting from the loss of information considered sufficiently sensitive to justify encryption, even a rumour of unauthorised access to a decrypting system could damage public and business confidence in the Internet as a safe way to communicate. The Government's plans for an e-society depend on citizens and businesses being willing to send and receive sensitive private information over the Internet, whether to e-government, e-health or e-business systems. If individuals do not believe that browser-encrypted communications are safe then it will be difficult to persuade them to use these systems.

August 2012

[174] http://spectrum.ieee.org/telecom/security/the-athens-affair/

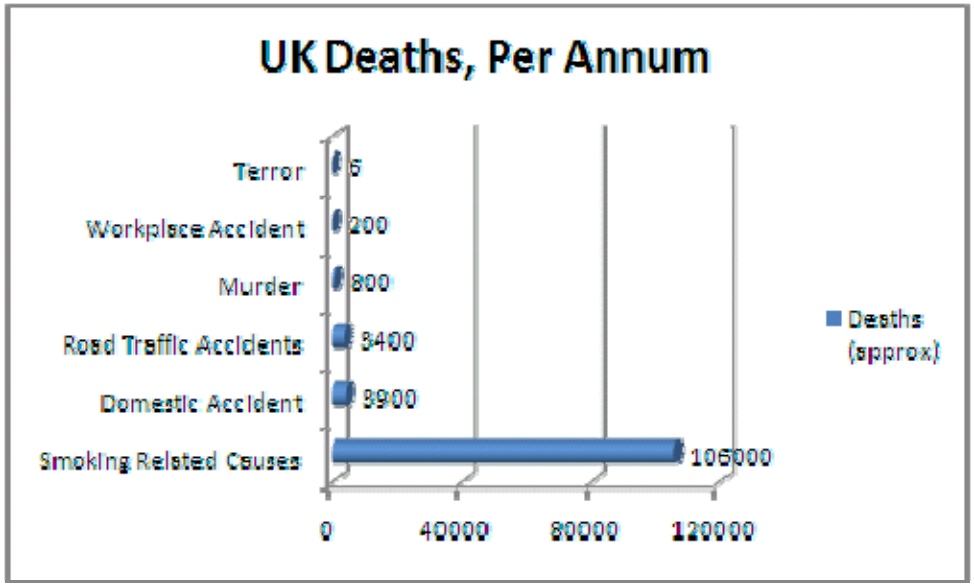
Peter John

General:

1. **Has the Home Office made it clear what it hopes to achieve through the draft Bill?**

It is important to understand that crimes like terrorism – often used by the Home Office to justify mass surveillance – presently pose a negligible risk to life in the UK;

UK Deaths, Per Annum



To put those numbers in perspective, 6 people die every year falling out of trees. But there is no expectation that crash mats will be placed under all trees in the UK 'just in case'.

If you want to save lives, the conclusion is inescapable… Best value is derived by spending £billions preventing people smoking. Rather than spending £billions intercepting the communications of innocent people and the law abiding businesses that serve them.

The other crime frequently cited as justification for mass surveillance is the heinous offence of child murder/paedophilia. The Home Office cited the shocking examples of Ian Huntley & Levi Bellfield.

In the case of Huntley, however, it was revealed that he had been a suspect in a series of sexual offences and burglaries.. yet had still been allowed to work in a school. **There is nothing to suggest that retained communications data would have prevented Huntley's offences. There was a serious failure by public authorities to accurately vet his background, and a serious failure by police to reconcile data on his behaviour.**

Bellfield was named by police as a suspect in connection with numerous unsolved murders and attacks on women dating back to 1990, and the murder of a 14-year-old girl in 1980. Assistant Chief Constable Jerry Kirkby said, "Questions will be asked whether Bellfield could have been caught and we must accept, and do, that mistakes were made". **There is no evidence to suggest that retained communications data would have prevented Bellfield's offences.**

In both cases, a serious failure by police to correlate **available conventional intelligence** allowed the offences to occur.

2. **Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?**

No (see prev answer).

Britain is – broadly - a safer place now than it has ever been.

Consequently, a reduction in unwarranted surveillance, and greater promotion of democratic freedom, would be a welcome change of strategy.

3. **How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?**

The UK has – through the laissez faire indifference of lazy and corrupt regulators – become a society I barely recognise it from my childhood. A place where intrusion into personal privacy has become so ubiquitous it *exceeds* the dystopian vision of George Orwell's 1984.

At the same time, the opportunities for redress when public & private sector organisations overstep the rights of citizens have been completely undermined by timid and corrupt regulation & law enforcement.

There is no effective protection or remedy when the law is broken.

For that reason, I fully expect to emigrate in the next 12 months, to a society where personal liberty is better protected.

4. **What lessons can be learnt from the approach of other countries to the collection of communications data?**

The Joint Committee might be wise to look to overseas history; "Those who cannot learn from history are doomed to repeat it".

There the activities of the Stasi bear comparison. The Stasi operated one of the world's biggest mass surveillance operations. The Stasi used mass surveillance to identify political dissent among citizens. Because citizens were aware that their government was spying on them a culture of mistrust resulted. Politics were only discussed where surveillance could not reach, and only with close family.

Is that really the example you think the UK should follow? A database that encompasses the private communications of all UK citizens? If so, I fear you're ignoring history at your peril.

5. **Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?**

Interception of communications should be a last resort, used in only the most serious cases of criminal misconduct, and only when a warrant has been obtained.

Mass surveillance will compel the unconditional use of encryption, ultimately driving up the cost of mass surveillance in an escalating self-destructive spiral of countermeasures.

That impacts both the costs to Government, and the cost to UK telecommunications users (including commercial and personal users).

6. **The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?**

It would be preferable if the Joint Committee were to recommend that legislation complied with the European Convention on Human Rights article 8, which stipulates;

> *Everyone has the right to respect for his private and family life, his home and his correspondence.*

Retaining communications data of **innocent people** (and we are presumed innocent until proven guilty of a crime) is not proportionate. Unless you consider the UK a nation of criminal suspects.

7. **If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?**

No.

To quote Benjamin Franklin;

> *"They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."*

The privacy/security/integrity of my communications is not a commodity I am prepared to trade.

8. **Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?**

Taking for example the Phorm affair, UK communications service providers demonstrated that they were incapable of being trusted to respect the privacy/security/integrity of UK telecommunications.

Phorm Webwise was an industrial espionage scam that harvested commercial intelligence from UK telecommunications, and sold the resulting intelligence to the highest bidder.

The effect on business? The only rational response to such a surveillance threat is to stop using the UK telecommunications network, or adopt the strongest possible encryption methods.

I would not recommend anyone launch a business in the UK at present because there are no effective safeguards in this country against unlawful communications surveillance.

Costs:

9. **Is the estimated cost of £1.8bn over 10 years realistic?**

It seems very poor value for money.

10. **The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?**

I don't believe the Home Office could ever justify that figure. The money would be better spent addressing the deficiencies in police investigative procedures, intelligence handling, the child protection register, and eliminating rampant police corruption.

Scope:

11. **Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?**

Sorry, no response to offer.

12. **Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?**

Sorry, no response to offer.

13. **How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?**

Essentially, it is a nonsense to believe that you can ever police overseas providers, or impose effective constraints on them. King Canute had more success turning the tides.

The belief among some Members of Parliament that there could ever be a 'global standard' for communications regulation is simply delusional. Inconsistent regulation will *always* exist between democratic nations on one hand, and the corrupt authoritarian nations on the other.

The issue is more about determining whether the UK becomes a model of a democratic nation, or a model of a corrupt authoritarian nation.

Use of Communications Data:

14. **Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?**

Communications Data should be used to detect any serious criminal offence. It should not be gathered from innocent people until a crime is suspected.

15. **Is the proposed 12 month period for the retention of data too long or too short?**

Communications Data should not be retained without a warrant obtained in advance. The evidence should be destroyed once a police investigation has concluded.

And retained no longer than that.

Safeguards:

16. **Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?**

Every supposed 'safeguard' failed when BT conducted illegal covert surveillance of its subscribers using Phorm's Russian developed spyware in 2006, 2007 and 2008.

The ICO refused to intervene.

Ofcom claimed it had no powers to act.

The various Surveillance Commissioners claimed they had no role to play.

And the police refused to investigate.

The CPS refused to prosecute.

So if British Telecom can covertly intercept the communications of 200,000 of their subscribers and the businesses who serve them, using Russian developed spying technology, with complete impunity… Why do you think anyone would have any confidence in the supposed 'safeguards' the Home Office claim will guarantee protection from abuse?

It is simply a preposterous lie.

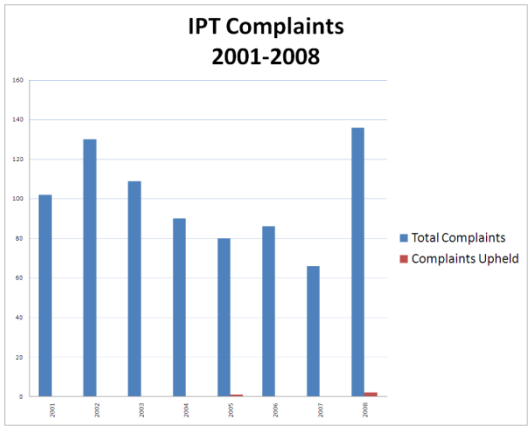
17. **Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?**

Yes, a warrant based system would be more appropriate.

18. **Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?**

The Investigatory Powers Tribunal has historically upheld few if any complaints;

IPT Complaints 2001-2008



In addition, they claim they have no role overseeing the actions of private sector organisations that engage in unlawful surveillance.

Until the oversight demonstrably includes robust enforcement of the law, and the scope of the oversight is extended to private sector organisations, the measures are utterly insufficient.

Parliamentary Oversight:

19. **Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?**

Parliament has demonstrated no capability to effectively oversee communications surveillance. I do not believe MPs have the technical expertise required to understand the means or extent of unlawful surveillance. Why do you believe that situation would change as a consequence of this bill?

Enforcement:

20. **Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?**

No, they are too weak. Evidence suggests that the police & regulators will not enforce penalties against people who violate the law, and will even cite the trivial nature of penalties as reason not to engage in enforcement.

21. **Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?**

The unlawful interception of communications is already a criminal offence. But few people are ever prosecuted.

Technical:

22. **Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?**

The technology exists to allow CSPs to capture some aspects of communications data about **innocent people** and the businesses that serve them.

However the question is more whether it is ever appropriate for them to gather such information without a warrant, or the explicit consent of the sender –AND- recipient.

I believe the answer to that question, in a democratic free society, is always **no**.

23. **How safely can communications data be stored?**

Very safely. Until it is compromised.

Examples of security specialists recently compromised include Stratfor (email stolen), HB Gary (emails stolen), US Army (the Wikileaks/Bradley Manning affair). And many others.

If organisations such as these cannot protect their own communications data securely, the Joint Committee might contemplate why any assurances of absolute security can ever be taken at face value.

In short, communications data once stored is likely to be stolen, abused and compromised.

24. **Are the proposals for the filtering arrangements clear, appropriate and technically feasible?**

No. I could explain why they will never be technically feasible, but not in 6 pages using language you would understand.

25. **How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?**

The bill will simply hasten the blanket use of encryption and/or onion routing… which will entirely defeat (or at least substantially impair) the value of mass surveillance.
In addition, counter surveillance tools (some of which I have developed) will likely further diminish the value of retained data by creating a blizzard of unusable noise (that will also need to be retained).

26. **Are there concerns about the consequences of decryption?**

If encrypted streams are routinely intercepted and decrypted, confidence in any form of UK telecommunications – encrypted or otherwise - will be lost.

At that point, any use of the UK communications network becomes wholly compromised, and the infrastructure becomes inherently untrustworthy. There then remains no basis for assuming that UK telecommunications are private or secure against unauthorised surveillance.
Which would be a tragedy, but assuming I can emigrate, one that would be your problem to resolve, and not mine.

August 2012

Just West Yorkshire

We do not believe that the UK government has put forward a convincing or cogent case for the need for the new powers proposed in the draft Bill and we believe that the proposed measures erode civil liberties.

We endorse the findings of the recently published Report by Big Brother Watch (*a civil liberties group*) entitled *'A legacy of surveillance'* which highlights very serious concerns with the use of surveillance by public authorities and the lack of transparency that currently exists. This position is also endorsed by the Community Secretary Eric Pickles. (http://www.guardian.co.uk/politics/2012/aug/22/bbc-ofsted-secrecy-surveillance)

We concur with Nick Pickles, director or the campaign group Big Brother Watch, condemnation of the proposals:
"This is an unprecedented attack on privacy online and it is far from clear this will actually improve public safety, while adding significant costs to internet business. No amount of scare-mongering can hide the fact that this policy is being condemned by MPs in all political parties."

Clearly there is a very real risk of the new proposed powers being abused or misused by public sector organisations. The plans would give unrestricted and carte blanche power to institutions without the proper checks and balances being in place. The extensive use of the RIPA legislation by local councils and public services clearly highlight the potential for abuse of any legislation which seeks to strip away the individual's rights to privacy.

We consider the argument that these powers will help to reduce crime to be fatuous. Positive outcomes in criminal investigations are best achieved not through increased surveillance but the appropriate deployment of police officers to tackle crime.

Furthermore the press and media have consistently highlighted cases of police corruption and fraud – the very groups that is most likely to use this legislation. JUST also believes that the lack of positive relationships between BME communities (viz, Muslims, African-Caribbean groups) and the police as a consequence of the police targeting potential terrorists and extremists and gun and knife crime could lead to these groups being unfairly targeted under the proposed measures. There is a real risk of sensitive, private and personal information being abused.

Although the proposed measure highlights one of its key benefits as the ability to track pedophiles, the recent example of a former police officer with West Yorkshire Police who was convicted of making indecent images of children, highlights that in the wrong hands, these powers carry a grave risk to the individual. http://www.wakefieldexpress.co.uk/news/local/more-wakefield-news/former-west-yorkshire-police-detective-s-child-porn-shame-1-4712857

The Office of the Information Commissioner has expressed grave doubts about the mass surveillance project too. He believes the case has ***'not been made'*** to justify the sweeping expansion in the power of the police and other public bodies to trawl through private communications, including visits to Facebook and eBay.

The government has claimed this proposal is needed to fight "terrorism and serious crimes;" However computer databases and systems such as NICHE, PNC, ANPR, VENOM, HOLMES, OIS, WYSE already exist and provide the police and other agencies with an extraordinary amount of data and intelligence on individuals, properties and businesses.

Likewise automatic classification, risk-based profiling, systematic tracking and recording of travel and use of public services, automated use of CCTV, analysis of buying habits and financial transactions, and the workplace monitoring of telephone calls, e-mail and internet use are already used extensively.

Presently, ISPs keep details of which websites users visit, and who they send and receive emails and internet phone calls from, for 12 months. ***This information can be accessed retrospectively by investigators, subject to complying with the relevant legal requirements during the investigation or detection of a crime. (not sure what this means)***

Under the new proposals, ISPs would install hardware from GCHQ - the Government's electronic snooping agency - allowing investigators to tap into a **real-time feed** of data, and examine when communications were sent, and who to, in order to build up intelligence on criminal activity. It is our clear position that sufficient powers already exist, which serve law enforcement and public agencies adequately.

Only very recently a Supreme Court ruling has confirmed that the retention of innocent people's DNA by the Police after they have been investigated and cleared of an offence is unlawful and that it was incompatible with a 2008 European Court of Human Rights decision. **Clearly therefore in the same logic around the 'lawful' retention of data in relation to innocent people should apply.**

Our concerns about the lack of safeguards around the confidentiality of the information is substantiated following the recent admission by the Ministry of Justice that their systems had been subject to an on-line cyber attack. http://www.independent.co.uk/news/uk/politics/home-office-and-ministry-of-justice-targeted-by-anonymous-hackers-in-assange-protest-8069811.html

Furthermore according to Google's Transparency Report, from January-June 2011 last year, they received 1,279 user data requests from UK authorities and refused to comply with 37%. Clearly there were concerns around the release of personal data that did not meet the disclosure tests under the Data Protection Act. Under this proposal, that number of refusals would drop to zero signaling no validity or threshold tests for the requests.

The proposal is a massive encroachment on privacy, and has many associated security risks and potential for further abuse. To store details of internet use for a year to allow police and intelligence services to access it is wholly disproportionate and unnecessary. There is clear disquiet among MPs too with the most recent concern being articulated by Senior Tory David Davis MP who labeled the proposal "incredibly intrusive"

The huge cost of the spying project at a time when the Government is making cuts elsewhere is not justifiable. In an era of austerity, the money would be better spent on funding key public services such as hospitals, schools and community projects and address the widening deficit.

JUST West Yorkshire fears that the very people that snooping plans are intended to uncover - serious organised criminal gangs, major fraudsters, paedophiles - are the very ones who are already using technology to avoid being snooped upon. Therefore the proposed law is not only a disproportionate response but wholly inadequate to deal with the proposed problem.

August 2012

JUSTICE

Executive Summary

Surveillance is a necessary activity in the fight against serious crime. When targeted, it can play a vital part in our national security. Unnecessary and excessive surveillance, however, destroys our privacy and blights our liberty.

The Draft Bill builds on the existing - and inadequate – regulatory provisions in Regulation of Investigatory Powers Act 2000 ('RIPA'). JUSTICE considers that the RIPA model is neither forward-looking nor human rights compliant.

The provisions in the Draft Bill propose a nationwide and blanket intrusion into the private life of every person in the UK using modern technology to communicate, to enhance their daily lives and support their freedom of expression. It would provide for the exponential expansion of the collection of information about how we use the internet, mobile telephones, landlines and the post to communicate with each other. The Information Commissioner has called this a step-change in the relationship between the State and the citizen. We agree.

The provisions in the Draft Bill are broad, vague and unjustified. No significant, new safeguards are offered. Importantly, we are yet to see clear evidence to support the Government's case that such expansion is necessary or appropriate.

Currently, around 500 public authorities are capable of accessing our communications data using existing surveillance powers. RIPA allows these public bodies to self-authorise access to our personal information. JUSTICE considers that this approach poses a significant threat to our personal privacy. Prior judicial authorisation for access to surveillance powers, including access to communications data should be the default in most circumstances. Fewer public authorities should be able to access this sensitive information about our private lives and access should be limited to those circumstances when surveillance is strictly necessary, principally, for the purposes of preventing and detecting serious offences.

Root-and-branch reform of our existing law on surveillance is needed to provide freedom from unreasonable suspicion and a modern surveillance framework for a digital age; not the further expansion of surveillance capability without truly effective safeguards against abuse.

(a) Introduction

1. Founded in 1957, JUSTICE is a UK-based human rights and law reform organisation. Its mission is to advance access to justice, human rights and the rule of law. It is also the British section of the International Commission of Jurists. Last year, we published *Freedom from Suspicion: Surveillance Reform for a Digital Age,* calling for the wholesale reform of the existing legal framework for surveillance, in the Regulation of Investigatory Powers Act 2000 ('RIPA').[175]
2. We welcome the opportunity to submit both written and oral evidence to the Joint Committee on the Draft Communications Data Bill ('the Joint Committee'). We regret that the Draft Communications

[175] JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age,* Nov 2012. Hard copies of this report will be provided to members of the Joint Committee on request. Chapter 4, which considers communications data, is provided as an Annex to this submission. http://www.justice.org.uk/resources.php/305/freedom-from-suspicion Hererin, '*Freedom from Suspicion*'.

Data Bill ('the Draft Bill') is severely lacking in detail and posed as a broad enabling power to arrange for the collection, retention and use of personal information, with very little detail provided on how these powers might be exercised in practice. This approach will significantly undermine the effectiveness of pre-legislative scrutiny by Parliament, commentators and the wider public.

(b) Background

3. The Communications Data Bill introduced in 2008 by the previous Government, would have, among other things, required communications service providers to give police and intelligence agencies unprecedented access to their networks for the purposes of facilitating interceptions and requesting data. It was withdrawn in the face of widespread opposition from JUSTICE and other civil liberties organisations, Parliamentarians and the public. The former Director of Public Prosecutions Sir Ken Macdonald QC, for instance, described those proposals as seeking to create 'an unimaginable hell-house of personal private information'.[176] In 2009, the Labour Government consulted on a series of proposals which would enable the Government to require private providers to collect communications data, again for the purposes of facilitating access to that data by public authorities. Again, in the face of opposition, these proposals were shelved.[177]

4. The Coalition Programme for Government committed to 'end the storage of internet and email records without good reason'.[178] Yet, early in its life, the Coalition also committed to 'introducing a programme' to revisit access to communications data.[179] However, the Government also promised to legislate in order to 'put in place the necessary regulations and safeguards' that would 'ensure that our response to this technology challenge is compatible with the Government's approach to information storage and civil liberties'.[180]

5. Unfortunately, the Draft Bill fails to make good on these commitments to robust safeguards for the protection of our right to privacy online.

6. The Draft Bill builds upon our existing framework for surveillance in the Regulation of Investigatory Powers Act 2000 ('RIPA'). RIPA currently provides for requests for access to communications data.

---

[176] See '*Private firm may track all email and calls*' by Richard Norton-Taylor and Alan Travis, The Guardian, 31 December 2008.

[177] JUSTICE's submission to the Home Office Consultation, *Protecting the public in an changing communications environment,* in 2009 is available, here: http://www.justice.org.uk/resources.php/190/communications-data-collection-and-use-justice-response

[178] Cabinet Office, *The Coalition Programme for Government*, p11

[179] ***Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (Cm 7948, October 2010), p44.**

[180] ***Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (Cm 7948, October 2010), p44.**

Communications data is defined by RIPA and includes subscriber data, traffic data and user data. Broadly, subscriber data is information held by a provider about a user; traffic data outlines information such as the location of the communication and the people involved, and details of the equipment used; and use data relates to the use made of the relevant service (for example, what websites a user has visited etc).[181] Named public bodies can access different categories of data for different purposes, following internal administrative authorisation by a senior officer within their organisation. Following the passage of the Protection of Freedoms Act 2012, local authorities may only access limited data following authorisation by a magistrate (although these provisions are not yet in force).

7. The request to a service provider may be in the form of an authorisation (section 22(3)) or a notice (section 22(4)), the difference being the former is a request for information that the provider already holds, while a notice is a direction to the provider to acquire it on behalf of the requesting body. Notices and authorisations last one month unless renewed.[182] Service providers must comply with notices requiring access to communications data under RIPA, unless it is 'not reasonably practicable' to do so.[183] If necessary, the Secretary of State can seek an injunction for the enforcement of the notice.[184] Oversight is provided by the Interception of Communications Commissioner.[185] Since late 2005, public bodies able to make requests have been subject to an inspection regime carried out by an inspectorate under the direction of a Chief Inspector and the supervision of the Commissioner.

8. The Data Retention (EC Directive) Regulations 2009 (which implement the EU Data Retention Directive)[186] require certain public communications operators to retain information originally held for commercial purposes for up to 12 months.[187]

9. The overriding difference between the existing framework and the Draft Bill is the shift away from the presumption that for limited purposes, the State may access data already retained or reasonably obtainable by service providers, when shown to be necessary and proportionate for the prevention or detection of crime and other reasons which serve the public interest. While the existing measures are flawed (we return to this below); the Draft Bill would create a power for the Secretary of State to determine that all communications data about the population's activities and habits should be retained

---

[181] *Freedom from suspicion,* Chapter 4, provides fuller details on the existing rules governing interception of communications data. Sections 21 and 22, RIPA govern the current framework.

[182] Section 23(4) and (7).

[183] Section 22(7).

[184] Section 22(8).

[185] Section 57(2)(b)). See further Chapter 3 above.

[186] Directive 2006/24 EC

[187] SI 859/2009

on a blanket basis, "just in case" it should prove justifiable for a public authority to seek to access that information. This potentially exponential expansion of the storage of data about our personal lives would create a new, and JUSTICE submits, inappropriate, understanding about the role of the State in private communications.

(c) The Draft Bill

10. Part 1 of the Draft Bill closely follows the intention of the previous Government by proposing that the generation, collection and retention of data about all online and telephonic communications in the UK becomes universal, with information about us all gathered and stored without any connection to the likelihood that our communications are connected with criminal behaviour.[188]

11. Clause 1 creates a broad delegated power which will allow the Secretary of State to compel "telecommunications operators" to generate, collect or otherwise obtain new data about our communications which is neither required by providers for commercial purposes nor currently held.[189] It makes clear that the requirements which can be imposed will be very broad, including to generate, collect, retain and process data; to comply with specific standards or to use specific systems (including through the development, acquisition and use of new software or hardware).

12. However, the detail of how these arrangements will be secured is left to secondary legislation and very little information is provided in either the Explanatory Notes or the accompanying impact assessments prepared by the Home Office. No Draft Order has been produced for consideration by the Committee. Detailed arrangements will be made by a combination of Order (by affirmative resolution) and subsequent notices served on individual providers (which may not be published or provided to parliament for scrutiny).[190] Given the seriousness of the change proposed by the Draft Bill, the limited information provided for the purposes of parliamentary and public scrutiny significantly limits the

---

[188] The previous proposals initially proposed a Government database for this purpose; early in the opposition to its intent those proposals shifted to focus on compulsion of private providers to gather information about their users for the purposes of ensuring that material should be available should it be requested by public authorities.

[189] Clause 1

[190] Clause 7(1) explains that notices served and provided for by any Order made under Clause 1 must be in writing and must specify the person to whom it applies and must be given in such a way as to draw it to that person's attention. There is no requirement for publication. It is clear that the Secretary of State would be empowered to publish but not required to do so. While providers might insist on a certain degree of commercial confidence, since a significant amount of detail about how our communications data will be retained and protected from inadvertent disclosure may be in such notices, it limits the opportunity for both parliamentary and public scrutiny significantly if even the general terms of how the technology and processes envisaged by the Bill will operate in practice. Similar notices served under existing powers – e.g. under the Data Retention Regulations – have not been published. When requests for publication have been made, they have been refused for reasons of "national security".

ability of both decision makers and commentators to closely examine how the technology and procedures envisaged by the Government will operate in practice.

13. Part 2 of the Bill provides the regulatory regime for access to the data collected under Part 1. It broadly replicates the existing administrative procedures in RIPA, with the only prior judicial authorisation required by local authorities (Clause 11). All other public authorities will be able to access the data after self-authorisation following an administrative process set out in the Draft Bill (Clause 9). The list of public authorities empowered to access the data collected will be provided by Order (no draft has been provided, as the Secretary of State is reviewing whether existing authorities empowered to access communications data to continue to do so). At a high point, in 2007, 795 public bodies were eligible to access communications data under RIPA.[191] There remain over 500 bodies currently authorised under RIPA.[192]

14. Clause 14 of the Bill gives the Minister the power to establish 'filtering arrangements' for the purposes of 'facilitating the lawful, efficient and effective obtaining of communications data'. The Government has explained that the 'filtering mechanism' will be automated but will be able to search across different sources of data held by different providers to ensure the most effective answer to an individual public authority request for access to data. The Explanatory Notes make clear that the filtering mechanism may operate before a request has been formulated (that is, before an individual authority has determined that a request is necessary and proportionate).[193] The Government stresses that although this information will be processed by a Government controlled mechanism, it will be done automatically and will not allow the public authority in question to access data unless specifically authorised under Part 2. The Bill provides for the Secretary of State to delegate the operation of this filtering mechanism to another public authority. It is unclear how this filter will operate, its intended technical specifications or who its intended operator will be.

(d) Privacy, communications and data

15. That each of the distinct acts of collection, retention and use of personal information is protected by our right to respect for private life, home and correspondence guaranteed by is trite.[194] The protection

---

[191] *Freedom from Suspicion,* para 173.

[192] In his last report, the Interception of Communications Commissioner reported that 400 local authorities alone were eligible to access data (he inspected 71 of those bodies). He inspected a further 99 public authorities also authorised to act under RIPA for this purpose. See Annual Report of the Interception of Communications Commissioner 2011, HC 496.

[193] Explanatory Notes, paras 74 – 77.

[194] In *Malone v UK* (1984) 7 EHRR 14, the Court considered the attachment of a 'meter check printer' to a telephone line for the purposes of recording the time calls were made, to whom and for how long. The Court considered that the collection of this information engaged the right to privacy, but in these

of private correspondence is guaranteed by international and European law, in both Article 8 of the European Convention on Human Rights and the equivalent provision of the European Charter of Fundamental Rights.[195] The collation, retention and use of personal information are specifically protected by the domestic and EU legal framework on data protection, for example in the Data Protection Act 1998.

16. The authority for both the extension of the collection of data (in Part 1 of the Bill) and the provisions for access to it (in Part 2) must be justified separately by reference to a legitimate aim and must be shown to be proportionate and necessary to meet that aim. To avoid violating the right to respect for privacy, the statutory provisions authorising both retention and access must be "in accordance with the law":

    a. Are the provisions in the Draft Bill sufficiently clear and precise to allow individuals to understand when their data will be retained, and in what circumstances it may be accessed by the State?

    b. Do the provisions address a legitimate aim, addressing the prevention and detection of crime or other significant public interests?

    c. Has evidence been produced to show how the provisions in the Bill will benefit this aim, and to support the Government's case that the interference with individual privacy posed by the Bill would be proportionate to the benefit to be achieved?

    d. Are the proposals the least restrictive means of achieving the aim in question and have alternatives been considered?

---

circumstances could be justified by reference to the commercial need for a supplier of services to legitimately ensure a subscriber is charged correctly. This use was proportionate and justifiable. However, passing the information to the police without statutory authority and relevant safeguards against abuse was not. See, for example, paras 56 – 84. It is worth noting the gathering and collation of the information here is justified by the commercial need to retain information. The Draft Bill does not limit its effect to material already held by suppliers and operators, but will require the generation or retention of data not needed for any commercial purpose. The question of justification here goes to whether the generation or retention of this information can be justified for the purposes set out by the Home Office in connection with the potential for some communications to inform investigations and inquiries by public authorities. In *Amann v Switzerland* (2000) 30 EHRR 843, for example, the Court held that the storing of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted. In *Rotaru v Romania* (2000) 8 BHRC 449, at para 43, the Court stressed that even 'public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities'.

[195] Article 7.

e. Are adequate and effective safeguards against abuse provided in the Bill?

17. We explain below why, in our view, each of the distinct parts of the Draft Bill pose a significant risk to the individual right to privacy. As explained in one of the leading cases, surveillance often occurs without the knowledge of the individual whose rights are in play. So, in most cases an individual will never know whether his information has been reviewed or what has been retained. Only in the limited circumstances when the information is used in a trial or when an authority acknowledges the surveillance that an individual may be able to challenge its propriety. In these circumstances, there is a significant obligation on the State to ensure that surveillance powers are closely drawn, safeguards appropriate and provision made for effective oversight:

> *[it is] unacceptable that the assurance of the enjoyment of a right … could be…removed by the simple fact that the person concerned is kept unaware of its violation..*[196]

18. The Court stressed that the justification of any surveillance measures places a significant burden on States to adopt the least intrusive measures possible:

> *[P]owers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.*[197]

19. JUSTICE strongly opposes the proposal in Part 1 of the Bill to expand the generation, collection and retention of communications data. We consider that the expansion of the pool of data collected about our on and offline relationships with one another poses a significant risk to our privacy and ultimately, the Government has failed to provide evidence to support this extended provision for the capturing of data. Existing provisions under RIPA to access communications data are already extremely broad and the Government has failed to illustrate clearly why these powers are inadequate or why proposals of the breadth proposed in the Bill are justifiable.

20. The retention of data poses an interference with the right to privacy, both in its creation and in the risk that it may be accessed unlawfully or in error. As the Newton Committee reported in 2003, 'there are obvious risks to privacy in keeping information about individuals. The existence of data creates its own demand for access to it from a wide range of bodies for a variety of reasons, mostly unrelated to

---

[196] (1978) 7 2 EHRR 214, paras 36, 41.

[197] Ibid, para 42. See also Para 49: *'The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism adopt whatever means they deem appropriate'.*

national security. It also creates the potential for abuse'.[198] We therefore consider that the existing pool of communications data liable to be retained should not be expanded unless a case of strict necessity can be made out.

21. The Government must illustrate why these measures are needed. We accept that technology is changing; as is the way we communicate with each other. However, simply because it may be possible for the State to gain access to a significantly greater pool of information about our private lives as a result of this shifting technological and social base does not mean that it necessarily should.

22. We regret that the ECHR memorandum and the Privacy Impact Statement prepared by the Home Office and the other material provided to the Joint Committee falls significantly short of providing parliamentarians and the public with adequate information on its case for reform. We are particularly concerned about a number of statements made by the Government:

    a. **Expansion, not maintenance:** We take issue with the repeated assertion in the consultation document and associated materials with the assertion that these proposals are needed because a "vital tool is disappearing" or that the provisions are necessary to ensure "communications data is available…in the future as it has been in the past".[199] This is compounded by the ECHR Memorandum which refers to the "reduction in the availability of communications data" that "will have serious consequences for the UK" and the need to "mitigate the reduction in capabilities caused by the decline in the availability of communications data".[200] This capability gap is not evidenced in any of the documents associated with the Draft Bill. The Impact Assessment asserts that 'increasingly police and others are unable to get access to communications data; some data is no longer retained…for business reasons; some [providers] offering services in this country are based overseas'.[201] There is little clarification of the circumstances when communications data which would previously available is no longer, nor any evidence provided of how this gap has impacted on the ability to prevent or detect crime. Neither is information given about the Government's predictions on the impact of changing technological capabilities. In other words, the government seeks to justify the expansion of its – already considerable – powers to require the retention of communication

---

[198] Report of the Review of Privy Counsellors of the Anti-Terrorism Crime and Security Act 2001 (December 2003), para 398.

[199] Foreword, *Draft Communications Data Bill*, Theresa May.

[200] Draft Communications Data Bill, page 100.

[201] Impact Assessment, page 3

data on the basis of a series of predictions, each of which is questionable at best and speculative at worst.[202]

The motivation for this change is in the evolving way that we communicate with each other. There is no change or decrease in the capacity of the authorities to access existing data, as provided by RIPA (by issuing a notice under RIPA, a public authority can require a body to generate information not otherwise held or under an authorisation to provide data already stored). Instead, the real concern is that as we change our means of communicating, the potentially available pool of communications data is expanding. Much of the data that could be collected about how we relate to one another is not currently collected and it may be technically impossible for providers to do using their existing systems. Without any statutory compulsion or business need, there is no motivation for private providers to generate this data about their users' activities. This is explained more clearly in the Impact Assessment which accepts that the Government has considered two specific problems: (a) that certain types of data about our communications is not currently generated; and (b) that many new forms of technology are based overseas and third-party providers within the UK do not routinely store information about their users activities on these forums.

The provisions in the Draft Bill are not designed to redress a reduction in capability. Instead they are designed to increase the ability of public authorities to access information about how we communicate by widening the pool of information that is held in the UK about our activities on and offline. Specifically, they will target our use of new technologies like Facebook or Gmail which are web-based and without any need to store information about users within the UK. It will also cover private communications networks, such as those run by Blackberry or internal communications networks operated by companies and other businesses.[203]

b. **State collection of personal information:** The Government has implied that, since the data retained under the Bill will be retained by private sector providers, the obligation on the State to justify the retention is less onerous. The Government's view is that the only obligation in play on the State in these circumstances may be a "positive" obligation to effectively regulate the activities of the private sector in order to secure the safe retention of the data, including by enforcing the existing legal framework.[204]

This is potentially misleading. The State has distinct positive obligations to regulate the processing of personal information by private individuals, in order to protect individual rights.

---

[202] This reflects the last consultation on this issue undertaken by the previous Government on this issue. The JUSTICE response to that consultation is available here: http://www.justice.org.uk/resources.php/190/communications-data-collection-and-use-justice-response. See para 6.

[203] The Telegraph, *Data Watchdog questions case for e-mail snooping*, 02 April 2012. The Information Commissioner's Office referred to the expansion of the collection of communications data as a "step-change in the relationship between the citizen and the State.

[204] Explanatory Notes, ECHR Memorandum, paras 10 - 15

However, the issues raised by the Bill are far removed from the questions raised by the mishandling of personal information gathered by the private sector; for example, a failure of the State to regulate the misuse of privately gathered CCTV footage. The Draft Bill would place a compulsory obligation on the private sector to retain information which it would not otherwise need nor want. It is this compulsory obligation to retain – an act of the State, not the private sector - which must be justified. It may assist, in these circumstances, to view the providers as agents acting on behalf of the Government for the purposes of collecting and retaining data. The first question must be whether the Government has produced sufficient evidence to justify the requirement to retain. The second, whether that retention is in practice accompanied by adequate and effective safeguards for the protection of private information.[205]

c. **What does 'data' mean?:** The Government explains its view that interception of the content of communications should be considered a more serious interference than the data associated with it. However, the historical distinction about the retention of communications data and the interception of communications is not necessarily feasible in the light of evolving technology. The information recorded by a phone meter in the early 1980s is nothing, when compared to what is today recorded digitally in respect of every mobile phone call, text message or internet session. 'Traffic data' for a phone call, for instance, includes not only the numbers of the caller and the called, the time, data and duration of the call, but also data showing the location of each party, whether the nearest telephone exchange or – increasingly – GPS data. Similarly, the traffic data associated with a single email message will typically include not only the data and time of the message, when it was sent and received, etc but also the sender's login name and IP address, from which can be gained a variety of information including, in certain cases, the particular computer used and its location. Traffic data from an internet session will include similar information as well as, for instance, the URLs of websites visited (e.g. www.justice.org.uk), and the time spent on each site. In addition to so-called

---

[205] Draft Communications Data Bill, pages 96 – 99, paras 8 – 15. In this section of the memoranda, the Government relies on a series of cases which relate to the positive obligations of the State to act to protect one individual against the actions of another private individual by regulating their conduct by law, including through the criminal law. So, in *Botta v Italy,* the Italian Government had a positive obligation to enforce disability legislation against private providers to ensure access for the applicant; in *KU v Finland*, the inability to force the disclosure of the identity of the user of an internet service meant that the Government failed in its positive obligation to provide a form of redress and protection for a child whose identity had been abused online; and in *Von Hannover,* the State had an obligation to protect an individual's privacy against the publication of photographs taken in a public place by a private provider without consent. None of these cases are analogous to the proposals in the Bill and we urge the Committee to examine the evidence which the Government has provided to justify the need to compel private providers to generate, collate and retain data for its purposes closely. These cases have more in common with the cases where the Government has collated material but not necessarily used the material in practice or where it has conducted "strategic" surveillance (see for example, *Rotaru v Romania*, *Amman v Switzerland* and *Liberty v UK* (App No 58243/00, Judgment dated 1 July 2008). The Government refers to the case of *Malone v UK*, considered above, where the Court considered the collation of metering information for billing purposes legitimate and compatible with Article 8 ECHR. As explained, the collection of information for legitimate commercial reasons will involve distinct consideration to the proposal to require the private sector to retain material it would not otherwise retain for public purposes.

'traffic data', communications data also includes 'service use' data produced by service providers, e.g. itemised phone bills or internet records, and 'subscriber data'; i.e. the name and date of birth of the customer, their billing address, contact and payment details.

In this sense, the idea of communications data as being purely 'envelope data' is highly misleading: nobody writes their friend's credit card details on an envelope, still less their own. It should also be obvious that the unnecessary or disproportionate disclosure of details about a person's private communications can in some cases be every bit as damaging to that person's privacy as an actual interception of their communications, particularly when it reveals their location at a particular time and date or the fact of their contact with a specific person. Similarly, a review of a person's internet activities can allow an intimate picture to be built about their individual choices and personal history, including information about their health. Storing the sum of our annual communications data across multiple providers could create an extremely full picture of our personal preferences, activities and habits. The collation of this kind of data, accessible directly or across data sets through a filtering mechanism could have a serious impact on our right to respect for our private lives.

Others are more capable of commenting on the technological feasibility of dividing content and communications data, but JUSTICE understands that this is increasingly difficult. As a group of academics in the Information Systems and Innovation Group of the London School of Economics noted in their 2009 briefing on the government's Interception Modernisation Programme,[206] the distinction between so-called 'traffic data' relating to internet use, on the one hand, and the actual interception of the contents of a communication, on the other, is becoming increasingly blurred, particularly by the use of deep packet interception:[207]

d. **Does collecting data violate our privacy?:** The Government argues that the collection and retention of data requires a lesser degree of justification than use of data. We accept that the proportionality of individual measures will vary according to the seriousness of the interference concerned (and its potential impact) and the significance of the evidence that the measures utilised are necessary and proportionate to any legitimate aim. However, the documents accompanying the Bill give very little weight, if any, to the proposed interference with individual privacy posed by the expanded retention of communications data. Importantly, although the Privacy Impact Assessment tackles the privacy implications of access under Part 2, and safeguards associated with retention, it makes no provision or assessment of the justification for the compulsory retention provisions in Part 1. Significantly, it fails to grapple with ongoing European challenges to the Data Retention Directive; the

---

[206] LSE Policy Engagement Network, *Briefing on the Interception Modernisation Programme* (June 2009).

[207] Professor Peter Sommer of the Information Systems and Innovation Group quoted in the LSE press release, 'Home Office internet surveillance proposals won't work says LSE study', 17 June 2009.

specific implications of the collection of data for particular groups of individuals; or any wider human rights considerations associated with the generation and collection of data:

i. These provisions will operate in addition to the existing Data Retention Regulations which provide for some providers to retain certain user data for up to 12 months. The Regulations further than required by the EU Data Retention Directive. The Draft Bill would go significantly further by creating a default assumption that all information about our communications with each other might be retained "just in case", on a rolling 12 month basis, ensuring that at any one time the State will have access to an annual history of our on and offline activities. A significant number of EU countries have refused to implement the EU Data Retention Directive; and its provisions, or associated implementing legislation, declared unconstitutional by judicial authorities in a number of countries, including Ireland, Belgium and Germany. The European Court of Justice is expected to consider the compatibility of the Directive and its implementation across Europe in more detail during the next year when it considers a case referred to it from Ireland (*Digital Rights Ireland*).[208] That the Government has chosen to press ahead with the expansion of our framework for the collection and retention of communications data while this uncertainty continues at a European level is surprising.

ii. That the Government fails to grapple with the privacy impact of the retention of communications data is disappointing; but it also neglects to consider the potential impact of Part 1 on particular groups. For example, the Bar Council has, in its evidence to the Joint Committee highlighted the specific problems which may result from the collation of information generated by individuals communicating with their legal representatives, by lawyers communicating with their clients or with lawyers communicating with each other about their cases.[209] In so far as it fails to effectively recognise the right to legal professional privilege, the existing RIPA framework is flawed. That this Draft Bill fails to recognise the potentially chilling effect that Part 1 could have on the confidence of clients in the secrecy of their communications with

---

[208] See for example, *Digital Rights Ireland v The Minister for Justice and Others*, [2010] 2006/3785P. A fuller consideration of each of the challenges is provided by the European Commission in its report to the Council and the European Parliament on this issue: COM (2011) 225. http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

[209] http://www.barcouncil.org.uk/media-centre/news-and-press-releases/2012/august/bar-council-calls-for-'snoopers'-charter'-to-protect-legal-communications/

their legal advisers is worrying. Further, there are no specific exemptions provided from the scope of Part 1 at all. This could mean that individual legal firms could be required as telecommunications operators to comply with an individual notice to generate data. JUSTICE considers that this would clearly violate both the right to respect for private life and the right to due process. However, without a clear exemption, or any indication from the Government on how these particularly sensitive communications will be handled, it is difficult to be assured. Other groups are equally overlooked. Communications between Parliamentarians and lobby groups, between MPs and their constituents; the communication of journalists with their sources; and the activities of trade unions, protest groups and opposition parties will all be covered by Part 1.

iii. The internet is a vital modern resource for freedom of expression and freedom of assembly. The public reaction to the prospect that our internet use might be monitored through the retention of data about our use has been vehement. This has been replicated in other countries where increasingly draconian controls have been placed by the State on the conditions for its use (for example in other EU countries implementing the EU Data Retention Directive). That the Government has failed to grapple with the potentially chilling impact of these measures on ordinary users of these services is some cause for concern. The lack of public consultation before the Draft Bill was published is perhaps related to the Government's narrow view of its potential and perceived impact on individual users.

e. **What are the real crime fighting benefits?:** The Government's clearest assessment of the justification for retention is found in the Impact Assessment, which sets out in broad assertions the business case for reform and the expected benefits of the change proposed. However, the information provided is exceptionally slim. Expected benefits of the changes proposed in the Draft Bill are assessed at £5.0 - £6.2 billion and are based upon:

'*an analysis of criminal behaviours by the Serious and Organised Crime Agency and an analysis of the future communications market based on OFCOM and other market sources.*'

The benefits are said to accrue from preventing tax fraud and facilitating the seizure of criminal assets. However, they also include benefits accrued from 'lives saved and children safeguarded' based on standard estimates by Home Office economists. Other benefits which cannot be monetised include drugs seized, successful murder convictions and the prevention of terrorism. Without further explanation it is extremely difficult to understand how these asserted benefits have been calculated. It is clear that further evidence has been produced by the Government and Parliamentarians may wish to ask for further information.

However, nowhere in the information provided by the Government is there a clear explanation of the Government's view that the blanket collection of all communications data without connection to any specific type of communication or to the likelihood that the communications may lead to evidence of criminality can be justified. This unfortunately reflects the approach of the previous Government to the blanket retention of DNA gathered from people arrested but not convicted. The potential usefulness of successful DNA matches was inappropriately taken as the starting point for justification, as here the usefulness of access to communications data is held out as the sole pillar to support Part 1 of the Bill. However, this is inadequate for the purposes of the imposition of a blanket rule of this type, which must be examined closely for clear justification that the data retained is no more than necessary and proportionate.[210] For example, the Government makes no estimate of what proportion of the data retained is likely to be used in connection with the prevention and detection of crime; nor does it give any indication of how many cases where communication data assisted in conviction, that conviction could not have been obtained by other means; similarly, no figures are provided for the projected increase in capacity to secure convictions following the expansion of the collection of communications data proposed by Part 1. The answers to at least some of these questions must have been prepared in order to secure the financial estimates given in the Impact Assessment. However, they have not yet been disclosed.

f. **Striking the right balance?** JUSTICE considers that it is clear that the proportionality of these measures have not yet been fully explored by Government. The Government has not, satisfied the requirement for compelling evidence that these measures are strictly necessary. In our view, it is clear that they are likely to violate the right to respect for private life.

(e) The relevance of safeguards

23. The Government relies predominantly on proposed 'safeguards' against the arbitrary abuse of the new powers to support its case for reform. The case-law from Strasbourg on surveillance has focused closely on the efficacy of safeguards associated with surveillance in their examination of local laws for the protection of the national interest. As an international court, it has generally afforded a significant margin of appreciation to States in connection with State surveillance in assessing the necessity for particular measures. [211]

24. However, there can be no question that it is for Parliament to be satisfied that these intrusive measures are truly necessary and appropriate before proceeding with the proposals in the Draft Bill. Safeguards alone cannot justify the shift in the relationship between the State and the individual envisaged.

The generation, collection and retention of new data (Part 1)

---

[210] See for example, *Marper v UK* (2009) 48 EHRR 50. In that case, the Court explained that measures which operate without regard to individual impact and characteristics must be accompanied by clear justification and appropriate safeguards, concluding that the then arrangements for the indefinite retention of DNA samples taken from innocent people arrested but never convicted was disproportionate and in violation of Article 8 ECHR.

[211] *Freedom from Suspicion,* Chapter 2.

25. The safeguards outlined by the Government in connection with the expanded collection and retention of communications data are themselves limited:

    a. **Retention is limited to 12 months**. The Government explains its view that the data retained will be destroyed after 12 months (except where extended for the purposes of legal proceedings) is a significant safeguard against abuse.[212] However, this safeguard should not be overplayed. While data will only be retained for a year, the effect of Part 1 will be to create at any point in time an annual picture of the population's communications activity. This rolling diary of communications data could be kept for each individual in the country, albeit stored across multiple providers and accessed through the Government controlled filter mechanism.

    b. **Use and processing limited:** The Government also points to the express responsibility on providers to destroy the data when it is no longer lawfully held and that use of the data other than authorised by the Draft Bill will be prohibited.[213] However:

        i. This fails to acknowledge the significant number of public bodies who are already capable of accessing communications data for an extremely broad range of purposes (we return to this issue, below);
        ii. It also neglects that the larger the pool of data collated, the greater the risk that it may be mismanaged or disclosed in error. In his latest report, the Interception of Communications Commissioner refers to almost 900 self reported errors under the existing framework for access. A failure to understand the scope of the powers in the Draft Bill could lead to unlawful disclosure. However, human and mechanical error can equally lead to the unlawful disclosure of data. Both private and public bodies have, over the past five years, suffered from significant embarrassment as a result of lost data (for example the Department for Work and Pensions losing information about families claiming child benefit).
        iii. The Draft Bill and its Explanatory Notes make clear that not only will access be permitted for the purposes specified in the Bill, but for other 'lawful purposes'. The Government have explained that this could include a Court Order.[214] So, for example, disclosure might be sought in the course of civil litigation from a telecommunications provider through the use of a *Norwich Pharmacal* Order, for example, where one party to litigation argues that the provider is 'mixed up' in the dealings of the other party as a result of the use of his service for wrongdoing.
        iv. The Draft Bill provides for the Secretary of State to expand the purposes for which access is permitted by Order (we return to this below);
        v. The Draft Bill does not propose to create an offence of unlawfully disclosing data. If material is disclosed other than in accordance with the Draft Bill, it is likely that the most significant deterrent will be a fine imposed under the Data Protection Act 1998. In light of the fact that these requirements may be applied to businesses with a multi-million pound turnover, a fine may not be a significant deterrent. While we are reluctant to recommend new offences, but the limited deterrent of the existing measures reduce the limits placed on individuals subject to Part 1 requirements.

    c. **'Security obligations':** The Bill requires persons retaining data subject to Part 1 to put in place adequate security systems to govern access to the data and to protect against unlawful disclosure. Unfortunately, without further information about the technical and procedural arrangements imposed by Part 1, and the corresponding need for security, it is extremely

[212] Draft Communications Data Bill, ECHR Memorandum, para 14

[213] Ibid

[214] Clause 5. Explanatory Notes, paras 30 – 31.

difficult to assess the likely capabilities of any security arrangements. Since these specifics are likely to be confined to notices served on persons under Part 1, which may not be published, independent and impartial assessment of the effectiveness of security arrangements is likely to be impossible.

d. **Consultation and procedural guarantees**: Clause 2 of the Bill provides that when a notice is imposed, the Secretary of State must comply with certain consultation and procedural requirements. Unfortunately, these measures are entirely geared towards the protection of the interests of the persons subject to Part 1 notices, not the privacy rights of users. It provides for consultation with the person subject to requirements, with the Technical Advisory Board established under RIPA and OFCOM, none of whom have any specific obligation to consider privacy or the necessity and proportionality of the requirements being considered. We consider that while this would be a vital procedural requirement for the protection of the commercial and other interests of telecommunications operators, it adds little to the protection for individual users. There is no statutory requirement for public consultation proposed, nor is it proposed that the Information Commissioner's Office would be consulted.

e. **The role of the Information Commissioner's Office:** Part 3 of the Bill provides a new role for the Information Commissioner in relation to data held under Part 1. The Commissioner is required to keep under review the operation of measures relating to data security; the destruction of data and any provision in any Clause 1 Order which relate to data security (Clause 22(5)). While we welcome the recognition of a role for the Information Commissioner, we note that the proposed duties echo and supplement existing statutory functions which exist under the Data Protection Act 1998. While specific statutory functions here provide a degree of specific scrutiny, these are in themselves limited to data security. The Information Commissioner is not empowered to consider the necessity or proportionality of any specific requirement or any issues relating to access by a public authority to data. These functions are reserved to the Interception of Communications Commissioner. In any event, the Information Commissioner has himself questioned whether without significant further resources he would be capable of conducting the review proposed in the Draft Bill.

f. **The role of the Interception of Communications Commissioner:** We consider that the oversight of the Interception of Communications Commissioner ('ICC') under the existing RIPA procedures is inadequate to protect the individual right to privacy. The provisions in the Draft Bill extend the existing measures to the new proposals in Parts 1 and 2 with little or no modification. We address the work of the ICC below.

Access to data (Part 2)

26. That the provisions in Part 2 broadly replicate the provisions in RIPA for access to communications data is disappointing. JUSTICE considers that there are a significant number of flaws within RIPA which are magnified when applied to the proposed expansion of data generation in Part 1. Principally, we are concerned that these powers will continue to be exercised by a far greater range of bodies than may be strictly justified and for purposes which are not necessarily proportionate in light of the impact of compulsory surveillance powers on individual privacy. As explained above, the bodies which will exercise the right to access data under the Draft Bill have not yet been finalised.

27. The purposes which trigger the right to access data gathered under Part 1 broadly follow those outlined in RIPA. JUSTICE considers that the purposes outlined in RIPA are already overly broad. Measures designed as compulsory powers for surveillance by the State may be essential for the investigation of serious crime, but as the purposes in RIPA devolve from the prevention and detection of serious offences the risk that they will be used disproportionately increases. When RIPA was introduced, the

only bodies to exercise powers under the Act were the police, intelligence services and HMRC. While the powers under the Act might appropriately be extended to other law enforcement agencies and the emergency services, its extension to other bodies should be justified by reference to the strict necessity test identified by the Strasbourg Court. When these powers are extended to the investigation of minor criminal or regulatory offences such as fly-tipping, or for administrative purposes, such as the checking of school catchment, we consider that their use is highly likely to be disproportionate. That is not to say that such minor offences are not important or deserving of investigation. Rather it is that the harm involved is by definition insufficiently serious to justify the inherent risk that surveillance poses to the privacy of any person under suspicion. Similarly, in connection with the use of these powers for other purposes (such as the identification of persons), less intrusive forms of investigation are likely to be an equally effective and therefore more proportionate means of investigating minor crimes than the resort to surveillance powers.[215]

28. In addition, many of the safeguards relied upon by the Government are also based upon the flawed procedural arrangements of RIPA:

    a. **Authorisation:** JUSTICE considers that the administrative authorisation procedure provided for in Clauses 9 and 10 provide for inadequate independent scrutiny of the need for access to data. These provisions are largely modelled on RIPA. In *Freedom from Suspicion,* we explained our view that prior judicial approval should be the default authorisation mechanism for most surveillance activities, including access to communications data. While it is no doubt true that senior members of organisations are typically well-placed to supervise the operational decisions of their subordinates, and more mindful of their ultimate accountability to the public, it is also clear that senior and junior members of the same organisation will inevitably share an interest in achieving the necessary results. The relative seniority of a Police Superintendent would not normally be enough, for instance, to make her sufficiently objective to authorise a search warrant, unless it was a genuine emergency and there was not sufficient time to approach a judge. Still less is it realistic to expect a Deputy Chief Inspector to be sufficiently independent of an investigation being carried out by his subordinates in the Trading Standards Service, for example, to objectively assess whether secretly accessing someone's communications data is a necessary and proportionate interference with their right to privacy.[216]

       Although the Courts have stopped short of expressly requiring prior judicial authorisation in all cases, in many cases it has been considered essential. It is seen as the paramount means of protecting individual privacy in instances where the individual themselves may be unaware that their information is being handled. In those cases where no form of prior judicial oversight has been available the other safeguards imposed by domestic arrangements for surveillance have been robust and scrutinised extremely closely and the measures in question have been subject to robust review after the event.[217] For example, in a recent decision involving retention of information about a student, the Court said:

       > *The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be*

---

[215] *Freedom from Suspicion,* paras 180 – 181.

[216] See e.g. LSE Policy Engagement Network, *Briefing on the Interception Modernisation Programme* (June 2009), p30: 'now seems a good time to question whether a senior official in an organisation with an interest in the outcome of an investigation is the best person to judge the application for access to communications data made by a junior figure in the same organisation'.

[217] See for example, *Uzun v Germany*, App No 35623/05, 2 September 2010.

carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure. [218]

b. Proportionality and necessity: The requirement in the Bill that only authorisations which are proportionate and necessary should be a significant safeguard against abuse. The Bill requires that the measures in question be proportionate to the goal to be achieved. Since access engages privacy, this requires public authorities to effectively apply the Convention test set out above to each access authorisation. Unfortunately, in practice, the application of this restriction in RIPA has not proved a significant barrier to access. Neither public authorities, individual officers or the Interception of Communications Commissioner appear to have applied a rigorous review of the proportionality of existing requests from a human rights perspective.

For example, in the context of restricting access of local authorities to communication data, the Interception of Communications Commissioner considered existing powers exercised proportionately as requests from local authorities made up a low proportion of overall requests and there had been very few errors self-identified by local authorities. He also considered the use of RIPA for the purposes of pursuing fly-tipping an appropriate and proportionate use of compulsory surveillance powers, regardless of other means of investigation.[219] He failed to consider whether the use of the powers in individual cases had been justified. Similarly, during the Joint Committee's evidence on the Draft Bill, it has been suggested that the police use these powers for "non-crime" purposes and for low level traffic offences.

There is, an inherent risk in any criminal investigation involving intrusive surveillance that the resulting invasion of privacy will in hindsight prove to have been unnecessary because the initial suspicion turns out to be false: what Lord Neuberger described as one of the paradoxes of surveillance.[220] This inherent risk can be minimised by, for example, requiring that less intrusive means be considered first, but it can never be eliminated.

Whether it is proportionate, therefore, to run the risk of invading someone's privacy in the knowledge that they may turn out to be innocent depends on several factors, including the reasonableness of the suspicion *but also* the seriousness of the offence in question. It is the difference, in other words, between breaking down the door to someone's hotel room because you think they are being murdered, and breaking down to door to their hotel room because you think they have stolen your toothbrush. In both cases, your suspicion may be very well-founded but there is also an inevitable risk that you are mistaken. And should it turn out that you are mistaken, the reasonableness of your suspicion will be of little comfort to the person whose privacy you have unnecessarily invaded. But at least in the case of suspected murder, we would say that the seriousness of the suspected offence, combined with the reasonableness of your suspicion helped to excuse your actions. The same could not be said of the toothbrush.[221]

Unfortunately, there is little evidence that this test is being applied appropriately in practice or that it operates as a significant safeguard for personal privacy.

---

[218] *Rotaru v Romania* (2000) 8 BHRC 43 at para 59.

[219] *Freedom from Suspicion,* paras 172 – 181.

[220] *In re McE* [2009] UKHL 15 at para 111.

[221] For further information about the application of the proportionality test in this context see: *Freedom from Suspicion,* paras 172 – 181.

c. The role of the Interception of Communications Commissioner and the Investigatory Powers Tribunal: The role of the Interception of Communications Commissioner and the Investigatory Powers Tribunal is not capable of providing adequate, independent and transparent review to provide reassurance that individual privacy is respected in the operation of RIPA. As explained above, ex-post judicial review may be adequate in order to ensure respect for private life only where that review is accompanied by adequate existing safeguards to ensure that individual rights are afforded appropriate respect. Unfortunately, review by the ICC and the IPT is significantly lacking. Both mechanisms are fundamentally flawed. As we explain in *Freedom from suspicion*:

i. Review by the ICC is by way of 'dip-sample' and the self-reporting of errors. This means that only a handful of the almost 500,000 requests for communications data a year are reviewed (for example, there were 895 individual errors self-reported to the Commissioners office during the last reporting period; and he inspected less than 200 individual public authorities exercising powers in connection with communications data);

ii. Between 2005 and 2010, no reports were made that any public authority decision had been disproportionate or unnecessary. In 2011, the Commissioner reported that in one case it had been reported that powers had been used inappropriately. However, this latter case involved use of communications data powers in connection with school admissions, an issue which had been considered by the IPT in the *Paton* case and held disproportionate (and which had been covered significantly in the press during 2011). As the Commissioner highlights in his report, this is the only case in which his inspections have identified an inappropriate use of these powers.[222] Given that there have been probably somewhere close to three million requests made since January 2004, this suggests either a degree of effectiveness in public body decision-making that approaches infallibility, or more likely, that the Commissioner's oversight is ineffective.

iii. The IPT lacks transparency and any of the procedural safeguards associated with accessible redress or effective oversight offered by ordinary tribunals. The likelihood that individuals will become aware of surveillance is low (in the *Paton* case, the surveillance came to light due an error made by a local authority employee), making bringing a case before the IPT extremely unlikely. When cases are brought, they may be argued in secret, and in the absence of the applicant and their legal team. If a case proceeds to a decision by the Tribunal, the applicant may only be told if he has won or lost and may be significantly deprived of any reason for the decision in the case.[223]

d. **Filtering:** The Government refers to the filtering arrangements in the Draft Bill as "minimising" the likely interference with Article 8 rights posed by requests for access.[224] As explained above, we find this argument extremely difficult to follow. There is very little information available about how the filtering mechanism will operate. However, what has been explained is that this mechanism will allow the Government to "join up" data sets held by numerous providers to provide a fuller picture relevant to a request. This mechanism will enable the creation of an extremely full picture about an individual's private life – or the activities of a group of individuals. This information will be accessed before a request is

---

[222] 2011 Annual Report of the Interception of Communications Commissioner HC 496, page 44.

[223] A fuller critique of the ineffectiveness of the IPT is provided in *Freedom from Suspicion,* at Chapter 9.

[224] Explantory Memorandum, para 21

authorised, albeit within the filtering process. This in itself would appear to create a greater risk to individual privacy, not an additional safeguard. Without significant further details on the technical and procedural arrangements for the operation of the filter, including which public authority will operate it, it is impossible to provide a reliable and clear analysis of the risks associated with its functioning.

e. **Repeal of General Powers:** The ECHR Memorandum and the Privacy Impact Assessment includes the decision to repeal certain general powers to access data within the Government's assessment of the proportionality of these measures.[225] JUSTICE have called for the repeal of these general powers, which would most likely fail any Convention challenge if one were brought, for lack of legal certainty or appropriate safeguards. The Government committed in its counter-terror review published in January 2011 to rationalise the bases by which communications data could be acquired.[226] We welcome the decision to repeal these provisions. However, this decision should not be treated as a trade-off or a *quid pro quo* for the expansion of data collected.

(f) Time to rip up RIPA?

29. The introduction of the Draft Communications Data Bill provides an ideal opportunity for Parliament to consider the underlying legal framework for the existing broad powers of state surveillance in RIPA. The existing pool of communications data liable to be retained should not be expanded. Instead, RIPA should be revisited with a view to significant reform. In so far as access to communications data is concerned:
    a. **Public authorities:** The number of public authorities able to access communications data should be significantly reduced; and ideally limited to the police, law enforcement agencies intelligence and emergency services and to any other bodies dealing with serious criminal offences;
    b. **Access:** The purposes for which communications data may be accessed should also be revised, with a view to limiting significantly the circumstances when communications data may be used proportionately. While the requirement that the measures should only be exercised when necessary and proportionate should be a significant limitation on the circumstances when data requests are made; in practice this has not operated as a particular restriction to administrative authorisation;
    c. **Prior judicial authorisation:** The default for the majority of requests should be prior judicial authorisation. This will significantly increase the independence of the oversight mechanisms in play and the likelihood that data will only be accessed when necessary and proportionate. Exemptions may be considered to allow police, law enforcement agencies, intelligence and emergency services access to limited subscriber data (including information about account holder's name, address and contact details, for example) and for access in emergency situations to other data (subject to a subsequent judicial authorisation within a reasonable period, for example, 48 hours).[227] Some objection has been raised about the use of prior

---

[225] Explanatory Memorandum, para 21.

[226] Cm 8004, January 2011, page 5.

[227] An exception based on ad-hoc supervision could be carved out for law enforcement bodies acting in an emergency (as explained above and in *Freedom from Suspicion*). The bulk of requests for communications data relate to requests from the police, law enforcement and other agencies for subscriber data. (Between 2005 – 2011, the proportion of requests has been between 54% and 80%. See *Freedom from suspicion,* para 160. See also 2011 Report of the Interception of Communications Commissioner.) Access to limited subscriber data (such as name, address and contact details) by the police and other law enforcement agencies or emergency services might justifiably be exempted and subject to administrative authorisation. However, we note that although the definition of subscriber data used in the Bill reflects the provision in RIPA, the application of that definition to the new

judicial authorisation in connection with administrative difficulties, the need for speed and costs. We consider that these difficulties should not be overplayed, particularly in light of the breadth of the powers being exercised and their implications for personal privacy.

d. **Review and oversight:** If prior judicial authorisation is in place as a default, the importance of subsequent review will be less significant and less onerous. However, we have recognised that independent monitoring and review of decisions made and the operation of the legislation would be sensible. In our view, this should be conducted by the Information Commissioner in connection with non-law enforcement activities and by the Surveillance Commissioners in so far as review is necessary in connection with the activities of the police, law enforcement and intelligence agencies.[228]

(h) Conclusion

30. These proposals have been presented by Government as an innocuous and technical shift necessitated by degradation in existing investigatory powers. Instead, the Draft Bill creates a platform for the Government to collate information about each of us which would allow an undefined list of public authorities access to a rolling annual diary of our on and offline personal lives for an extremely broad range of purposes. This would be a step-change in the way information about our conduct is stored, being collated "just in case" it may be useful for State purposes.

31. We urge the Joint Committee to reject the Government's case for reform and to call for renewed focus on the failings of our existing law on surveillance before further legislative expansion of the collection of personal data is pursued.

August 2012

Annex – Call for Evidence: The Committee's Questions

In our written evidence, we have focused on our key concerns about the Bill.

We provide below short summary responses to a number of the questions issued by the Committee, for ease of reference. These summary responses should be read together with our full submission and paragraph numbers are provided for cross-reference. That we have not provided an answer to one of the Committee's questions should not be read as support for any part of the Bill.

General:

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

- JUSTICE does not consider that the Government has made a convincing case for reform. The powers provided for in the Draft Bill are extremely broad and the justification provided is entirely lacking in evidential support. They supplement an already broad legal framework for surveillance in RIPA, which in our view, lacks the essential substantive and procedural safeguards necessary for the protection of individual privacy.

---

proposals to gather data in Part 1 will expand its effect (for example, subscriber data might include a Facebook profile, information held by a university network about its students, including for example, transcripts, or by employers about their employees). We would consider prior judicial authorisation as a default the appropriate trigger for access to this kind of data.

[228] Further, more detailed information about JUSTICE's recommendations for reform can be found in *Freedom from Suspicion,* at pages 85 -86. See Annex 2

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

- The proposals in the Draft Bill would create a blanket authority for generation and collection of unprecedented amounts of information about how we all communicate in the UK, whether on or offline. We consider that its provisions pose a serious risk to our right to respect for privacy.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

- These provisions will operate in addition to the existing EU Data Retention Regulations which provide for some providers to retain certain user data for up to 12 months. The Regulations go far further than required by the EU Data Retention Directive. The Draft Bill would go significantly further by creating a default assumption that all information about our communications with each other might be retained "just in case", on a rolling 12 month basis, ensuring that at any one time the State will have access to an annual history of our on and offline activities.
- A significant number of EU countries have refused to implement the EU Data Retention Directive and its provisions, or associated implementing legislation, declared unconstitutional by judicial authorities in a number of countries, including Ireland, Belgium and Germany. The European Court of Justice is expected to consider the compatibility of the Directive and its implementation across Europe in more detail during the next year when it considers a case referred to it from Ireland (*Digital Rights Ireland*). That the Government has chosen to press ahead with the expansion of our framework for the collection and retention of communications data while this uncertainty continues at a European level is surprising.

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

- As explained above, the legality of the provisions in the EU Data Retention Directive is subject to review. JUSTICE has commissioned further research on the relevance of the EU Framework for the debate on the Bill. If this is available while the Joint Committee's inquiry is ongoing, we will provide it to members.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

- We consider that these measures pose a significant risk that they will violate the individual right to respect for privacy in practice. Rights cannot be swopped like trading cards. If interference is identified, the only way of addressing the violation concerned is to remove the interference or to adopt additional safeguards to reduce its impact. Removing unrelated but offending measures cannot provide redress.
- That the Government's Memorandum on the ECHR and the Explanatory Notes accompanying the Bill present the repeal of a number of general powers for public authorities to obtain information as a "quid quo pro" for the provisions in the Bill or an additional safeguard for personal privacy is inappropriate. Each of these ill-defined general powers were liable to challenge regardless of the introduction of the new measures in the Bill.

  While their repeal is welcome, this should not be treated as a "trade-off" for the equally ill-defined and contentious powers in the Draft Bill.

Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?
12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

- The number of public authorities currently able to use surveillance powers under RIPA has expanded exponentially. We consider that the number of bodies capable of using surveillance powers more generally is disproportionate. Equally we are concerned that the use of surveillance powers disproportionately in connection with administrative or regulatory offences and minor crimes is inappropriate and consider that the purposes for which surveillance powers might be used should be revisited.
- The Secretary of State seeks the flexibility of a discretion to expand the scope of the powers in the Draft Bill, arguing that the repeal of general powers may require the expansion of the scope of the Draft Bill as bodies make a business case for the use of the powers therein.

  JUSTICE considers that many of the general powers are ripe for repeal and that alternative means of pursuing the functions they were determined to serve are available without resort to surveillance. That the necessity for the use of these powers has not been explored at this stage is a cause for concern, not justification to provide the Secretary of State with a delegated power to revisit the list of bodies which are able to access our communications data.

Use of Communications Data:
14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

We consider that the existing provision for access to communications data should be reviewed, with a view to restricting the number of public bodies who can use these powers. Ideally the powers should be used principally for the prevention and detection of serious crimes and by bodies with functions designed for that purpose.

Safeguards:
16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?
18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

We consider that the existing framework for access to communications data should be amended to provide for prior judicial authorisation as a default in most cases. We consider that the oversight offered by the Interception of Communications Commissioner does not provide adequate scrutiny to protect the individual right to respect for privacy.

Parliamentary Oversight:

32. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

- We consider that there is very limited provision for parliamentary oversight in the Draft Bill. The Draft Bill and its accompanying documents provide little detail on how the measures proposed will work in practice, including how safeguards will be formulated. The Committee has not been provided with any Draft Order which would provide a fuller picture of how the Government proposes to proceed.

- The Draft Bill would achieve its goal by a combination of Order (affirmative resolution) and notices (governed by the Order and not necessarily published). We consider that the lack of detail about the proposed Orders, and the lack of transparency which will operate in the notice scheme significantly limits the opportunity for effective parliamentary scrutiny of the impact of these measures on the right to privacy in practice.

Technical:
22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?
23. How safely can communications data be stored?
24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

- These questions are best addressed by others with greater technological expertise. However, there is limited information available on the technology which the Government intends to use, and it is clear that it is expected to vary according to the arrangements in place with each provider or operator. This information will likely be included in notices which may never be published and the opportunity for independent scrutiny of the effectiveness of the technology utilised will be extremely limited

- Storage of personal data by the public and private sector is notoriously difficult. Errors have occurred in both human and automated systems which have led to the inadvertent disclosure of information unlawfully.

- As we explain above, we regret that the filtering arrangements provided for in the Bill are far from clear or appropriate.

Annex 2
Freedom from Suspicion: Chapter 4

August 2012

Sir Paul Kennedy

Please accept this as a response to the five questions in your letter dated 17th July 2012. In addition Annex A (attached) contains my written evidence in relation to the draft Communications Data Bill. My written evidence only addresses the questions that are relevant to my role or those in relation to which I am able to contribute evidence.

1. How would you wish to change your communications data request inspection regime in light of the proposals in the draft Bill and if costs were no object? What new powers and resources would you require to satisfy yourself that you could really get to the bottom of whether every public authority was using its powers correctly and if not why not?

The draft bill does not change the current application or authorisation process for the acquisition of communications data by public authorities. The same tests of necessity and proportionality must be met and the requests must be authorised by a senior officer from each relevant public authority. The current inspection regime works well and I regard it as robust. As such, I do not anticipate changing my current oversight regime in relation to the acquisition of communications data by public authorities as a result of the bill. My latest annual report outlines the current inspection regime (2011 Annual Report - Section 7.2).

As part of the current inspection regime applications are scrutinised to ascertain whether public authorities have used their powers correctly. During the local authority and 'other' public authority inspections (such as Gambling Commission, Information Commissioners Office etc) it is usually feasible for my Inspectors to check every application. As a result I am satisfied that these public authorities are using their powers correctly, or that my Inspectors have reported on cases where they are not. It is obviously not feasible during the inspections of the larger users, such as police forces, to examine every application and instead a random sample is selected from the public authority's database and from some of the communication service providers (CSPs) systems. Arguably it is less likely that the larger volume users would inappropriately use their powers, as the Single Points of Contact (SPoCs) in these organisations are full time communications data staff who are trained to a high level. They robustly perform a guardian and gatekeeper role. However it would be helpful if the record keeping requirements (specified in paragraph 6.5 of the current Acquisition and Disclosure of Communications Data Code of Practice) were extended to collect statistics in relation to the number of applications (rather than just the number of authorisations and notices), the necessity purpose under which the data was acquired (such as prevent / detect crime etc) and the specific offence / crime under investigation. This would enable more meaningful conclusions to be drawn and would provide a further indication as to whether public authorities are using their powers appropriately.

The proposals in the draft bill would extend my oversight in two areas. First, my role would be extended to oversee the collection of communications data by CSPs. Second, my role would be extended to oversee the operation of the filtering arrangements. In order to carry out this additional oversight it is likely that more resources will be required as my Inspectorate is already working at full capacity. However until the technical details of this oversight are determined (i.e. number and frequency of CSP audits, format of filtering oversight, etc.), it is not possible for me to comment on the extent of the extra resources required.

2. Your 2010 annual report states (at para 7.26) that while a good label of independence and objectivity exists in the Designated Persons approvals process in most organisations, the exception is Special Branch and Professional Standards. I would like a report on what was going wrong in these organisations and what steps were taken to address these issues during the last year.

This statement related to two specialist departments - Professional Standards (PSD) and Special Branch (SB) - which exist within the majority of police forces and law enforcement agencies (LEAs). During the police force and LEA inspections, the applications made by these two specialist departments are always scrutinised due to the fact that there might be slightly different systems and procedures in place. In 5 of the 40 police and LEA inspections that were undertaken in 2010, my Inspectors were concerned that the Designated Persons (DPs) were not independent in either one or both of these specialist areas.

Paragraph 3.11 of the CoP outlines that "*DPs should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reason. Where a DP is directly involved, their involvement and their justification for undertaking the role of DP must be explicit in their recorded considerations.*" Due to the sensitive nature of the work undertaken by SB and PSD it is accepted that on occasions, for reasons of security, a person who is directly involved in an investigation may need to act as the DP. This is permissible, but in such cases the DPs must ensure that their involvement and their justification for undertaking the role is explicit in their recorded considerations.

Essentially, my Inspectors identified that the DPs who were scrutinising the applications in one or both of these specialist areas in 5 police forces and LEAs were directly involved in the investigations, but were not making this explicit in their recorded considerations. This conduct constitutes non-compliance with the CoP. However the applications were lawful as they were approved by a DP of the required rank. I can report that recommendations were made for these 5 public authorities to take corrective action and they are now compliant in this respect. My Chief Inspector disseminates the most frequent recommendations (of which this was one) to all police and LEA SPoCs on an annual basis to enable them to review their systems and procedures. In my 2011 Annual Report (page 34, paragraph 3) I commented that there is now a good level of compliance in this area. I can further report that this issue has not been identified in any of the police force or LEA inspections conducted to date in 2012.

3. Your report states (at para 7.27) that three police force professional standards departments requested communications data for disciplinary investigations rather than for criminal investigations. Was this breaking the law or only the voluntary code of practice?

My report stated that <u>two</u> police force professional standards departments requested communications data in relation to disciplinary investigations where there were no criminal offences under investigation. Such conduct constitutes a breach of Part I Chapter II of RIPA. The communications data in these cases was not acquired in accordance with the law due to the fact that communications data can only be acquired if it is necessary on grounds falling under Section 22(2) of RIPA.

It is also worth noting that the Acquisition and Disclosure of Communications Data Code of Practice is not voluntary (See Sections 71 and 72 of RIPA). The Code of Practice is issued by the Secretary of State and is admissible in evidence in criminal and civil proceedings.

4. Your report notes (at para 7.28) a very significant increase in the use of the urgent oral process for acquiring communications data. Were you satisfied that this increase was justified? You noted that record keeping with 87% of the police forces and law enforcement agencies was good or satisfactory in

this area. What type of mistakes were seen in the other 13% of agencies? What steps have been taken to improve the problems with record keeping in these agencies and how have things changed since 2010?

Essentially yes – this process is still predominantly used in life at immediate risk cases. As you will see from my 2011 annual report, 90% of public authorities inspected in 2011 are achieving a good standard in this area overall. My 2011 annual report outlines that one serious compliance issue (blanket or rolling authorities) was identified in a small number of the urgent oral requests in 3 police force inspections (Page 35 Paragraph 2). As I outline in my report, I was satisfied that these instances were not wilful or reckless failures, however it is still important to ensure that the correct process is always applied and that the data is acquired in accordance with the law. The 3 police forces have taken corrective action in this area to prevent recurrence.

The majority of the other recommendations in this part of the process relate to the quality of the contemporaneous record that is maintained during the urgent oral process – in some police forces and LEAs this record was not sufficiently completed and as a result there were gaps in the audit trail or an incomplete record of the actions taken and decisions made. In such cases, my inspectors discuss the individual investigations with relevant staff and examine other available documentation (such as incident logs and policy books) to satisfy themselves that the process was used appropriately. The frequent recommendations in this area have been disseminated to all SPoCs to enable them to review their systems and procedures. Good practice templates in this area have been shared by public authorities and adopted by those who had failings in this area.

5. You note (at para 7.34) that the Security Services were responsible for some significant and recurrent breaches of the Code when data requests were regularly approved by Designated Persons of insufficient rank. What penalties do you think should exist when an organisation repeatedly breaks the Code?

The instances described above represented breaches of Part I Chapter II of the Act as the DPs were not of the prescribed rank / level. This was not a wilful or reckless failure to comply with the legislation and the errors were caused by an incorrect system setting which unfortunately went unnoticed. It is important to make the point that these errors had no bearing on the actual justifications for acquiring the data (i.e. the requests were necessary and proportionate) and furthermore, that no collateral intrusion occurred in relation to these requests. I was satisfied with the measures put in place to prevent recurrence of the error.

Should I establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the Act in relation to the acquisition or disclosure of communications data, I shall, subject to safeguarding national security, inform the affected individual of the existence of the Investigatory Powers Tribunal and its role.

Furthermore, a number of pieces of legislation and offences already exist to address instances where communications data is requested inappropriately, i.e., malfeasance in public office, Data Protection Act offences etc. If the investigation results in a court case, the public authority risks having the communications data evidence ruled as inadmissible if it has not been obtained in accordance with the law. The ultimate penalty would be for the public authority's powers to be removed by Parliament. I see no current need for further sanctions.

I would of course welcome any further questions you have in relation to my 2011 Annual Report to the Prime Minister once the Committee has had time to study it.

Annex A

Submission of Written Evidence to the
Joint Committee on the Draft Communications Data Bill
by Sir Paul Kennedy Interception of Communications Commissioner

Question 2: Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

1.1 It is clear that the intention of the new powers is to ensure that communications data continues to be available to public authorities. I believe that it is right to update the legislative framework so far as is necessary to ensure that there is a continuing capability to obtain communications data. A strong case is made that without the new powers there will be a decline in capability.

Question 3: How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

1.2 The draft bill does not change the current application or authorisation process for the acquisition of communications data by public authorities which is human rights compliant. The same tests of necessity and proportionality must be met. Requests will only be made by the public authorities approved by Parliament to acquire data and the requests will be approved by a senior officer who must believe the tests of necessity and proportionality have been met.

1.3 The new powers will also provide for filtering arrangements, which will reduce the amount of communications data that is disclosed to a public authority when more complicated data requests are made, thus reducing the intrusion into privacy.

1.4 In addition the draft bill will close the loophole through which local authorities and some other public authorities are able to use other powers (such as the Social Security and Fraud Act 2001) to acquire communications data. I welcome this and have expressed concerns in the past that two regimes exist for acquiring communications data in some public authorities. The current RIPA process (to be replaced by the CD bill) is a robust system, under which all applications are scrutinised by a trained and accredited SPoC prior to being considered and approved by a DP who holds a senior position in the public authority. The oversight of the exercise of RIPA powers is my responsibility and the means of redress for complaints is through the Investigatory Powers Tribunal. Other pieces of legislation that are currently used to acquire communications data do not have any such oversight. The draft bill will remove these other statutory powers with weaker safeguards.

Question 12: Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

1.5 The powers should not be limited to just police and intelligence agencies. Parliament has delegated statutory enforcement functions to a number of other public authorities and as a result they have a clear statutory duty to investigate a number of criminal offences, some of which are their sole responsibility. Often the criminal offences that these public authorities investigate are regarded as very important at a local level and provide the public with reassurance and protection. For example, local authorities use

communications data to identify criminals who persistently rip off consumers, cheat the taxpayer, deal in counterfeit goods, and prey on the elderly and vulnerable. The statistics provided to my office show that such other public authorities accounted for just over 1% of the total requests submitted in 2011. The volume of requests is low, but this does not mean that such public authorities should not be able to use the powers when they can demonstrate necessity and proportionality. It is sensible to take the opportunity to review the current list of public authorities who have access to ensure that it is still required, but the power to vary the list of authorised authorities by Order is valuable and should be retained. It enables the Secretary of State to respond to changing circumstances and emerging needs.

Question 14: Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

1.6 The draft bill does not change the current application or authorisation process for the acquisition of communications data by public authorities which is human rights compliant, apart from the addition of one more statutory purpose relevant to the Financial Services Authority. The same tests of necessity and proportionality must be met. Requests can only be made by the public authorities approved by Parliament to acquire data and any requests will be approved by a senior officer who must believe the tests of necessity and proportionality have been met. The majority of communications data requests are submitted for the purpose of preventing or detecting crime, but communications data may also be required for other purposes, such as in order to prevent death or injury or in the interests of public health.

1.7 It would be difficult to set a crime threshold for the use of communications data for a number of reasons, even by reference to the gravity of the offence. Previous statutory attempts to define serious crime have not produced satisfactory results (e.g. in relation to minimum sentences) and some "less serious" offences can have very serious impacts on the victims. It is therefore much better to leave it to the authorising officer to decide, in relation to the facts of each individual investigation, whether the application to use communications data to detect it is necessary and proportionate.

Question 15: Is the proposed 12 month period for the retention of data too long or too short?

1.8 On the basis of the information at present available 12 months seems to be an appropriate period, but it should be open to review in the light of experience

Question 16: Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory?

1.9 There is a robust application and authorisation process in place to acquire communications data. Each application has to be vetted and quality assured by an accredited SPoC before being considered by a DP. I have observed that public authority staff undertake this internal scrutiny with dedication and integrity. There is a robust system in place to prevent anyone other than an accredited SPoC from acquiring the communications data from the CSPs and this is an important safeguard.

1.10 A DP must be a senior officer in that public authority whose rank / level has been prescribed by law. This system is satisfactory. It is important to ensure that the designated senior officers are comparable in terms of rank / grade / level across the various public authorities that have access.

Question 17: Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances?

1.11 A warrant system would not be appropriate for communications data requests in the same way that it is for interception warrants. The volume of communications data requests is too high in comparison to interception warrants to make this feasible and in addition communications data requests are significantly less intrusive than acquiring the content of communications.

1.12 I am not convinced that the Government's proposal to require all local authorities to obtain the approval of a magistrate before they can use these powers will have much impact other than to introduce unnecessary bureaucracy into the process and increase the costs associated with acquiring the data.

Question 18: Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

1.13 It is crucial for there to be independent and robust oversight of these powers. The division of the oversight between the Information Commissioner and the Interception Commissioner is clear and appropriate. I am supported by a Chief Inspector and five inspectors who are all highly trained in relation to the acquisition and disclosure of communications data. My team has a good understanding in relation to how the human rights principles of necessity and proportionality apply to the acquisition of communications data and the extent to which communications data may assist public authorities in carrying out their functions. I will continue to provide oversight in relation to the acquisition of communications data, and in addition I and my successor will also oversee the collection of communications data by CSPs and the filtering arrangements. These two additional functions require a level of technical knowledge and expertise which is present in my staff. The Commissioner will continue to report to the Prime Minister annually with respect to the carrying out of his functions.

Question 20: Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

1.14 The present regime is effective because the participants are co-operative. It is important that their co-operation is maintained.

Question 21: Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for the draft Bill amount to an offence?

1.15 My experience is that all public authorities try hard to co-operate, and welcome assistance to enable them to do so. They admit their mistakes, and try to devise ways to avoid any repetition. All of that could be jeopardised by increasing penalties, and I fail to see what would be gained.

August 2012

Mr J R S Kistruck

1 Effectiveness

The purpose of the proposal is to make communications patterns visible to the authorities. This depends on the idea that identifiable persons or organisations use the same communication endpoints (such as email addresses, phone numbers and IP addresses) over substantial periods of time.

Any half-intelligent criminal, following this bill, will use frequent changes of address and phone number, among perhaps hundreds at any one time, in order to fragment and confuse the patterns visible to any investigator. The techniques for this style of evasion are already well-developed among the hacker community. They will spread, and cause a slight increase in communications costs for criminals because of the inconvenience. Unfortunately, the extra cost to the baddies will be much less than the extra cost to the rest of us, and it will not even slow them down.

The proposal will therefore be ineffective for its primary purpose.

2. Wide accessibility

Making communications data accessible to the police and the security services might be justifiable if it were effective. Making the same enormous range of data accessible to other public bodies is quite a different proposition. Few people would trust local offices of the DWP with their personal communications data, let alone the interested officers of local councils.

Any assurance that "we won't allow that in the rules" is not worth the paper it would be published on. Once the data is on file, the uses of it will creep outwards step by step, and each step looks small to the government that allows it. Within ten years use of that data would be widespread, and vested interests would be too big to let it be given up.

3. Safeguards

If the bill goes ahead, the information about most people's communications will be held by a modest number of well-defined private companies, the ISPs. They are large, bureaucratic institutions, run by ordinary human beings largely governed by procedures. There will perforce be people and procedures for recovering the data about past communication patterns. Those people and those procedures will be vulnerable to error and to corruption.

Where there is a strong incentive to investigate, mere procedures will not stand in the way. The history of the News of the World phone-hacking scandal shows just how easy it is for 'safe' repositories of information to be breached when enough money or other interest is involved. Note that this is a *human* problem, not a technical one!

Reviewing the history of known leaks and losses of personal information both from the private and the public sector over the last five years, no reasonable person would willingly trust their data to such a scheme.

August 2012

The Law Society

The Law Society of England and Wales ("The Society") is the professional body for the solicitors' profession in England and Wales, representing over 150,000 registered legal practitioners. The Society represents the profession to parliament, government and the regulatory bodies and has a public interest in the reform of the law.

I. Historically English law has protected privacy in particular circumstances but has never accepted a general right to privacy. The Human Rights Act 1998, by incorporating the European Convention on Human Rights (ECHR) into English law, changed that. Via the incorporation of Article 8 of the ECHR, English law now recognises a qualified right to respect for private and family life. This general right is supplemented by the data protection framework enshrined in the EU Data Protection Directive and the UK's Data Protection Act 1998.

II. Effective data privacy and data protection rights are essential to life in an Information Society. The vast quantities of personal data generated by digital technologies of all kinds mean that without constant vigilance, and some restraint by the State, personal data privacy will quickly collapse. It is worrying, therefore, that the Government's plans will compel organisations to collect information about their users that they would not have previously had a reason to capture, using technology mandated by and for the purposes of the Home Office.

III. It is essential to recognise that, rightly or wrongly, the Government's proposals are highly intrusive. The Government has emphasised that its proposals involve the retention of, and access to, communications data not content. The implication is that they are only mildly intrusive. However, as the Information Commissioner points out: 'You can tell an awful lot about some people's personal circumstances from the people they are talking to and the websites they visit'.[229] Indeed, it would scarcely be worthwhile from the Government's perspective to introduce this measure if you could not.

IV. The Government has also sought to distinguish its proposals from those of the Communications Data Bill 2008 by emphasising that there are no plans to create a single government database. These earlier proposals were scrapped, in light of widespread condemnation from politicians of all parties, as well as non-politicians.. It is clear that a single, central database captures the public imagination in a way that highlights the privacy and security issues at stake; it is not clear, however, that numerous privately owned databases are less privacy intrusive. Mass surveillance of innocent people is still being proposed.

V. A comprehensive review of the legal, institutional and technical framework within which surveillance powers are exercised in the UK is long overdue and, in this regard, the Protection of Freedoms Act 2012 (POFA) was a missed opportunity. In particular, the Law Society has repeatedly called for an overhaul of the Regulation of Investigatory Powers Act to ensure explicit protection of communications between lawyers and their clients, which is a common position accross the legal profession.

VI. The Society welcomes the Joint Committee's pre-legislative scrutiny of the draft Communications Data Bill and the challenging questions on which it has invited comments and on which the Society offers its views below.

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

[229] Information Commissioner's statement on the Communications Data Bill, 27 April 2009

1.1. The broad objectives of the Bill are clear. That is, to ensure that communications data from internet-based communications (instant messaging, social networks etc) are obtained and retained by CSPs and can then be obtained by authorised public authorities in appropriate circumstances.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

2.1. The Government's case is that communications data have played a role in all major Security Service counter-terrorism operations and most serious organised crime investigations. It now argues that lack of communications data is beginning to hamper investigations.

2.2. The Law Society's view of this argument mirrors that of the European Data Protection Supervisor (EDPS), Peter Hustinx, in relation to the European Data Retention Directive. Hustinx has argued that if a measure is already in place and practical experience has been gained 'there should be sufficient qualitative and quantitative information available which allows an assessment of whether the measure is actually working and whether comparable results could have been achieved without the instrument or with alternative, less-privacy intrusive means. Such information should constitute genuine proof and show the relationship between *use* and *result*.[230]. Hustinx concluded that the quantitative and qualitative information provided by Member States was insufficient to confirm the necessity of data retention as required by the Data Retention Directive. In the Society's view the Government's published evidence-base for additional data retention powers is similarly weak.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

3.1. The proposals in the Bill reinforce and extend an enabling framework in the UK that underpins what many, including the Information Commissioner, have called a surveillance society. The drift into a surveillance society is why the Society argues that POFA was a missed opportunity. The Society does, however, welcome the recognition in POFA of the principle of judicial approval for certain applications to obtain or disclose communications data. The case for extending this principle should form part of any future review of surveillance.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

4.1. The Law Society has not explored this question in any depth. However, the Society notes that Privacy International have claimed that the only other countries in the world that have the kind of mass surveillance systems that are proposed are China, Iran and Kazakhstan[231].

5. **Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?**

5.1. The Society is not aware of any. The Society does think the Home Office should identify alternatives, publish the evidence for and against, and consult both experts and members of the public to ensure that we can have an informed debate.

---

[230] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC). 31 May 2011

[231] Privacy International, *Submission to the Joint Committee on the draft Communications Data Bill*

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

6.1. The relationship between the Data Retention (EC Directive) Regulations 2009 and the proposals in the Bill is not entirely clear. The Regulations apply to communications data to the extent that such data are generated or processed in the UK by a telecommunications operator in the process of supplying a particular communications service. The draft Bill enables the Secretary of State to make an order to ensure that communications data are available to be obtained from telecommunications operators. The implication is that the data to be obtained under the Bill are not data that would be retained by operators in the normal course of their business. However, as the Home Office acknowledges, and the rationale for the Bill, is that the UK's telecommunications infrastructure is changing rapidly. It follows that the boundary between data that will be retained in the course of business and data that will not is also shifting (and not necessarily simply in the direction of less data retention for business purposes) On the face of it, therefore, one overarching piece of legislation would be preferable.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

7.1. Civil liberties should not be traded in this way. If the provisions of the Bill are wrong they should not be adopted; if other measures deserve to be scrapped on human rights grounds they should be.

8. **Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?**

8.1. This is a question for CSPs.

Costs:

9. Is the estimated cost of £1.8bn over 10 years realistic?

9.1. The Society does not take a view on this matter.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?

10.1. No comment.

Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

11.1. No comment.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

12.1. The limited evidence provided by the Home Office explaining the need for this Bill concerns Security Service anti-terrorist operations and serious and organised crime investigations. Limiting access to the Security and Intelligence Services (for their statutory purposes) and to the police for the investigation and detection of serious crime would be appropriate.

12.2. It should not be possible for the Secretary of State to vary the list by Order. Parliamentary debate and approval should be necessary before any extension of access is permitted.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

13.1. It seems entirely unrealistic to pursue overseas providers. The Home Office should explain how its plans will work in practice.

Use of Communications Data:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

14.1. As stated above (Q.12), in the absence of any clearer justification, limiting access to the Security and Intelligence Services (for their statutory purposes) and to the police for the investigation and detection of serious crime would be appropriate

15. Is the proposed 12 month period for the retention of data too long or too short?

15.1. Without a stronger evidence base it is unclear whether or not any retention is necessary and, if it is, whether 12 months is too long or too short. The Home Office should explain the basis on which 12 months has been chosen.

Safeguards:

16. **Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?**

16.1. As the Society explained in its introductory statement, the Society regards these proposals as highly intrusive and does have concerns about compliance with Article 8. Independent judicial review would be better. In cases of urgency such review might need to take place *after* communications data had been accessed. Such cases should be exceptional.

17. **Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?**

17.1. A warrant system would be appropriate. It should apply to all public authorities. Any evaluation of the resource implications should take into account the probable reduction in the number of applications for communications data.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

18.1. Yes, if the Offices which support them are properly resourced. Oversight arrangements can only be effective if they can be implemented in practice and the Information Commissioner has already highlighted the need for additional resources.

August 2012

George Lawrence

Costs / Technical

My understanding is that the Bill seeks to expand the existing interception framework to cover peer-peer communications (like Skype). The suggested cost is around £10 annually per electronically connected person.

The concern is that unlike historical networks based on high transmission costs which require to be centrally switched to conserve transmission resource, modern communication is most cost effective when the network is distributed because transmission is relatively very cheap in comparison to central switching.

The requirements of monitoring re-impose the central ('hub') control element and invalidate a modern communication system's distributed architecture. So while purely monitoring may be costed as suggested, the loss of opportunity cost of being unable to make use of the modern architecture for new communication modes is much higher.

General

It is widely recognised that security agencies need to monitor communications. This has been on a targeted basis – non-communications evidence pointing to individuals under suspicion. The communications of the individuals can then be *selectively* monitored. However what is being proposed is to use a search of data for all communications to find people to watch. It's this blanket proactive trawling, not as a targeted response, that will invalidate the cost-effective technology that people expect. It is also a conceptual shift in approach to an individual's right to privacy.

August 2012

Stacey Leigh Ross

General:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

My understanding is that this Bill is deemed necessary to give the Police the tools to fight terrorism, paedophilia and other nefarious organised crimes.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

Not to my mind. While I understand the need to provide our law enforcers with the tools to do their jobs effectively, I feel this is not the way to do it. The constant mention of terrorists and paedophiles almost seems to be a way to frighten the public into agreement with this Proposal. When I questioned the need for such an invasion of civil liberties with my local MP, this was the standard response.

Frankly, I feel that this is creating a haystack within which to find a needle. Collecting this much information will make mean that much more info will need to be sifted to find the suspects you are after. Surely there is a more effective way.

In addition, the people who this Bill wants to target are media savvy enough to avoid the 'communications net' that anyone might design to catch them. I suspect you will only nab the rank amateurs and careless young people who use inflammatory language that causes a red alert on your security sweep systems.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

I am concerned about the precedent that this sets. A few years ago, RIPA was passed and we gave away some of our freedoms. I feel like this is a slippery slope. If we say yes to this, in a few years time when technology evolves, will we be back again, infringing further and further until we truly have a Big Brother state where everyone is under surveillance.

This proposal makes it seem like everyone is a person of suspicion, and if we're all suspicious individuals then who are we truly being protected from?

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

I don't know, I'm not that versed in this. Perhaps what we need is a think tank comprising "on the ground" officers who actually have to use the system to do their jobs, members of the public from a varied cross section, and technological experts. I believe this might be a better way to design a more effective and less invasive solution.

5-6 No answer

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

Is it even legal for the government to suddenly decide to remove this aspect of my civil liberties. Is this proposed invasion of privacy even legal?

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

I would think they'd find it more attractive, they get money to hold a veritable marketing gold mine that they could use to boost their sales!

Costs:

9. Is the estimated cost of £1.8bn over 10 years realistic?

Is any estimate ever realistic in government? Budgets always end up going over. My concern is more that, here we are being beaten over the head about "the deficit, the deficit, the deficit" and in the midst of cutting

back on real essentials like school repairs, policing, fire services, etc. we're looking to find almost £2bn to hand over to private companies (some of which aren't even UK companies) to collect a truckload of data, most of which we don't even need cause it will be random info like how many times I call my mum, shop on Amazon for baby products and look up a recipe on bbc.

Surely, if we're going to find money for something, it should be to:
- build up our education system,
- support our young people so we have better adults in the future,
- enable our defence forces to do their jobs with the right equipment and
- look after them when they come home (properly!),
- build up our research and development sectors so we're ahead in the energy game,
- pump money in to our small businesses to help rebuild our economy

The list is endless. As far as I'm concerned, collecting mountains of irrelevant data that *will* eventually fall into the wrong hands and used for purposes for which it was not intended, is NOT a priority.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5 - 6bn. Is this figure realistic?

Great! Has anyone worked out the possible costs of this going wrong? Data being lost, sold, used by the wrong people? Prosecution of innocent people? More instances of wasted court time with people like Paul Chambers who "threatened" to blow up a local airport in frustration and had to wait for an appeals judge to figure out it was a joke! Lawsuits from these innocent people who've had their lives turned upside down? All the actual criminals that we will be ignoring until it's too late because we assume our new grand system will catch all, when the very ones we want to catch are slipping through the net?

Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

No. I am especially concerned about conflicts of interest. Will it be deemed in poor taste for wealthy businessman friends of politicians and senior officials to be the ones whose companies are collecting this info and making a tidy sum doing so?

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

We simply should not be collecting this info in this manner so for me, this question is irrelevant.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

Based on our history with the USA bending over backwards to help us the way we do to help them? Highly unrealistic. China and India are also becoming technological super powers, do we really imagine that we would have any control over information that they might decide to keep and hold?

Use of Communications Data:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

This Bill seems to suggest that there are no circumstances. All communications providers will be collecting all your traffic info regardless of whether they have reason to or not just in case you turn out to be suspicious (within the 12 months retention period, of course). I can just picture it now. Cameron, Clegg, or whoever else might end up in power says something that irritates me. In a subsequent phone call to my mum, I get over excited and say "I wish someone would bomb his bicycle" or something equally silly and the next thing I know MI5 is on my doorstep interrupting me hanging out the laundry or feeding my child because I'm a threat to the PM of the hour.

15 No answer

Safeguards:
16-18 While I appreciate that these seem a logical safeguard to put in place, I am sure that you will forgive my lack of faith in most political offices after the last few years of proof that few, if any, positions of power are not abused. I only need to cite the top brass at the Met police, the fall of News of the World et al, the MP's expenses scandal and that's just the top billed ones. Given that history, what guarantee does any ordinary citizen have that with access to so much information that those in power will not succumb to temptation and find profitable uses for what they should be safeguarding. I'd rather not be watching court proceeding 10 years from now with the various Commissioners defending the 'loss' and 'resurfacing' of data that they should never have had to safe guard in the first place. As my mother used to say, why tempt people?

Parliamentary Oversight:
19. No answer

Enforcement:
20-21 A bit too little too late. After the horse has bolted and the information is out there in circulation, all the fines in the world will not stop it from being used. People will always find a way. We won't need to enforce anything if we never collect such a massive amount of personal data that we don't need in the first place.

Technical:
22-26 My only comment here is to ask how you plan to deal with false positives and false negatives, but I maintain that I feel this data should not be collected in such a wide reaching manner therefore eliminating the need for this technical conversation.

In Conclusion:
For decades big businesses have been trying to track customers every move for marketing success (think Tesco Club Card). As someone who used to work in advertising and marketing research I know this information would be a veritable gold mine for any business. I cannot see how any government can ensure that a company does not use the information that they are collecting and storing for their own purposes. I also would like to know how we can be sure that the information has been destroyed after a year has passed.

Furthermore, I reiterate that we have more pressing needs than the funding of heavy-handed plan that creates a mountain to find a mole hill. Why aren't we finding money to support the development of our future? Our young people, our NHS, our business development and career opportunities, our police service, our research and development, our energy dilemmas, our defence forces? Surely these are more important right now.

I honestly do not care whether this is/was a Labour, LibDem or Conservative proposal - my response is the same. I feel there is no realistic or feasible way to truly police this information or ensure its safety and so it would be safer to only collect what is actually needed rather than more than is needed. In practice, this is too costly an excess. The argument that we need this for national security and to be able to ensure convictions in court is valid but this solution is way too extreme. I am sure that there is a hybrid, a middle ground that can be found that doesn't compromise every individual's civil liberties for the sake of a precious few. I truly believe there are enough intelligent and enlightened minds in parliament to come up with a better solution. This is not it.

August 2012

LGA

What access do councils currently have to communications data?

- Councils can access communications data for the purpose of preventing or detecting crime or preventing disorder.
- Councils currently have access under RIPA to telephone / internet subscriber and billing information only. **Councils do not have the powers to obtain the content of any telephone call or email.**
- Councils use communications data to protect residents and businesses from those that are **deliberately and purposefully trying to cause harm**.
- Communications data is **essential** to the work carried out by councils to tackle benefits / council tax fraud, rogue traders, loan sharks, doorstep crime, anti social behaviour, serious environmental crime, commercial flytippers, animal welfare issues and counterfeit goods. **These crimes are often targeted at the most vulnerable in our communities.**
- **Losing access to communications data would leave councils without the tools to protect residents and leave rogue traders to operate more freely in our communities.**

Rights to privacy for individuals

- The LGA recognises that the public are understandably concerned about unnecessary and intrusive use of investigatory powers by Government bodies.
- We support the use of safeguards that can reassure the public that access to data is used responsibly and proportionately.
- While the LGA believes that councils only access data when absolutely necessary and in proportion to the suspected crime, we accepted the introduction of magistrates approval under the Protections of Freedoms Act 2012 for access to data.

Safeguards to accessing data

- The LGA believes that the current framework through which councils can access communications data provides the safeguards that the public are looking for.
- Under RIPA, access to communications data was already subject to internal approval at a Director or Head of Service level and by elected members through regular reviews of requests made under RIPA.
- Councils are also subject to external, independent oversight by the Surveillance Commissioner and Interception Commissioner's offices, which report directly to the Prime Minister each year.
- The Protection of Freedoms Act requires councils to seek magistrate's approval each time councils want to access communications data.

Councils behaving responsibly

- The introduction to the Draft Bill itself states, 'Local authorities account for less than 0.5% of total RIPA requests for communications data'. This extremely low figure shows that councils are exercising their powers in a responsible way and only requesting data when absolutely necessary. In fact, local authority requests only constitute 0.3% of requests for communications data. This figure has remained consistent since 2006 when reporting was introduced.
- Sir Paul Kennedy, in his position as Interception of Communication Commissioner, presented evidence to the Freedoms Bill Committee in 2011, which stated, *'I am aware that some sections of the media continue to be very critical of local authorities and there are allegations that they often use the powers which are conferred upon them under RIPA inappropriately. However,* ***I can categorically state that no evidence has emerged from our inspections that have taken place between 2005 and 2010, which indicates that communications data is being used to investigate offences of a trivial nature, such as dog fouling or littering. On the contrary it is evident that good use is being made of communications data to investigate the types of offences which cause harm to the public, such as investigating rogue traders, loan sharks and fly tipping offences.*** Sir Paul

Kennedy added, *'**Often the telephone number or communications address is the only information / intelligence the local authority has to progress the investigation and identify the alleged offender.'***

Communications data supporting Government priorities

- The Government is running a campaign entitled, 'Targeting benefit thieves' with the tag line, *'It's not if we catch you, it's when'*.
- In April 2012, the Government launched the National Trading Standards Board to provide a structure through which councils would be responsible for *'combating priority areas such as loan sharks and internet scams.'*
- Councils have a crucial role in delivering these strategic Government aims, which can only be achieved with access to communications data to tackle persistent offenders.
- **The LGA provided extensive evidence on the value of council access to communications data during the debate on the Protection of Freedoms Act.** This Act only received Royal Assent on 1st May and we are disappointed that we are required to commit resource to revisiting this debate so soon.
- Clause 11 of the draft Communications Data Bill and the recent Protections of Freedoms Act provide councils with the powers to continue accessing communications data with approval from a magistrate. This shows a clear recognition from Government of the importance of these powers for councils to protect communities from crime.
- However, since the Bill was published, the Home Office has advised that the LGA is expected to make a business case for a specific Order to ensure that councils can retain access to communications data.
- This change in stance, along with differing legal views about whether an Order is actually required, has created significant confusion and concern about Government intentions on this matter. It would be helpful to have a clear message from Government to support the importance of councils retaining access to communications data in order to protect the most vulnerable parts of our communities from crime and to acknowledge that councils are making good use of current powers in a wholly proportionate manner.

Case studies

1. Shropshire Council tackling benefit fraud

A benefit claimant convicted by Shropshire Council received 26 weeks imprisonment for failing to notify of the council of her partner's presence in the household, leading to an overpayment of over £40k in council and DWP benefits. Checks on telephone numbers and SKY requests were critical to establishing the partner was resident at the property.

2. Protecting responsible businesses and creating a fair economy

Wolverhampton City Council acquired communications data to investigate the large scale manufacture and distribution of counterfeit media products via the Internet and computer fairs. The offender was convicted and sentenced to three years imprisonment. The estimated loss to legitimate businesses was in the region of £1 million and this was stopped when the four counterfeiting factories were dismantled.

3. Protecting the public from dangerous goods

Nottinghamshire County Council successfully put a stop to the import and sale of dangerous counterfeit electrical goods, which were putting unassuming consumers at risk. Data about mobile telephone use enabled the Council to obtain details of associates of the main offenders. The case resulted in the main offender getting a 4 1/2 year prison sentence for importing dangerous counterfeit electrical goods. An associate got a 10 month sentence.

Nottinghamshire County Council advises that without the communications data the investigation would certainly have been prolonged (and more expensive) and is unlikely to have succeeded.

4. Protecting vulnerable residents from rogue traders

An elderly couple had been cold called at their property. The couple were advised by Designer Driveways that various works needed to be carried out including power washing the patio; laying a new block paving driveway; a new garden wall; supplying a new gate; removal of conifers from the back garden and laying a patio over the area; treating the joists in the attic for woodworm and laying new insulation. The paperwork provided for the various jobs did not comply with legislation; cancellation rights were not provided and surveyors reports showed that the work had not been carried out properly or that there was no need for the work in the first place. The couple paid Designer Driveways £14,500.

The trader concerned indicated that the company that had carried out the work was nothing to do with him. A subscriber check carried out by Cardiff City Council showed that the mobile phone was registered to him and illustrated clear linkages to the limited company. On the 17th April 2012 the defendant pleaded guilty to fraud charges. He was sentenced to 18 months imprisonment which ran concurrently with a prison sentence that he was already serving.

5. Protecting vulnerable residents from rogue traders

The Central England Trading Standards Regional Scambuster Team based at Solihull Borough Council, and West Midlands Police jointly investigated a rogue builder when complaints were received from two members of the public that they had been ripped off. Initially the Crown Prosecution Service advised against going to trial because there were only two victims and it would therefore be difficult to prove the full extent of his criminality. Outgoing call records were obtained in relation to the suspect's phone and this enabled the investigation team to identify a number of other victims who were prepared to give evidence, many of whom had been unaware that they had actually been the victim to a fraud. The offender obtained approximately £200,000 by fraud from his victims over an 18 month period. The case was eventually tried in Birmingham Crown Court and the offender pleaded guilty and was sentenced to 4 years imprisonment. It is extremely unlikely that he would have been brought to justice if the investigating officers had not made effective use of the powers to acquire communications data.

6. Preventing outbreaks of food poisoning

The case concerned the supply of chicken to several food businesses in the Cardiff area. The business was not registered as a food business and it was not known whether the meat was illegal sourced and unsafe. None of the invoices given specified a company name, address or contact telephone number. However, one of the food business owners confirmed that he ordered the chicken from a mobile telephone number.

A subscriber on this number gave a residential address from which the defendant was subsequently traced. On the 21st July 2011 defendant pleaded guilty to offences under the General Food Regulations 2004 and fined. This could not have been traced without access to communications data.

The economic impact of an outbreak of food poisoning would have been significant and, potentially, fatal to elderly and vulnerable people.

7. Policing online sales

Hampshire CC were called to investigate importer of counterfeit golf clubs and accessories who sold them via eBay. Despite two seizures from HMRC at port of entry, he continued. Records from eBay and Paypal were contradictory in terms of identification of location of offender. A series of email addresses provided to eBay/Paypal were checked by means of requesting subscriber details and the offender located as a result.

Despite pleading guilty at first opportunity (and therefore getting a mandatory 30% discount on the penalty), the offender was sentenced to 30 months imprisonment (reduced on appeal to 21 months) and was ordered to pay a confiscation order in the regions of £108,000. This demonstrates the seriousness of the crime.

8. Maintaining road safety

A large scale purchaser and seller of was found to be selling 'clocked' cars. Cars were bought at auction with high mileages and then sold via eBay/Auto Trader website with fraudulent descriptions applied. The cars concerned were low value ones, typically no more than £2000. Over 50 cars were sold in a misdescribed manner and with falsified service history. The value of the fraud was in excess of £60,000. False names and addresses were used, however, it was possible to trace those concerned using subscriber details in respect of mobile telephone numbers and email addresses provided. Despite pleading guilty at first available opportunity (and therefore getting a mandatory 30% discount on the penalty), the offender was sentenced to 20 months imprisonment.

9. Working with the Police to stop email scams

The Council received notification of residents receiving Chinese inheritance scam letters. The letters promised release of an inheritance from a person in China on payment of an administration fee. Letters were posted with Royal Mail Smart Stamp details on them and to potential victims already on 'sucker lists' who are therefore potentially very vulnerable to such activity. The Council obtained subscriber details from Royal Mail indicating the persons and addresses within the United Kingdom who had received letters, making the fraud much easier to tackle.

The investigation was referred to the Metropolitan Police as it involved work on a scale beyond the council boundaries. However, council involvement enabled a rapid response and enabled the police to target their resources at dealing with the offenders. The council was also able to provide advice to residents on avoiding the scam.

10. Tackling benefit fraud

Neath Port Talbot CBC successfully prosecuted a man for illegally claiming £5000 of housing benefits using communications data. Official telecoms information was used to show that the numbers listed in his planning application form and mortgage application were false and deliberately misleading. The evidence from the telecommunications companies was used to prove intent to commit benefit fraud and that the individual had provided false information for financial gain. He was given a 12 month community punishment order for 240 hours of unpaid work and told to repay the overpayment of benefit and court costs.

July 2012

Liberty

Executive Summary

The Draft Communications Data Bill relates to the proposed collection, retention and availability of "communications data" across the UK. It is no exaggeration to say that these legislative proposals signal a major shift in the relationship between the communications industry, the state and the public. Never before have private companies been called upon to orchestrate blanket collection of personal data which they have no business reason to retain. This briefing will interrogate the capacity which could be created under these proposals, the depth of the civil liberties implications and the limitations of the proposed system in law enforcement terms.

Communications data is highly revealing. In an average day we can expect to generate a large amount of communications data, including from activity on social networking sites such as Facebook and LinkedIn, the details of communications via Twitter, the history of websites visited, the time at which telephone calls were made, who they were made to and how long the call lasted, the location of an individual making or receiving a mobile phone call as well as the duration and timing of the phone call and subscriber information relating to the source or recipient of communications and their direct debit details.

Such data is increasingly difficult to distinguish from "content" and we understand that in order to facilitate the collection of data under this Bill, telecommunication providers will be required to install technology that has the capacity to routinely intercept all communications. This not only exacerbates human rights concerns but also makes clear that this proposal is about extending rather than maintaining the ability of the State to monitor communications.

In the UK arrangements currently exist for the retention of some communications data. This is as a result of an EU Directive that was transposed into UK law in 2009. However, similar rules in place in other EU countries have been recently subject to successful legal challenge. Indeed constitutional courts across the continent – including in Germany, Romania and Bulgaria – have ruled that their respective arrangements for retaining some communications data are unconstitutional. A significant case is currently pending before the European Court of Justice which, for the first time, will directly interrogate the compatibility of the EU Directive with human rights obligations. We are unsure why the Government has not waited for the outcome of this judgment before pressing ahead with more intrusive plans.
Liberty believes that current UK data retention arrangements are a disproportionate interference with the right to respect for private life and undermine respect for freedom of expression. The proposals set out in the Draft Bill go significantly further and suffer even greater flaws as a result.

Liberty has never opposed targeted surveillance with prior authorisation, on the basis of individual suspicion, but this Draft Bill amounts to nothing less than blanket surveillance of the population at large, turning a nation of citizens into a nation of suspects.

Introduction

1. The Draft Communications Data Bill ('the Draft Bill') was announced in the Queen's Speech and published by the Home Office on 14th June 2012. It is currently undergoing a period of pre-legislative scrutiny by the Draft Communications Data Bill Committee ('the Committee'). Liberty appreciates the opportunity presented by pre-legislative scrutiny of the Draft Bill, but given the privacy implications these proposals carry for all UK residents we are disappointed that there has been no prior public consultation undertaken by the responsible department. In particular, we understand that there has been no formal process of consultation with communication service providers. On this basis we find it very difficult to understand how the Home Office has reached its conclusions about the extent of potential collaboration, nor indeed the costs implications of its proposals.

2. Before embarking on a substantial analysis of these proposals we must further express concern at their broad and vague nature. Our attempts to critique this Draft Bill have been hampered by a serious lack of detail. The best way to describe its provisions is 'future-proof': highly enabling and lacking in focused prescription.

The detail of the Draft Bill

Part 1 - Data Collection

3. Clause 1 of the Draft Bill grants the Secretary of State the power, by order, to impose any requirement or restriction on an operator which is aimed at ensuring the availability of communications data to specified bodies. Arrangements around access to data are dealt with in Part 2, but Clause 1(b) makes clear that operators may be required to retain or otherwise handle data in order to facilitate access outside the arrangements provided for in Part 2 of the Draft Bill. The non-exhaustive list of requirements which may be imposed on operators include obtaining or processing data and entering arrangements with third parties in order to facilitate the availability of data.[232] The processing of data includes the reading, organisation, analysis, copying, correction, adaptation or retrieval of data and its integration with other data.[233] Requirements may be placed directly on an operator by order or provision may be made in an order to allow for restrictions or requirements to be imposed by notice.[234]

4. Subclause 1(3) provides that operators may be made subject to additional regulatory obligations designed to facilitate swift access to data and make provision about standards, equipment, systems and techniques.[235] Requirements may be placed on operators in relation to services provided by another operator. Communications data for the purposes of the permissive regime set up by clause 1 carries substantially the same meaning as provided for under RIPA; the regime applies to postal operators.[236] Subclause 1(4) states that an authorisation may not permit conduct consisting of the interception of communications; as explored below this prohibition is difficult to square with our knowledge of the technological limitations of DPI software and hardware.

5. Under the heading 'safeguards' clause 2 places the Secretary of State under an obligation to consult with OFCOM, the Technical Advisory Board and operators or persons representing operators or with statutory functions in relation to operators.[237] The Technical Advisory Board is solely concerned with the technical or financial viability and not the privacy impact of proposals.

6. Clause 4 provides that data must be retained for 12 months from the date of the communication unless a shorter period is provided for in a specific notice or the operator is informed that the data is or may be required for legal proceedings, in which case operators will be required to retain data until informed otherwise. If it becomes apparent that communications data is not required for legal proceedings, the public authority which has requested the information should inform the operator of that fact.

7. Clause 5 makes clear that operators cannot disclose data except in accordance with Part 2 of the Draft Bill dealing with access and authorisation, or *'otherwise as authorised by law'*, this could include a disclosure required by court order as suggested by the explanatory memorandum, but would clearly cover

---

[232] Clause 1(2).

[233] Clause 1(5).

[234] Clause 1(2)(b).

[235] Clause 1(3).

[236] Clauses 28 and 25.

[237] Clause 2.

other situations in which the Secretary of State authorises access otherwise than in accordance with Part 2 under subclause 1(b). The operator is required to put in place security provision to protect against unlawful disclosure which can include management checks and controls; no further detail is provided about the requirement of 'adequate security systems'.[238]

8. Clause 6 provides for the destruction of data at the end of the retention period. Destruction can take place at monthly intervals, meaning data can be retained for up to an additional month pending the next round of data destruction.

9. Clause 7 sets out 'other safeguards'. All listed safeguards set out in this section of the Bill relate to process and specifically the form of requests. A notice made pursuant to an order requiring retention of data must be in writing, specify the recipient and be given in a manner 'appropriate' to bring it to the intention of the recipient. [239] The recipient of the notice must be allowed to refer the notice to the Technical Advisory Board, in accordance with timescales specified in the order – the board will consider technical and financial concerns raised by operators, reporting back to the operator and the Secretary of State. The Secretary of State will have the option to withdraw the order after receiving a report from the Board: this is the second safeguard. If the Secretary of State chooses to confirm her order no further referrals are possible.

10. Clause 8 deals with enforcement. Requirements dealing with the way data should be held, the duration of retention, access and destruction or any other requirement or restriction imposed by order are enforceable by the Secretary of State through civil proceedings.[240] Where work is incidental to or *'reasonably undertaken in connection with'* conduct that is authorised under this Part of the Bill and it is not conduct for which an authorisation or warrant could and should have been sought independently, it is not to lead to civil liability.[241]

Part 2 - Accessing data

11. Clause 9 makes legislative provision, via a process of internal authorisation, for access to all forms of communications data by any police force, the Serious Organised Crime Agency, HMRC, the intelligence services and any other public authority designated in a Secretary of State order.[242] Before data can be accessed by an employee the authorisation of a designated senior officer of the authority concerned must be sought. If granted the employee who made the request becomes an authorised officer for the purposes of the request. The designated senior officer may only grant authorisations where he or she believes that it is:

(i) necessary to acquire the data for a permitted purpose; (ii) necessary to obtain the data: (a) for the purposes of a specific investigation or operation; or (b) *'for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data'*; and (iii) the conduct authorised is necessary and proportionate to the aim.[243]

12. This provision mirrors RIPA and the permitted purposes set out at subclause 9(6) remain as broad and ill-defined. An additional purpose is added at subclause 6(c) which relates to the prevention and

[238] Clause 5(2).

[239] Clause 7(1).

[240] Clause 8(3).

[241] Clause 8(4).

[242] Clause 21.

[243] Clause 9(1).

detection of any conduct in respect of which civil enforcement action for market abuse may be taken by the Financial Services Authority.[244] These permitted purposes can be added to or restricted by the Secretary of State by order.[245]

13. The designated senior officer may grant authorisation for himself or any other employee within his public authority and the authorisation can extend to any conduct in relation to a communications system or data derived from such a system in order to obtain communications data.[246] Clause 9(3) contains a non-exhaustive list of the type of conduct which can be authorised including requiring any person whom the authorised officer believes holds communications data to disclose it to a person identified in the authorisation. Clause 9(4) states that an authorisation may grant access to communications data to a person who is not authorised in the order for any conduct which has, as its aim, the enabling or facilitating of obtaining communications data. Subclause 9(5)(b) provides that authorisations made under sub-clause 9(3) may not involve the disclosure of data to those outside of the public authority in question.

14. Clause 10 makes provision for the form in which authorisations or notices made pursuant to authorisations are to be made – in particular the nature of requirements should be specified. Notices must specify the office or position of the person giving it, the requirements imposed and the operator upon whom the requirements are imposed.

15. Clause 11 sets out a regime of judicial approval for local authority access to communications data which mirrors the provisions of sections 23A and B of RIPA.[247] Where an application is made for a Magistrate's order approving an authorisation, the individual who is the subject of the authorisation need not be informed; the same is true of his legal representatives. A Magistrate may approve the authorisation where satisfied that, at the time of the grant and at the time the application comes before the Court, the requirements set out at subclause 9(1), which deal with internal authorisation, are satisfied.

16. Local authorities can still only seek access to use and subscriber data.[248] Aside from local authorities and those public authorities listed on the face of the Draft Bill, provision around the range of public authorities to which access will be granted, the types of data to which access is authorised and authorisation processes are left to secondary legislation: no draft order has yet been forthcoming.[249]

17. Clause 12 provides for authorisations to be operational for renewable periods of a month. If the grounds for the original authorisation no longer exist, a designated senior officer must cancel the authorisation. Clause 13 places operators under a duty (enforceable by civil proceedings brought by the Secretary of State) to *'obtain or disclose the communications data in a way that minimises the amount of data that needs to be processed for the purpose concerned'*.[250] Clause 13 also reaffirms an operator's duty to act in accordance with the requirements of a notice given in accordance with an authorisation, however they are not required to do anything in pursuance of that duty which it is not reasonably practicable to expect them to do.

---

[244] The Draft Bill provides for the repeal of other corresponding powers and is therefore effectively a consolidation of existing provision in one piece of legislation.

[245] Clause 9(7).

[246] Clause 9(2).

[247] Uncommenced provisions inserted by section 37 of the *Protection of Freedoms Act* 2012.

[248] See clause 17.

[249] We understand that the Secretary of State has asked those public authorities seeking to retain access to communications data to set out the 'business case' for ongoing access.

[250] Clause 13(1).

18. Clause 14 provides for filtering arrangements to be put in place by Government. The clause is incredibly broadly framed and its scope obscure. The Secretary of State is empowered to put in place any 'arrangements' she sees fit, for the purposes of 'assisting' operators to determine whether retention could be secured in accordance with the provisions of clause 9, or to 'facilitate' efficient and effective access to data. In particular the Secretary of State can obtain data on behalf of an authorised officer and obtain the *'data from which the data may be derived'*.[251] It is also clear that the Secretary of State can retain data for the purpose of processing that data, allowing for temporary executive retention, processing and distribution of data brought together from many different sources.[252] The Government maintains that clause 14 is designed to create an automated system which will ensure that only that information relevant and required by a particular authorisation is retained, but the extent to which this central filter will be automated is not clear. Clause 16 which sets out duties in connection with the operation of the filter provides that aside from disclosure to designated senior officers, disclosure is permitted for the purposes of support, maintenance, oversight, operation or administration of the filtering arrangements. What is clear is that the filter amounts to a temporary centralised store of potentially large amounts of communications data operated and maintained by the executive, giving the Government a very significant role at the centre of the data retention and disclosure regime.

19. Through the filter, the Secretary of State will seek to make public authorities aware of the extent of communications data available and process data with disclosure based on an assessment of what is needed by the requesting authority. The central filter will bring together atomised pieces of data to create a revealing whole. Further, according to Professor Peter Sommer, a leading technical expert in the field, the filter is likely to use 'content' and 'communications data' in order to correctly identify patterns of communication.[253]

20. Clause 15 makes clear that the proposed central filter may be used both for the purposes of obtaining and disclosing communications data. Subclause 15(2) refers to the temporary retention of data and subclause 16(1)(c) provides for the destruction of data obtained and processed through the filter *'when the purposes of the authorisation have been met'*: no upper time limit for retention of data in the central filter is provided. An authorisation made by a designated senior officer must record the officer's decision as to whether data is to be obtained and disclosed through this centralised process and the description of data that may be processed in accordance with a particular authorisation. Clause 16 restates the purposes for which communications data retained in the central store can be disclosed. There is a requirement to put in place a security system to govern access, no details are given about the form or extent of security required. Retrospective annual reports on the operation of the filtering database are to be supplied by the Secretary of State to the Interception of Communications Commissioner as soon as possible after the end of each calendar year.[254] *'Significant processing errors'* must be reported to the Commissioner.[255]

21. Clause 17 provides that local authorities may not access traffic data or any extra data 'generated' by operators in response to a request by a relevant public authority. The Secretary of State may place restrictions on the granting of authorisations by designated senior officers including in relation to data

---

[251] Clause 14(2)(b).

[252] Clause 14(2). In the accompanying explanatory notes the Government notes that data generated by current forms of online communication will require greater aggregation and processing – for example they envisage cases in which fragmented communications data from a number of different sources will be co-ordinated through the filter to provide a fuller picture.

[253] Submission of Professor Peter Sommer to the Joint Committee on the Draft Communications Bill, para 44.

[254] Clause 16(6).

[255] Clause 16(7).

stored by Government as part of 'filtering arrangements'.[256] The Secretary of State may delegate any of her functions in relation to filtering arrangements to a designated public authority.

Part 3 - Scrutiny of retention of and access to communications data

22. Part 3 replicates provisions of RIPA providing for the retrospective oversight of data retention and disclosure by the Interception of Communications Commissioner.[257] Operators must keep sufficient records of actions taken in accordance with the provisions of the Bill to allow for review by the Commissioner.[258]

23. Clause 23 provides for the jurisdiction of the Investigatory Powers Tribunal to be extended to cover new powers granted under Parts 1 and 2.

Part 3 – general provisions

24. Clause 25 extends the reach of Parts 1 and 2 to cover postal operators in the same way as they apply to telecommunications operators. Clause 26 obliges the Secretary of State to make payments towards the costs incurred or likely to be incurred by telecommunications and postal operators. Payment may be made subject to conditions. It is for the Secretary of State to determine the scope and extent of arrangements for payments, including specifying which payments should be made to particular operators.[259] Clause 27 incorporates Schedule 3 which provides for amendments to RIPA to extend Codes of Practice to cover the provisions of this Draft Bill. Schedule 3 also provides for amendments to RIPA allowing for regular revision of codes of practice. The Secretary of State is required to consider representations made around draft codes and may modify a draft. Both codes and revisions to codes must be laid before Parliament and are subject to the affirmative resolution procedure.

Background

25. The *Regulation of Investigatory Powers Act 2000* (RIPA) governs the use of targeted surveillance in the UK. Before RIPA came into force, our statute book contained a number of targeted surveillance powers developed in an ad hoc way over the years. RIPA was designed to consolidate the law and to incorporate human rights principles of necessity and proportionality. At its inception, RIPA was designed to deal with access to communications data and access is currently governed by Chapter I, Part II of RIPA and the *Regulation of Investigatory Powers (Communications Data) Order* 2010. Section 22(4) of RIPA provides the current definition of communications data which has three components:

(i) Traffic data: this tells you, amongst other things, where the mobile phone, internet connection etc was located at the time a communication took place – e.g. where a mobile phone was when it received or made a call as well as data going to the identity of the source and recipient of the communication;

(ii) Service use: this tells you how a communication occurred (i.e. was it via email, a text or a phone call etc), the date and time it occurred and how long it lasted;

(iii) Subscriber information: this tells you any information held by the person who has signed up to the communications service, for example the name and address and any direct debit details of the user.

---

[256] Clause 17(4).

[257] Save where oversight is reserved to the Information Commissioner or the judiciary (under clause 22(1), this is a Magistrate for England and Wales).

[258] Clause 22(6).

[259] Clause 26(5).

Access

26. RIPA provides, on the face of the Act, for all forms of communications data to be available to the intelligence services, the police, the Serious Organised Crime Agency (SOCA), HMRC and other specified public authorities provided for by order; these include the Financial Services Authority, the Gambling Commission and the National Health Service Trust.[260] The power to acquire service use data and subscriber information is available to over 430 local authorities and a significant number of other public authorities, including the Food Standards Agency, the Charity Commission and the Environment Agency.[261] The permitted purposes for which communications data may be accessed are broad and ill-defined, including in the interests of the economic well-being of the UK and to assess or collect any tax, duty or other type of government charge.[262] The Act provides for a regime of internal authorisation for access to communications data for a large number of public bodies. Section 37 of the *Protection of Freedoms Act* 2012 amended RIPA to require prior judicial authorisation for access to communications data by local authorities[263] however this section is not yet and even once in force, will only affect a small fraction of communications data requests.

Availability

27. While communications service providers (BT, Virgin etc) typically retain some information about their customers' past use of communications for their own business purposes (e.g. itemised phone bills) they were not – until relatively recently - obliged to retain any such data about their customers.

28. A small shift in this area took place in 2001 when the *Anti-Terrorism Crime and Security Act* was rushed through Parliament following the tragic events of 9/11. Amid a host of draconian anti-terror powers stood Part 11, providing for the creation of voluntary agreements between service providers and the Government for the extended retention of communications data The internet initially objected to these voluntary agreements, with the Secretary General of the Internet Providers Association informing then Home Secretary, Rt Hon David Blunkett, that the industry was not convinced that extending the length of time companies hold on to customer logs was necessary for the fight against terrorism and organised crime.[264] In July that year the Information Commissioner publically warned the Home Office that plans for a voluntary code of practice for the retention of communications data could violate human rights protections because logs supposedly retained for the purposes of serious criminal investigations could be accessed for such purposes as the levying of taxes.[265] The Foundation for Information Policy Research also

---

[260] For the full list see the *Regulation of Investigatory Powers (Communications Data) Order* 2010, Schedule 2, Part 1.

[261] For the full list see the *Regulation of Investigatory Powers (Communications Data) Order* 2010, Schedule 2, Part 2.

[262] See section 22 of RIPA. Communications data can also be accessed in an emergency to prevent death or to prevent or mitigate injury or any damage to a person's mental or physical health. For the types of surveillance local authorities have access to, the Secretary of State can make orders extending the purpose for which authorisations can be made. To date orders have been made to allow communications data to be accessed to investigate alleged miscarriages of justice and to assist in identifying deceased persons or persons unable to identify themselves because of a physical or mental condition. See *Regulation of Investigatory Powers (Communications Data) Order 2010*, SI 480/2010.

[263] Section 37 of the Protection of Freedoms Act has not yet been brought into force.

[264] The Guardian, *Internet providers say no to Blunkett*, 22 Ocober 2002, available at: http://www.theregister.co.uk/2002/10/22/uk_isps_oppose_data_retention/.

[265] The Guardian, *Internet providers say no to Blunkett*, 22 Ocober 2002, available at: http://www.theregister.co.uk/2002/10/22/uk_isps_oppose_data_retention/.

came out in opposition, warning of the dangers of a policy rejected by *'civil society, Europe's data protection commissioners and now internet service providers'*.[266]

29. Notwithstanding widespread concerns about the impact of a proposed voluntary code, in 2003 the Home Office, secured a series of agreements with service providers. To date we do not know the details of these agreements nor do we have confirmation of the parties involved. These initial agreements related to information already kept for commercial purposes, establishing a minimum period for retention.

30. In 2002 the Home Office attempted another policy to extend access to communications data to a wide range of public authorities – authorities with no law enforcement remit whatsoever, including parish councils. In the face of huge opposition, these plans were scaled back, however the RIPA regime still grants access to a huge range of public authorities on the basis of a process of internal authorisation.

31. Still dissatisfied with capabilities in this area, in 2005 the Home Office used the UK presidency of the EU to push through compulsory arrangements for communications data retention which resulted in the EU Data Retention Directive 2006.[267] The Directive provides for the mandatory retention of communications data (already retained for billing or commercial purposes) for between 6 and 24 months. Sweden postponed the implementation of the Directive facing huge fines, whilst across EU member states cases were brought challenging the domestic legislation transposing the Directive.[268]

32. Back in the UK and before the transposing legislation had even come into force, the Home Office 'Interception Modernisation Programme' (IMP) was already in train. The Government declared an intention to bring forward legislation, a 'Communications Data Bill' in 2008-2009.[269] Initial proposals were premised on the construction of a centralised database, but these plans were hastily dropped in favour of a series of industry controlled mini-databases. Opposition to the explosion in state surveillance facilitated by the last Government was pronounced, with Liberal Democrat Leader Nick Clegg observing of the last Labour Government, in February 2008, that *'it is this Government that has turned the British public into the most spied upon on the planet.'*[270]

33. In April 2009 the UK fully transposed the Directive by way of the Data Retention (EC Directive) Regulations 2009 ('the regulations'), which provide for requirements to be placed on service providers to retain communications data kept ordinarily for commercial purposes for a minimum of 12 months. We still do not know which UK based communications companies are required to retain our data; requests for disclosure are met with the familiar refrain that information cannot be revealed for reasons of national security.[271] Two months later in June 2009, the Home Office launched its consultation *'Protecting the Public in a Changing Communications Environment'*.[272] Having rejected plans for a centralised database, the resulting proposals strongly resemble those which now form the Draft Communications Data Bill. Then

[266] The Guardian, *Internet providers say no to Blunkett*, 22 Ocober 2002, available at: http://www.theregister.co.uk/2002/10/22/uk_isps_oppose_data_retention/.

[267] Directive 2006/24/EC of the European Parliament.

[268] Explored further at paragraphs 64-68 below.

[269] See House of Commons Briefing note, *'Internet Surveillance'*, pg 2. Available at: www.parliament.uk/briefing-papers/SN06304.pdf.

[270] Hansard, 6 Feb 2008 : Column 951.

[271] The Data Retention (EC Directive) Regulations require the Secretary of State to give notice to those telecommunication providers he or she wishes to retain data. In 2009 a Freedom of Information Request was submitted to the Home Office requesting information regarding the identity of those service providers which had received notices under regulation 10 of the Regulations. This request was refused by the Home Office and the related correspondence is available at: http://www.whatdotheyknow.com/request/notices_under_regulation_10_of_s

[272] http://www.official-documents.gov.uk/document/cm75/7586/7586.pdf. Read Liberty's Response here: http://www.liberty-human-rights.org.uk/pdfs/policy09/liberty-s-communications-data-consultation-response.pdf.

Home Office Minister Lord West stated that *'the objective of the IMP is to maintain the UK's lawful intercept and communications data capabilities in a changing communications environment.'*[273] In its response to the consultation, the UK's largest communications service provider, BT, pointed out that:

'[t]he proposals would outsource data collection, processing and retention to CSPs rather than building a central Government database and could result in significant brand, reputation and customer relationship issues for CSPs… retaining data on the scale proposed would raise significant issues of proportionality, especially in view of the fact that only a fraction of the data might be used. Moreover, finding the pieces of information that might prove to be useful to the relevant authorities amongst the mountain of data that will be available to them will be no easy task – the proverbial "needle in a haystack"'.[274]

In June 2009, the same month that the consultation was launched the Leader of the Conservative Party, David Cameron, argued that *'[t]oday we are in danger of living in a control state. Every month over 1,000 surveillance operations are carried out. The tentacles of the state can even rifle through your bins for juicy information.'*[275]

34. Liberty was amongst the many groups and individuals, including service providers and other industry bodies who expressed concerns at these proposals and in light of widespread opposition, Labour shelved the project in November 2009.
Notwithstanding the Coalition's commitment, in July 2010 the first signs of a u-turn emerged as the Home Office, in a 'Draft Structural Reform Plan', stated that it would *'publish proposals for the storage of internet and email records, including introducing legislation if necessary.'*[276] By October 2010, the Government's plans had apparently solidified into an attempt to revive the discredited IMP, with the Strategic Defence and Security Review outlining – amongst a wide range of other proposals - plans to *'introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to obtain communication data and to intercept communications within the appropriate legal framework.'*[277]

Key changes proposed to the current regime

35. The Draft Bill would change current arrangements for the retention of communications data in three significant ways:

(i) First, under the Draft Bill, unprecedented requirements may be placed on UK based operators to collect and process communications data generated by web-based services such as Gmail and Facebook, provided by overseas operators, which cross their domestic networks.[278] It is widely suggested that the only way to

---

[273] Hansard, 8 July 2008 : Column WA76.

[274] See BT Response to 2009 Home Office Consultation: Protecting the Public in a Changing Communications Environment available at http://www.btplc.com/thegroup/regulatoryandpublicaffairs/ukpublicaffairs/responsestopolicyconsultations/commsdata-btresponse200709.pdf, paragraph 5.

[275] Speech by Rt Hon David Cameron, *Giving Power Back to the People*, 25th June 2009, available at: http://www.conservatives.com/News/Speeches/2009/06/David_Cameron_Giving_power_back_to_the_people.aspx

[276] Home Office Draft Structural Reform Plan (July, 2010) available at: http://www.homeoffice.gov.uk/publications/about-us/corporate-publications/structural-reform-plan/pdf-version?view=Binary.

[277] Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, October 2010, available at: http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf?CID=PDF&PLA=furl&CRE=sdsr, page 44.

[278] Clause 1(3)(c)(ii).

obtain such information, in the absence of voluntary agreements with third party providers, is through Deep Packet Inspection (DPI) technology. According to one leading expert, whilst DPI can operate as software, when traffic levels are high specialised hardware must be installed which captures a data stream as it crosses an operator's network.[279]

(ii) Second, the definition of those bodies required to retain data is significantly wider covering all 'telecommunications operators' ('operators') as opposed to the 'public communications providers' referred to in the retention regulations. An operator is 'a person who controls or provides a telecommunications system, or provides a telecommunications service'.[280] This includes all telecommunications companies BT, Orange, TalkTalk, Vodafone and others, but would also extend to manufacturers of communications equipment who could be called upon to adapt their products with the aim of facilitating access to communications data, and to private networks for example blackberry messenger or internal 'intranet' operators in private companies or other organisations. Requirements could also be placed on anyone who owns a mobile phone or other telecommunications equipment including a private individual.

(iii) Third, the Bill makes provision for central filtering arrangements to be operated by the Home Office. The central filter will bring together atomised pieces of data to create a revealing whole which can be disclosed to public bodies in response to specific requests. Whilst not a comprehensive central database in itself, this is a co-ordinated Government operated facility through which many requests for data will be processed. The privately operated databases will be joined up to create an integrated system. This regime raises many of the same concerns as a large and centralised store and no details are given about security arrangements, or the clearly envisaged human involvement in what the Government describes as an 'automated system'. Further the filtering arrangements provided for in the Bill throw into sharp focus the depth and breadth of the information which can be gleaned through a comprehensive system of data retention combined with substantial and sophisticated processing arrangements. The Government has laboured the distinction between content and communications data; its case is that the privacy implications of the later are small by comparison. Yet the central filter will provide for vast swaths of data, retained by disparate companies, to be scanned for relevant information, connected up and shaped into a coherent and acutely revealing whole – data can be matched up to reveal a huge amount about an individual's life in order to work out whether a request made by a designated senior officer is necessary and proportionate. The Bill anticipates the kind of advanced processing, shaping and linking of data provided for in the filtering arrangements to take place as a precursor to establishing the necessity of access. This carries huge potential for in-depth processing of the data of innocent individuals – individuals who will likely never know that their data has been handled in this way and are consequently deprived of any opportunity to mount a challenge.

36. The Draft Bill contains substantially the same provisions for access as provided for under RIPA as amended by section 37 of the *Protection of Freedoms Act* 2012. Aside from the four enforcement agencies provided for on the face of the Draft Bill which mirror provision in RIPA, details about the public authorities, including local authorities which will be permitted to access data will be provided in secondary legislation expected to reflect the provisions of the *Regulation of Investigatory Powers (Communications Data) Order* 2010. As at present, local authorities will not have access to traffic data and access to traffic data by other public authorities (outside of those listed in the Bill) will be governed by Secretary of State order. Scrutiny arrangements provided for under the Bill substantially mirror those provided for in RIPA.[281]

The civil liberties implications of blanket data collection

---

[279] Submission of Professor Peter Sommer to the Joint Committee on the Draft Communications Bill, para 41.

[280] Clause 28.

[281] See, Chapter 2 of Part 1 of RIPA, in particular section 57.

37. The civil liberties concerns around this Draft Bill relate to all three of its component parts: data collection, access and scrutiny – additional concerns around the processing of data in a central filter which span collection and access also carry significant privacy implications.

38. Much attention has been given to the proposed access arrangements provided for in the Draft Bill which largely mirror those already in existence. Liberty agrees that pressing concerns exist in this area and these concerns intensify as the pool of data retained increases. However we believe that the more fundamental danger of this Draft Bill is the provision it makes for a shift from limited data retention to blanket data collection.

39. The Government's attempted justification for requiring the blanket collection and retention of communications data is based on four highly questionable assumptions which we will examine in turn, first that communications data is not particularly revealing, second that communications data can always be practically and conceptually distinguished from content, third that blanket retention of communications data will lead seamlessly to gains in law enforcement and finally that requiring blanket collection of this information will do no more than "maintain capability".

Revealing nature of communications data

40. The Government argues that communications data is less revealing than data generated by, for example, interception or bugging, and that this justifies a considerable divergence in approach to that taken with other targeted surveillance powers. This assumption is highly questionable. Communications data can build up an incredibly intimate picture of our lives. With the proliferation of mobile forms of communication, in addition to tracing the timing, duration, recipient and source of a communication, specific details about an individual's location can also be collected. When combined with substantial subscriber information, the revealing nature of communications data is hard to dispute. Compile and co-ordinate this information for every call, text, email, tweet, blog and Facebook posting and you have a map of our daily routines, our relationships, our habits and preferences, the streets we walk, where we work and socialise, the extent and nature of our communications with others. Furthermore, consider the range of situations in which just the fact of a single communication and the identity of the parties speaks volumes: the phone call from a senior civil servant to a Times reporter immediately before a major whistleblower scandal fills the front pages, the email to a civil liberties watchdog from a police officer during the course of an inquest into a death in police custody. The record of a website visited, which falls firmly within the definition of communications data, can also be incredibly revealing. Consider, for example, the case of a teenager viewing an abortion website, a celebrity accessing the website of an HIV service provider. We must not underestimate the intrusion that the retention of communications data, without more, represents.

41. In April this year, in response to the disclosure of further details of the Government's plans to extend the collection of communications, Sir Tim Berners-Lee, inventor of the world wide web, came out in opposition to the proposals. In an interview with the Guardian he stressed that the planned extension of the state's surveillance powers would make a huge amount of highly intimate information vulnerable to theft or release by corrupt officials, adding that:

"The amount of control you have over somebody if you can monitor internet activity is amazing. You get to know every detail, you get to know, in a way, more intimate details about their life than any person that they talk to because often people will confide in the internet as they find their way through medical websites … or as an adolescent finds their way through a website about homosexuality, wondering what they are and whether they should talk to people about it."[282]

---

[282] The Guardian, *Tim Berners-Lee urges Government to stop the snooping bill*, Tuesday 17 April 2012. Available at: http://www.guardian.co.uk/technology/2012/apr/17/tim-berners-lee-monitoring-internet.

42. The Internet Service Providers Association has also joined the building opposition to these proposals pointing to its concerns *'about the new powers to require network operators to capture and retain third party communications data… includ*[ing] *the scope, proportionality, privacy and data protection implications and the technical feasibility.'*[283] According to a report in the Independent, after being informally briefed by Government earlier this year, the Association expressed concern that *'network operators are going to be asked to put probes in the network and they are upset about the idea... it's expensive, it's intrusive to your customers, it's difficult to see it's going to work and it's going to be a nightmare to run legally.'*[284]

Blurring of record and content of communications

43. At one time a firm distinction between communications data and content would have been more credible, for example when much communication was by letter: everything inside the envelope is content, everything on the outside communications data. To say that things are no longer so simple is a significant understatement. The proliferation of innovative new forms of online communication and the resultant fragmentation and diversification has created a complex and multifaceted communications landscape. In support of its argument that technology is making the RIPA definitions of communications and interception more and more difficult to sustain, the LSE, in a study examining remarkably similar proposals put forward by the last Government, observed:

> *Historically there have been two entirely separate regimes for authorising access to [communications data] and for intercepting content. We strongly doubt that this framework can be maintained in the new ICT environment of web-based email, social networking, online gaming and cloud computing.*[285]

We do not pretend to be technical experts. We do however understand that there are increasing practical difficulties within new technologies in distinguishing communications data from content and perhaps more disturbingly in recording communications data without capturing content.

44. Communications services are now provided by a host of companies based all over the world. Web-based services such as webmail and social networking sites dominate the communications landscape. The domestic companies who provide our internet access, for example BT, TalkTalk or Virgin, are no longer the companies which provide the most widely used email services such Gmail and Hotmail or social network sites like Facebook or Twitter. Details of these communications are not routinely retained by those that bill us because we are charged periodically for access, rather than for each use of a service. Despite Home Office claims that this Draft Bill is about working collaboratively with operators, including those based overseas, we have no clear picture of the extent to which, for example, webmail providers like Google collect or retain communications data generated by service users, never mind their willingness to hand this information over. The Home Office acknowledge that where voluntary agreements are not forthcoming, other arrangements will be put in place to ensure data collection and retention. Our understanding is that as traditional communications service providers like BT become increasingly a mere vehicle for accessing other web-based services the centrality of Deep Packet Inspection (DPI) technology to the system as a whole becomes inescapable.

45. DPI is the generic name for the equipment that would be required for the collection and analysis of third-party data. The LSE's study into the last Government's Interception Modernisation Programme

---

[283] Draft Communications Data Bill – ISPA's initial statement, June 14 2012. Available at: http://www.ispa.org.uk/draft-communications-data-bill-ispas-initial-statement/.

[284] Report made on the basis of a report in the Sunday Times. See the Independent, *Police and MI5 get power to watch you on the web*, Monday 2 April 2012. Available at: http://www.independent.co.uk/news/uk/home-news/police-and-mi5-get-power-to-watch-you-on-the-web-7606788.html.

[285] LSE Briefing on the Interception Modernisation Programme, page 3.

maintains that every use of DPI is in fact an interception, even if its purpose is to gain access to communications data.[286] DPI 'black boxes' capture the entire data stream, computer programmes or 'scripts' are then written in order to extract the description of data required.[287] By requiring UK based operators to install DPI black boxes on their lines to capture every data stream which crosses their networks, this Draft Bill provides for the creation of the physical infrastructure for the interception and retention of all of our communications. If we accept that effective programmes or 'scripts' can be written which discard the content and collect the communications data, we cannot avoid the fact that, with a reformulation of these programmes, the nature of the data retained could be dramatically altered. What is more, the LSE also describes how black boxes which contain DPI software can be programmed and re-programmed remotely.[288] Ultimately there is nothing to stop another administration from bringing forward legislation which makes fuller use of the new capability which will be created by the proliferation of DPI black boxes.

46. Liberty believes that a number of obvious unanswered questions arise around the use of this technology, for example who will exercise effective control over DPI boxes? Who will write the programs or 'scripts' which dictate those aspects of the data that are to be retained and those parts which will be discarded? What are the technological and cost implications of ensuring that software installed and programs written keep pace with the technological advancement including new forms of internet based communication? Will organised criminals be able to evade detection by using encryption or anonymisation techniques, hijacking the poorly secured internet connections of others or changing the IP address of a computer moment by moment? Further some technology experts have warned that modern communications are so complicated that it may be impossible to separate out the basic contact data from the content in terms of the data retained.[289]

Law enforcement gains?

47. Our ability to comment on potential law enforcement gains of blanket collection is restricted by the unanswered questions which remain around the role of communications data in law enforcement and other areas. We still do not have a full picture, across all those public bodies able to access communications data, of the types of investigation for which data is accessed, the extent of access and the number of individuals affected. We are told that, over the past decade, communications data played a role in 95% of all serious criminal investigations, but we have no idea about the extent of this role. Was communications data central to the operation or a peripheral detail? How many of these investigations led to successful prosecutions? Could the prosecution have been secured without access to this data? Further in how many low level, non-serious and even non-criminal investigations is communications data used? A recent freedom of information request involving Humberside police revealed that a residual category for communications data access requests is 'other non-crime'.[290]

48. The Government's argument assumes that further collection of communications data will lead seamlessly to better law enforcement, however the collection and storage of yet more personal information also brings risks. In recent years the government has lost 25 million child benefit records as well as the

---

[286] Ibid, pg 22.

[287] Ibid, pg 37.

[288] Ibid, pg 26.

[289] See Daily Telegraph article: *'Snooping' laws will stop paedophile rings, says Theresa May'*, 14 June 2012, available at: http://www.telegraph.co.uk/news/uknews/law-and-order/9330945/Snooping-laws-will-stop-paedophile-rings-says-Theresa-May.html.

[290] See evidence to the Draft Communications Data Bill Committee on Wednesday 11th July: *"Humberside police confirmed that they have used this nearly 200 times in three years for traffic offences, and terrorism is not listed as one of the crimes, they even beautifully list the category 'other non-crime'."* Nick Pickles, Big Brother Watch.

personal information of those serving in the armed forces, witnesses in criminal cases and prisoners. Further communications data collection and retention necessarily means that the data will pass through more hands and potentially be more susceptible to bureaucratic error and even fraud. Communications data can be just as interesting and revealing as intercepted content and in the aftermath of the phone-hacking scandal we should be particularly wary of create new targets for abuse and misuse.

49. In other countries reports of unlawful interception should serve to caution us against the creation of the infrastructure for the interception of all our communications. In Greece in recent years the unlawful use of interception capability was widely reported. The scandal reportedly involved wiretapping of Eriksson software used by Vodafone which had the capability to intercept communications data albeit that was not the primary purpose for which it was used. We understand that the hackers operated in such a way that it wasn't clear the intercept capabilities in the software were being used and their activities reportedly went undetected from August 2004 until January 2005; they were finally shut down in March 2005.[291]

50. Similarly in Italy a multifaceted wiretapping scandal reportedly involving Telecom Italia ranged from 1996 until it was finally uncovered in 2006. A fresh and apparently unrelated wiretapping scandal in which Telecom Italia was also implicated emerged in 2007. Both scandals were reportedly huge, complex and have still not been fully uncovered; it has been variously alleged that they involved intelligence services and were bound up in state surveillance and security, terrorism and rendition, as well as corporate infighting. The original, long running scandal involved the exploitation of a flaw in Telecom Italia's security systems, which allowed a person to set up wiretaps without leaving any trace. The phones of politicians and other high-profile politicians were reportedly tapped using existing infrastructure.[292]

51. According to the LSE multiple vulnerabilities in the infrastructure for the retention of communications data have reportedly been uncovered in the US that *'would allow adversaries to take them over and perform unlawful interception'*.[293] Securing the configuration of devices to protect against unwarranted intercept will be a matter of the utmost importance, but to date we have little information about the arrangements to be put in place to protect against security breaches. The scope of these proposals throws the potential implications of a breach into sharp focus.

52. The Interception of Communications Commissioner's latest report provides further cause for concern. During 2011 public authorities as a whole submitted 494,078 requests for communications data, 52% of these requests were for subscriber data, 25% for traffic data and 6% for service use data – 17% of requests were for a combination of different sorts of data.[294] During 2011, 895 communications data errors were reported, with approximately 80% of those attributable to public authorities and 20% to

---

[291] The scandal was report in the Wall Street Journal on 21 June 2006: *"In early March 2005, George Koronias, Vodafone Group PLC's top executive here, contacted the Greek prime minister's office about an urgent security matter. Vodafone's network in Greece had been infiltrated by phone-tapping software targeting an elite group of cellphones: those assigned to many of the country's leaders, including senior police and defense officials, cabinet members and the prime minister himself."* For more see: http://online.wsj.com/article_email/SB115085571895085969-lMyQjAxMDE2NTIwMTgyNTE1Wj.html.

[292] For reports of the scandal see: http://news.bbc.co.uk/1/hi/business/5367754.stm; http://www.reuters.com/article/2010/01/05/us-italy-spy-idUSTRE60435E20100105; http://www.infoworld.com/t/business/telecom-italia-embroiled-in-new-espionage-scandal-999; http://www.theregister.co.uk/2008/04/14/telecom_italia_spying_probe_update/.

[293] See Ibid, pg 26: *'Studies of interception equipment conforming to the US communications surveillance standards (under 'CALEA') were in the past found to contain multiple vulnerabilities that would allow adversaries to take them over and perform unlawful interception.'*

[294] Interception of Communications Commissioners Annual Report to the Prime Minister 2011, Chapter 7, pg 28-29.

Communications Services Providers.[295] This included 99 identified by the Commissioner's Office from the small sample of cases reviewed. [296] In a report a good deal fuller and more detailed than in previous years, the Commissioner also referenced two cases in which individuals were arrested, wrongly detained and accused of crimes on the basis of data errors,[297] further communications data had been illegitimately used by a local authority to determine whether a family lived in the right school catchment area.[298] 0.4% of annual requests for communications data are made by local authorities.[299]

53. Despite reiterated warnings about the diminishing capabilities of the State as regards communications data little mention is made of current loopholes in capability or the extent to which they would be left unchanged by the proposals. Our understanding is that there has and will always be methods of communication that do not come within the State's reach and these are just as likely to be methods of relatively little sophistication as well as those of greater sophistication. One example is the use of unregistered pay-as-you-go mobile phones. In reviewing the future communications landscape it is reasonable to suggest that truly sophisticated criminal networks will continue to make use of readily available anonymised methods of communication.

Extending rather than maintaining capability

54. In evidence before the Committee, in addition to in the explanatory notes and impact assessments accompanying the Draft Bill, the Home Office reiterates its claim that projected technological changes will decrease the State's capability as regards the use of communications data. While it is difficult to argue with the substance of the technological changes projected, the description given is notable for what is missing. Technological innovation has, and will continue to, reap huge gains for law enforcement in the UK but the Government makes no attempt to present the current proposals in historical context. By this we do not suggest that a protracted discussion of telephony or other technological innovations is required – rather some reference to how the ability to access records of communications between individuals is, in itself, a recent boon for law enforcement would give a much fuller picture of where we currently stand. Not too long ago, before the wide availability of mobile phones and email, most communications between individuals, if not carried out through traditional telephony or letter writing, would have been conducted face to face. This would have presented different - potentially more challenging - obstacles to law enforcement. Just because in recent times the State has benefitted from access to communications data that was already recorded and retained by communications providers does not mean that total access to all communications data should be required, for all time, regardless of cost and implications. Further, it does not follow that just because communications data can be recorded and historic records made available that they should. For good reason other - supposedly more intrusive - surveillance techniques available under RIPA such as bugging (whether in private or in public), the use of human covert surveillance or the interception of communications need *prior* authorisation on the basis of individual suspicion. Once authorised they can only be carried out in the future. The Government is not presently arguing that we should all be routinely or randomly subject to bugging, covert tracking or interception 'just in case' but, if the present proposal is allowed to pass, proposals for other types of blanket or random surveillance irrespective of suspicion "just in case" are a logical next step.

Impact on freedom of expression and assembly

---

[295] Ibid, pg 30.

[296] Interception of Communications Commissioner Report 2011, pg 30 and 32: http://www.intelligencecommissioners.com/docs/0496.pdf.

[297] Ibid, pg 31.

[298] Ibid, pg 43.

[299] Ibid, pg 39.

55. In addition to the very obvious privacy implications, it is important to remember that proposals of this nature engage other fundamental human rights, most notably the right to freedom of expression as protected by Article 10 of the ECHR and freedom of assembly as protected by Article 11. We need only look at the role of social media in organising the protests that have precipitated the spread of democracy across the Middle East, to realise that freedoms central to the promotion and preservation of democracy, freedom of expression and freedom of assembly in particular, are engaged by measures providing for the blanket collection of information about the web habits of the population at large. Freedom House's 2011 Freedom on the Net Report, observes that:

In Egypt and Tunisia, for example, democracy advocates have relied heavily on Facebook to mobilize supporters and organize mass rallies. Similarly, Bahraini activists have used Twitter and YouTube to inform the outside world about the government's violent response to their protests. Even in Cuba, one of the most closed societies in the world, several bloggers have been able to report on daily life and human rights violations.[300]

56. In Saudi Arabia, a country where freedom of expression is strictly circumscribed, online activists have been able to expose corruption and hypocrisy amongst the ruling royal family.[301] Similarly internet users in Thailand have played a significant role in challenging the ruling elites since the Thai military coup of 2006.[302] In Russia and Venezuala with restrictions on broadcast media outlets growing, the internet has been seized upon by those seeking to demonstrate their dissatisfaction with the regime and mobilize opposition.[303] The potential created by the internet for empowering ordinary citizens and giving a voice to the voiceless is arguably one of the most inspiring developments of recent history.

57. In our developed democracy too, the internet has had a huge role to play in the flourishing of democratic participation. Democracy requires free and fair elections, but it does not stop there. The internet has given ordinary people a forum to contribute to debates of national significance, organise peaceful protest on a large scale and put real and immediate pressure on our political representatives. Grass-roots activism aside, the internet has also given the whole population the ability to communicate in innovative new ways with loved ones no matter where in the world they are, it has allowed people to nurture friendships, develop contacts, share ideas and reach out to everyone or anyone about the issues that matter to them. Never before has the right to speak your mind been so real as in the internet age.

58. Repressive regimes throughout the world have felt justifiably threatened by the empowering impact of the web. Techniques employed to stifle online freedom include blocking huge areas of content and filtering access to every area of the web within a jurisdiction.[304] Widespread monitoring is also a technique used by some regimes to limit the capacity of the internet to effect social change. Freedom House reports that:

The Iranian authorities have taken a range of measures to monitor online communications, and a number of protesters who were put on trial after the election were indicted for their activities on Facebook and Balatarin, a Persian site that allows users to share links and news.[305]

---

[300] Freedom House, *Freedom on the Net Report 2011*, pg 3. Available at: http://www.freedomhouse.org/sites/default/files/FOTN2011.pdf.

[301] Ibid, pg 289-291.

[302] Ibid, pg 9.

[303] Ibid, pg 9-10.

[304] Ibid, with China, Cuba and Iran amongst the worst culprits see pg 23, 24 and 26 in particular.

[305] Ibid, pg 26.

59. One way many oppressive regimes have opted to control the internet is by requiring communications services providers to further a repressive agenda. After social networking sites facilitated pivotal protests in Egypt, the authorities directed internet service providers to remove pathways for computer users to connect to requested websites,[306] whilst in Iran tactics include ordering the removal of posts deemed offensive from the sites of blogging service providers.[307] Zimbabwe's 2007 Interception of Communications Act allows the authorities to monitor telephone and internet traffic, and requires service providers to intercept communications on the state's behalf. It is very difficult to accurately assess the scope of internet controls employed by secretive authoritarian regimes, but what is clear is that monitoring web-activities in various ways is a vehicle for curtailing the flow of ideas which may ultimately lead to social change.

60. If the scheme envisaged in the Draft Bill is brought into force, we will distinguish ourselves amongst European countries as the leaders in online surveillance and earn a place on a spectrum including some of the most oppressive regimes in the world. Liberty believes that the knowledge that details of web habits are collected on mass with the possibility of future access ever present, will create a real shift in online behaviour. There are many different ways to curtail freedom of expression online, mass collection of information whether carried out by the state or simply orchestrated by Government and operated by the private sector is one of those.

61. As well as an attack of the place of free expression in our wider social fabric, the spectre of online surveillance will have very real and specific impacts, for example on journalists, whistleblowers and trade unionists. The protection offered by Article 10 covers journalistic sources – one of the ethical cornerstones of reporting. The centrality of journalistic sources to a free media was fully endorsed in a case involving the *Financial Times* in 2001. Attempts to force the newspaper to disclose its sources were ultimately defeated in recognition of the real potential chilling effect on press freedom.[308] In another stark example of the role of data collection in stifling freedom of expression and freedom of assembly, Liberty recently took up the cause of thousands of workers whose details were stored on a secret database discovered three years ago. Full details of the information collected are still emerging, but amongst the data stored was information indicating a history of trade unionism.[309] An official from the Office of the Information Commissioner reportedly told a Tribunal that some of the information could only have been supplied by police or the security services.[310] A significant number of major firms allegedly used the information in making recruitment decisions. Data collection on the scale proposed can only add to the risk that scandals of this type will be repeated.

Unlawfulness of blanket communications data collection/retention

62. Proposals to collect and retain records of all electronic and postal communications necessarily engage the right to respect for private and family life protected by Article 8 of the European Convention on Human Rights as protected by our *Human Rights Act* 1998 (the HRA). As with most HRA rights, the right to private life can be limited where the limitation can be shown to be necessary and proportionate to satisfy the legitimate aim of preventing and detecting crime as well as other social interests. Whilst

---

[306] Ibid, pg 7.

[307] Ibid, pg 26.

[308] *Financial Times Ltd and Others v United Kingdom (Application no. 821/03).*

[309] See Liberty's blog, *Blacklisting scandal continues,* 8 August 2012. Available at: http://www.liberty-human-rights.org.uk/news/2012/blacklisting-scandal-continues.php.

[310] The Independent: *Thousands of workers 'blacklisted' over political views*, Tuesday 7th August. Available at: http://www.independent.co.uk/news/uk/home-news/thousands-of-workers-blacklisted-over-political-views-8010208.html.

communications data is undoubtedly useful in crime detection it does not follow that collecting and retaining all communications data between all individuals is proportionate. Still less that processing communications data *'just in case'* would satisfy requirements of necessity and proportionality which are central to the protection of personal privacy in this country. The law enforcement implications are at best unclear, the security risks great and the intrusiveness of communications data incontrovertible.

63. As a result of the Data Retention Directive, the current regime across Europe allows for the retention of certain communications data by communications service providers for a fixed period. The draft Communications Data Bill would extend the law beyond the Directive. As such, cases on the Directive are highly instructive: If the Directive is disproportionate under human rights laws, then the Communications Data Bill must be too.

64. Constitutional courts across the Continent have declared that the present EU regime for retention of records violates basic rights and freedoms. In October 2008, the Romanian Constitution Court became the first to declare legislation transposing the EU Directive in breach of its Constitution. The Court found that the mandatory retention of communications data scheme engaged a number of fundamental rights, namely the right to freedom of movement, the right to intimate, family and private life, privacy of correspondence and the right to freedom of expression. In finding its transposing legislation disproportionate, the Court relied on, amongst other issues, the reversal of the ordinary presumption of innocence and the lack of a reasoned basis for the retention period required, finding also that retention on the scale required was *'likely to prejudice, to inhibit the free usage of the right to communication or expression'*.[311] Two months later the Bulgarian Supreme Administrative Court followed suit, finding its own enabling legislation incompatible with the country's constitutional protection of personal privacy.[312]

65. In March 2010, Germany's Constitutional Court declared the provisions of its law transposing the Directive unconstitutional. In finding the communications data retention regime incompatible with constitutional protection for personal privacy, the Court commented that *'the protection of communication does not include only the content but also the secrecy of the circumstances of the communication, including if, when and how many times did some person…contact another.'*[313] The Court went on to find that *'the evaluation of this data makes it possible to make conclusions about hidden depths of a person's private life and gives under certain circumstances a picture of detailed personality and movement profiles; therefore it can not be in general concluded that the use of this data presents a less extensive intrusion than the control of the content of communications.'*[314]

66. The Cypriot Constitutional Court in February 2011 ruled orders issued under its transposing law unconstitutional[315] and in March the same year the Czech Constitutional Court annulled transposing

---

[311] Decision no 1258 of the Romanian Constitutional Court, 8 October 2009. Available at: http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html. See also European Commission, *Report from the Commission to the Council and the European Parliament*, Brussels, 18.4.2011, COM(2011)225 final, para 4.9.

[312] See EDRI report, *Bulgarian Court Annuls A Vague Article Of the Data Retention Law,* 17 December 2008. Available at: http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention. See also European Commission, *Report from the Commission to the Council and the European Parliament*, Brussels, 18.4.2011, COM(2011)225 final, para 4.9.

[313] Bundersverfassungsgericht, 1 BvR 256/08. English press release at http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html (judgment only in German), for translated extracts from the judgement see European Area of Freedom Security & Justice, On the BVG ruling on Data Retention: "So lange" – here it goes again, available at: http://afsj.wordpress.com/2010/03/05/so-lange-here-it-goes-again/. See also European Commission, *Report from the Commission to the Council and the European Parliament*, Brussels, 18.4.2011, COM(2011)225 final, para 4.9.

[314] Ibid.

[315] European Commission, *Report from the Commission to the Council and the European Parliament*, Brussels, 18.4.2011, COM(2011)225 final, para 4.9.

legislation, expressing doubt as to whether such widespread retention of data was necessary or even effective.[316] A case is pending before the Hungarian Constitutional court which involves a challenge to transposing legislation surrounding the depth of data processing.[317]

67. 2012 has seen more questions raised around the legitimacy of the EU regime, with a leaked European Commission paper setting out doubts as to the legality and utility of the Directive. [318] In this document, the Commission acknowledges the lack of support for the Directive's crime-tackling aspirations and points to the vagaries of the scheme. The legality of the Directive is now set to be challenged directly under Article 8 of the European Convention on Human Rights as well as parallel provision in the EU Charter, in the case of *Digital Rights Ireland* referred to the European Court of Justice (ECJ) by the High Court in Ireland.[319] In this preliminary reference, the High Court specifically ask whether the Directive is compatible with Article 7 of the EU Charter/Article 8 ECHR (rights to privacy); Article 8 Charter (protection of personal data); and Art 11 Charter/Article 10 ECHR (freedom of expression). The *Digital Rights Ireland* case will be hugely significant for the future of the present data retention framework as well as for the Draft Bill under consideration. It is startling therefore that the UK Government is not willing to wait for the decision in this important case before pressing ahead with even more intrusive rules. Assuming the ECJ clearly answers all the questions posed by the High Court, the implications of the case will be highly important. If the Court takes the same line adopted by so many national constitutional courts, then the Directive may be annulled on grounds of proportionality and breach of human rights. Such a decision could pave the way for a successful legal challenge to the lawfulness of the present regime in the UK courts and would seriously undermine government arguments about the need and legitimacy of going further under the draft Communications Data Bill.

68. Liberty believes that the present framework for communications data retention is in breach of Article 8 and that the proposals contained in this Draft Bill – which necessarily go much further - would put the UK further in breach. An analogy can be made with the retention of DNA. It is uncontroversial to say that DNA profiles can be incredibly useful in detecting and preventing crime. That is not to say that a universal DNA database would be desirable. Indeed the creation of a universal DNA database would be a disproportionate means of achieving the legitimate aim of crime detection and prevention. This was confirmed in the judgment in *S and Marper v UK* in December 2008 and reflected in the revising provisions of the *Protection of Freedoms Act* 2012.[320] There now appears to be a general acceptance of the fact that the last government's policy of indefinite, blanket retention of the DNA of all those arrested was unlawful and unacceptably detrimental to personal privacy.

Review of RIPA

69. While the original intention of RIPA was to bring the UK better in line with universally recognised human rights standards, the legislation which resulted and developments since mean that its review and revision is long overdue. Liberty has long called for an overhaul of the RIPA framework so that safeguards can be incorporated that better protect those in the UK from unnecessary and heavy handed surveillance.

Access arrangements

---

[316] European Commission, *Report from the Commission to the Council and the European Parliament*, Brussels, 18.4.2011, COM(2011)225 final, para 4.9.

[317] European Commission, *Report from the Commission to the Council and the European Parliament*, Brussels, 18.4.2011, COM(2011)225 final, para 4.9.

[318] The leaked report is available at: http://quintessenz.org/doqs/000100011699/2011_12_15,Eu_Commission_data_retention_reform.pdf.

[319] *Digital Rights Ireland* [2010] IEHC 221.

[320] See Part 1 of the *Protection of Freedoms Act* 2012.

70. Liberty supports the amendment to RIPA contained in the *Protection of Freedom Act* 2012 which requires prior judicial authorisation in some areas of communications data access. This reform is replicated in the Draft Bill. Whilst the inclusion of warranty requirements for local authority access is welcome, it does not address concerns about the additional capacity authorised by this Bill and the swathes of additional, revealing data which will be retained. Further the impact of limited provision for judicial authorisation should not be overstated, given that local authorities account for only 0.4% of requests for access to communications data.[321] The latest Report of the Interception of Communications Commissioner reveals that, during 2011 only 141 of 400 local authorities able to access communication notified the Commissioner that they had made use of their powers.[322] 79% of these local authorities made less than 20 requests, 58% less than 10.[323] Given the relatively small numbers involved, and the limited nature of a local authority law enforcement capacity, Liberty questions the need for any local authority access to communications data.

71. The purposes for which data can be accessed by local authorities or other relevant public authorities remain unnecessarily broad and ill-defined. No definition is given as to what is, for example, 'in the interests of national security' or the 'economic well-being of the UK'. We do know, however, that the last government took an alarmingly expansive view of what may be justified in the name of the 'economic well-being of the UK' arguing on one occasion that restricting drug-users access to welfare benefits is justified to further that aim.[324] In evidence to the Committee, Charles Farr, the Director of the Office for Security and Counter-Terrorism at the Home Office, refused to rule out access to communications data for the purpose of identifying those caught speaking on the telephone whilst driving.[325] Human rights standards require that in the exercise of surveillance there must be adequate safeguards to protect the citizen against excessive intrusion or other abuses of rights. The use of broad and vague notions such as 'national security' and 'economic well-being' give rise to a real risk that the disproportionate use of surveillance will be authorised, going beyond what is necessary to protect the public from harm. This could interfere unacceptably with political and other lawful activity that ought to go unimpeded in a democratic society. We believe that these grounds should be better defined, particularly as the prevention or detection of crime, or serious crime, is already included which should capture the majority, if not all, of the grounds on which surveillance needs to be authorised. The ability of the Secretary of State to expand the list by order also contrasts with the prescriptive nature of Article 8. This raises serious concerns over the compatibility of RIPA powers with the right to respect for personal privacy.

72. Liberty has ongoing concerns about the process of self-authorisation which currently applies across the board and remains in place for all those public authorities listed on the face of the Bill and, subject to provision to the contrary in secondary legislation, all other public authorities (save for local authorities) to whom access is granted. Under the Draft Bill other public authorities included in the access regime will continue to operate a system of internal authorisation. Senior police officers and Home Office officials claim that the designated senior officer authorising access to communications data will not be somebody involved in the particular operation or investigation for which the information is sought. It should be noted, however, that the Draft Bill makes explicit provision for a designated officer to authorise his own access to communications data and places no restrictions on his ability to authorise access by reference to the extent of his involvement in the investigation concerned.[326] The Code of Practice which currently governs access to communications data specifically deals with this issue and whilst maintaining that *'designated persons*

---

[321] Ibid, pg 39.

[322] Ibid, pg 38.

[323] Ibid pg 39.

[324] See the Explanatory Notes to the Welfare Reform Bill at paragraph 418, available at: http://www.publications.parliament.uk/pa/cm200809/cmbills/008/en/2009008en.pdf.

[325] See Evidence to the Committee on Tuesday 10th July.

[326] Clause 9(2).

should not be responsible for granting authorisations or giving notices in relation to investigations or operations in which they are directly involved', this assertion is substantially undermined by the caveat *'although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently or for security reasons'*.[327]

73. Liberty maintains that even if a designated officer is not directly involved in an investigation it is entirely unacceptable for public authorities to be able to self-authorise access to revealing personal data, particularly when the access regime is so broadly framed. Considerations of necessity and proportionality should be assessed by a member of the judiciary who will be both independent and adept at conducting the Article 8 balancing exercise. We do not seek to impugn the integrity senior employees of our law enforcement agencies, but rather point out the reality that their primary concern will relate to the operational capacity of their agency. This is a matter of organisation culture and is perfectly understandable, but it is also a reality which mitigates in favour of independent third party authorisation.

74. In the cases of those organisations which do not routinely access communications data, our concerns are greater still. A public official within a public authority that may not exercise such powers on a regular basis is hardly well placed to determine when conduct will or will not unnecessarily or disproportionately interfere with a person's privacy. We are further concerned about the lack of certainty around access provisions for public authority access which are left to secondary legislation.

Scrutiny

75. Under the draft Bill retrospective oversight of the new system of data retention will continue to be provided by the Interception of Communications Commissioner, the Commissioner will continue to be appointed by the Prime Minister with his annual reports made to the Prime Minister.[328] Notwithstanding the efforts of the present or future Commissioners, a system of limited retrospective authorisation comes nowhere close to providing effective scrutiny of a system which carries such huge consequences for personal privacy, particularly when we have so little detail about the resources and in particular the technical expertise available to the Commissioner.

76. It is not an offence under RIPA to unlawfully access communications data and whilst an offence may be made out under section 55 of the *Data Protection Act* 1998, the only available sanction is a fine.[329] While Liberty does not usually support the creation of new criminal offences given the excessive amounts of criminal law that already exists, unlawful access to communications data should be an offence under RIPA, with appropriate penalties. Whilst most people will never know whether or not their data has been improperly retained or accessed, for those who do find out, the main consequence for a public authority of accessing data without the appropriate authorisation, for example, is the possibility of civil action being taken against them under the HRA. However, the majority of actions taken under the HRA in respect of the use of RIPA powers must be taken before the Investigatory Powers Tribunal (IPT). The procedure operated by the IPT is far from adequate. It is under no duty to hold oral hearings before which a person may be represented and even if it does decide to hold a hearing (purely at its discretion) all of the Tribunal's

---

[327] Home Office Code of Practice for the Acquisition and Disclosure of Communications Data, paragraph 3.11.

[328] RIPA, ss 57 and 58.

[329] Offence of knowingly or recklessly, without the consent of the data controller (a) obtaining or disclosing personal data or the information contained in personal data, or (b) procuring the disclosure to another person of the information contained in personal data. Section 60 provides that successful prosecutions will result in a fine.

proceedings, including the oral hearings, must be conducted in private.[330] RIPA itself provides that, subject to any rules made by the IPT, the IPT can only notify the complainant whether they have won or lost.[331] Rules made in 2000 provide that if the IPT finds in the complainant's favour the IPT must provide him or her with a summary of their determination, including findings of fact. Note, however, that this is merely a summary of the determination and if a complainant loses no reasons at all will be given. Most astoundingly, there is no right of appeal from the IPT. Section 67(8) of RIPA provides that rulings by the IPT are not subject to appeal and cannot be questioned in any court, unless the Secretary of State orders otherwise. Section 67(9) provides that it is the duty of the Secretary of State to make such orders in relation to most categories of proceedings and complaints, yet no such orders have yet been made. This is because despite most of section 67 being brought into force in October 2000, subsection 67(9) has never been brought into force. This effectively means that in most cases in which a person seeks to argue that a public authority has used unlawful surveillance against them, they are required to bring proceedings before the IPT, which must hold proceedings in secret, may not hold an oral hearing, will not give proper reasons for its findings and from which there is no right of appeal. This is arguably a breach of Article 6 of the HRA itself which requires a fair and public hearing, and the right under Article 13 of the ECHR to an effective remedy. These provisions should be overhauled as a matter of urgency in order to provide an appropriate mechanism for the independent determination of any complaints regarding the lawfulness a disclosure. How can the public have any confidence in a process which is held in secret, gives little or no reasons for its decisions and whose judgment cannot be brought into question in any court of law?

Conclusion

77. The Government claims these proposals will do nothing more than 'maintain capability': in reality the Coalition is proposing much more. For the first time private companies will be instructed to collect information on billions of communications made by their customers for no other reason than the authorities' future demands for access. This amounts to mass, blanket, monitoring of the population paid for and facilitated by Government but outsourced to the private sector. This would represent a fundamental shift in the nature of our society turning a nation of citizens into a nation of suspects.

August 2012

[330] See Rule 9 of the *Investigatory Powers Tribunals Rules 2000,* SI 2665/2000.

[331] RIPA, s 68(4).

LINX

Executive Summary

1. Having had detailed involvement in the development of communications data policy since before RIPA was passed, and with a membership that provides crucial operational support for law enforcement needs in this area, LINX has no doubt of the value of communications data for legitimate law enforcement purposes.

2. Equally, we are fully aware of the impact of the use of communications data on the privacy of the citizen. As the development of the information society results in the creation of ever larger and richer data sets, and as analysis tools become increasingly sophisticated, the use of communications data can become increasingly intrusive.

3. We do not think it our place to suggest an appropriate balance between the citizen's interest in privacy and the interests of public authorities. We do, however, consider ourselves well placed to give independent expert advice on the nature of the data sought, and the nature of the technical capabilities that could be authorised by the powers contained in the draft Bill. We are also well placed to comment on the potential technical impact for telecommunications operators if they have to change their network design priorities to accommodate data gathering requirement or equipment.

4. The draft Bill contemplates the collection of a large amount of personal communications data. Both the volume and range of data to be collected are unprecedented in the UK, and probably in the world.

5. The collection and processing of "*third party*" communications data by network operators is a substantial extension of their duties that is, in our opinion, materially distinct from existing data retention requirements, amounting to a complete novelty.

6. In our analysis the "filtering arrangements" provided for in clauses 14-16 are best understood as a "*profiling engine*" which creates detailed profiles on all users of electronic communications systems and makes those profiles available for sophisticated data mining.

7. In our opinion this *profiling engine* amounts to an enormously powerful tool for public authorities. Its mere existence significantly implicates privacy rights, and its extensive use would represent a dramatic shift in the balance between personal privacy and the capabilities of the State to investigate and analyse the citizen.

8. In our opinion, whether – and to what extent – such a shift is justified is a matter for Parliament. We do not express an opinion.

9. We do believe that Parliament should take responsibility for making the basic value judgement as to the appropriate balance between personal privacy and the public interests of the State.

10. In its testimony to this committee the government placed great reliance on the general Human Rights Act requirement that public officials only use communications data in a manner that is proportionate; the draft Bill is itself quite empty of restrictions. We do not believe this lone prescription can bear the weight the government is placing on it without providing those officials more detailed rules and guidance in how it is to be applied. Development of and confidence in, such rules and guidance is inhibited by the government's reticence about discussing how communications data might be used.

11. While we recognise that certain details must inevitably remain hidden to protect the efficacy of investigation methods, the government's response to this problem has been to present a draft Bill which is so broadly written as to amount to a general authorisation of empowerment. In our view Parliament is being invited to abdicate its responsibility to set the basic standards by which we live. It would confer on the Executive an effectively unfettered and wholly inappropriate discretion to determine the appropriate level and circumstances for intrusion into personal privacy by means of analysis of communications data.

12. In our view any new legislation concerning covert investigation of communications data should contain on its face

    a. Sufficient detail concerning the nature of the data to be collected for Parliament to make a meaningful and informed value-judgement as to the fundamental balance between privacy and investigative capabilities, and to be able to legislate to ensure that this balance is applied;
    b. A coherent framework for establishing when it is proportionate to access private information, and what use is made of it, that makes draws relevant distinctions according to the level of intrusion implied by different uses and different kinds of communications data;
    c. Transparent, democratically accountable mechanisms for approving detailed rules on use of data, within the basic framework
    d. Credible oversight mechanisms to prevent and discover mis-use
    e. Effective and dissuasive sanctions for misuse, both by individuals and organisations
    f. A realistic opportunity for remedy for those who have had their privacy infringed without justification

13. We do not believe any of these expectations are adequately addressed in the draft Bill.

14. We believe that our members, who are commercial entities, share with citizens a legitimate expectation that such important regulation of their business environment and duties should be subject to full democratic scrutiny and approval.

15. While we strongly welcome the government's commitment to pay telecommunications operators the financial costs they incur in carrying out their obligations under the draft Bill, we do not believe this empties our members of a legitimate interest in this legislation.

    a. The challenges implied by the need for technical development, business and systems re-engineering and operational maintenance of the systems contemplated by the draft Bill are enormous, and we anticipate incalculable and hence irrecoverable opportunity costs as effort and skill is diverted from commercial ends to satisfying new legal duties.

b. Moreover, the draft Bill significantly implicates the intangible relationship of trust between a communications operator and its customer.

16. We have significant doubts about the technical feasibility of much of what is contemplated, but the government has been too reticent about sharing its actual expectations as to how far it would take the powers granted under the Bill for us to comment in detail.

17. In particular, we question the technical feasibility of constructing the "*profiling engine*", which represents an enormously complex systems integration challenge.

18. We have serious concerns about the challenges involved in protecting the systems established under the draft Bill and the data they generate. This is especially true in respect of the "*profiling engine*", which appears especially challenging to protect. If the security of the "*profiling engine*" were ever compromised we believe it would constitute a significant threat to national security.

About LINX

19. LINX, the London Internet Exchange, is a membership association for network operators and service providers exchanging Internet traffic. It is part of our core mission to represent our members' interests in matters of public policy.

20. With more than 430 member organisations, including most major UK ISPs and most formerly-incumbent European operators, we believe we have highly informed expertise and are well placed to reflect the views of the ISP industry as a whole.

21. LINX has worked on behalf of its members on the development of policy for covert investigation of communications, including communications data since before the inception of the Regulation of Investigatory Powers Act 2000. We have worked in cooperation with the Home Office and law enforcement representatives to develop primary and secondary legislation, Codes of Practice, building a partnership between the ISP industry and law enforcement interests. A LINX employee also represents the European Internet industry on the European Commission's Experts' Group on the Data Retention Directive.

22. We are committed to a regime for communications data retention and access that is both effective in meeting law enforcement needs and also respectful of the legitimate interests of the Internet industry, our members, and of the general public, the customers and end-users of our members.

23. We have consulted our membership both informally, during the development of this policy, and formally on drafts of this submission. This submission was finally approved by LINX's Board of Directors, which is elected by the membership. Although we would never say that any submission by us is endorsed by every one of our members in every last detail, we do believe that our position reflects a broad consensus of the network operator community.

Introductory remarks

24. We begin with some observations about the draft Bill, which will give some context to our answers to the Committee's specific questions.

25. Clause 1 of the draft Bill provides a very broad power to require the acquisition, collection and retention of communications data.

a. The power would apply[332] to private networks and services, not only to public telecommunications service providers as is the case under the current Data Retention Regulations[333].
b. The power appears to allow the Secretary of State to require that service providers collect subscriber data that they do not currently collect.
c. The government has stated its intention to access communications data under the Bill from telecommunications operators overseas.
d. Although the government has told us that their preference is to obtain communications data directly from the relevant service provider (eg. the web site operator), it also says that where the service provider is unable or unwilling to co-operate (for example, where the service provider is a foreign entity and prohibited from affording fully satisfactory co-operation with UK authorities by foreign law) it intends to use clause 1 to require network operators to monitor the network and extract communications data from the stream of traffic between their customer and the third party service ("third party communications data").
e. The types of communications data are not limited and specified, as under the Data Retention Directive, but unlimited and extensible. It is not clear whether extension would be by Statutory Instrument requiring Parliamentary approval, but the government's current reticence about disclosing what data types it intends to have collected indicates that any requirement would be specified in the Order to a telecommunications operator. If this is so, any change of extension would be at the discretion of the Secretary of State, which can be exercised in secret[334].
f. The Secretary of State is granted the power to micro-manage the means used by the telecommunications operator, even to the extent of specifying the exact equipment and network configuration that must be used.

26. In our opinion, any requirement to collect third party communications data is a material change to current arrangements. In many respects, collecting third party communications data is more similar to the interception of content than to the retention of existing communications records. At the least, it should be considered a novel, middle case, between classic communications data and intercept product.

27. We do not know which types of communications the government wishes to see analysed. The Bill provides for no limit, and government's comments on the challenges for the future suggest that communications services will be added progressively.

28. Clauses 14-16 create a substantial new facility.

---

[332] We acknowledge that the government is likely to concentrate in the first instance on public telecoms providers, but if Parliament grants a discretionary power then a much wider range of organisations could ultimately be required to collect communications data.

[333] Data Retention (EC Directive) Regulations 2009 No. 859.

[334] The Secretary of State is required to consult Ofcom, and those persons who would be subject to requirements under the Order that the Secretary of State deems appropriate, but this does not necessarily require publication of the notice to an operator or other transparency as to the specific intended requirements. On the contrary, a notice from the Secretary of State to an operator is likely to be covered by the Official Secrets Act.

a. The government has chosen to characterise this facility as "filtering requirements" and present it as a means to ensure that the data that is disclosed under Part 2 is limited; by contrast, some members of the Joint Committee have described this as a "search engine". While we think the latter characterisation comes closer to describing the power of this new facility, in our view comparison to web page search engines such as Google *understates* the significance of this new capability.
b. Clauses 14-16 establish a requirement that communications data be processed and assembled by matching related data from different operators, such that the relationships between diverse data elements relating to a particular user are capable of being machine-processed as such. **In other words, the draft Bill requires the functional equivalent of building *communications data profiles* on every user, which will contain everything within the definition of communications data, including time and geolocation data.**
    i. For example, in principle and within the terms and spirit of the Bill, the user profile[335] would contain the geolocation of their smart phone every time it checked for the new e-mail, which it might do automatically, every fifteen minutes.
    ii. The profile might also contain, for example, the name and date of access of every web site the user has viewed.
    iii. This would give a technical capability to perform profile searches of the following format: "List all persons who are the designated user of a mobile phone that was in Location (e.g. Trafalgar Square) at Time (e.g. noon last Tuesday), and who have read any of the following web sites more than once in the past period (e.g year)".
    iv. We are not clear whether it is also intended that this facility also include a technical feature known as "programmed triggers[336]". If so, that would enable searches of the form "Generate a notification when a mobile phone belonging to someone who has read any of the following web sites more than once in the past period (e.g year) comes within 500m of Location (e.g. Trafalgar Square).
c. An alternative designation for this facility would therefore be the "*profiling engine*".

29. To the best of our knowledge, these two main features (the nation-wide collection of third party data and the "*profiling engine*") are unprecedented, not only in the EU and UKUSA signatory countries[337], but also in China and the Middle East.

---

[335] Whether or not the data is literally stored in the form of "user profiles" is immaterial; the capabilities and user-interface to the facility provided under cl.14-16 would be the same.

[336] Programmed triggers is a term from database systems, referring to the ability to program the system to execute a command when certain conditions are met in the database.

[337] United Kingdom, USA, Australia, New Zealand and Canada.

Responses to the joint Committee's specific questions

Question 1: Has the Home Office made it clear what it hopes to achieve through the draft Bill?

30. The draft Bill provides extremely broad powers and appears to afford the Secretary of State a great deal of discretion as to how these are exercised.

31. The government has said about the Bill "Our work is about maintaining existing capabilities. It is not about developing new, more intrusive powers"[338].

32. In our view, the draft Bill would provide significant new and highly intrusive powers. How intrusively these are to be used is not clear, and would depend heavily on (a) the discretion of the Secretary of State as to what communications data should be collected, and (b) internal measures she establishes to guide public authorities' interpretation of the Human Rights Act requirement for proportionality in the use of communications data.

33. We are not clear on the extent to which the government intends that communications data made available under the draft Bill would be used as evidence in court proceedings.

a. In our view there are questions as to whether third party data and (especially) the product of the profiling engine in clauses 14-16, would meet evidential standards.
b. In the case of data that is the output of the profiling engine, produced by combining data from multiple sources, the authority operating the profiling engine would not be able to testify to the accuracy of the input data, nor would the telecommunications operators be able to testify that the data they supplied had been processed correctly by the profiling engine.
c. Therefore in many cases there might be no one entity in a position that could give assurance of end-to-end system accuracy and robustness.
d. Accordingly, we believe there are grounds to suspect that the product of the profiling engine might not be admissible in court. It would remain useful for intelligence purposes.
e. Analogous concerns apply in respect of third party data acquired by network operators: since the network operator is making mere suppositions as to how the third party service would use the data passing over the network it cannot be certain that the inferences it has drawn are reliable. In practice, we anticipate that there will be some cases where there is considerable confidence (for example, processing of what appears to be the use of a standardised and well-known communications protocol such as SMTP) but very many where there can be no particular confidence (for example, processing a web page input form). Thus, for a significant proportion of the data collected, it might be either inadmissible in court, or if admitted it might be granted limited weight.

[338] Home Office web site, 15th August 2012 http://www.homeoffice.gov.uk/counter-terrorism/communications-data/

Question 2: Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

34. The government has denied that the draft Bill amounts to new powers. Accordingly it has not presented a case for establishing the significant changes we identify in the Bill and set out in our opening remarks.

35. Instead, the government rests the case for the draft Bill on the claim that existing capability is receding:

> *Why is legislation needed?*
>
> *New communications technologies are generating communications data in different ways and communications data is no longer always retained by communications service providers. This has a direct impact on the investigation of crime in this country and on our ability to prosecute criminals and terrorists. Given the pace of technological change, this problem will grow.*
>
> *Legislation is needed to ensure that communications data continues to be available to the police and others in the future as it has in the past. This legislation will replace the communications data provisions of RIPA.*
>
> *Without action by the government there is a growing risk that crimes enabled by email and the internet will go undetected and unpunished.*[339]

36. Certainly, as people make ever greater use of Internet-based services, there is an ever greater quantity of data that either exists, or could be brought into existence by statutory requirement. However to say that this "is no longer always retained by communications providers" is highly misleading: communications providers are retaining more communications data than ever before and making it available to public authorities under existing law. The mere fact that even more data could be created, collected and made available hardly constitutes a loss.

37. We also note that the government estimates that its proposals will entail direct financial costs of £1.8bn over ten years. Even on the assumption that they can in fact be delivered for that budget, this is a substantial sum that could otherwise be used to fund substantial additional policing. We do not doubt that communications data is extremely useful for intelligence purposes and as evidence, but note that the additional communications data would have to be very important to be worth forgoing so much front-line policing.

---

[339] Ibid

Question 3: How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

38. As the government indicates in the quotation above, people are making ever greater use of Internet-based services. In fact, such services are becoming ever more tightly integrated into people's everyday lives, and entirely routine behaviour generates a complex trail of communications data from moment to moment.

39. As a consequence, the availability, value to law enforcement, and level of intrusion implied by even existing powers to access communications data continues to increase.

40. As noted above, the proposals in the draft Bill, specifically the requirement to capture third party data and the creation of a profiling engine, would dramatically increase the level of intrusion into individuals' privacy.

41. None of this is to give a view as to whether this level of intrusion is *justified*; it is for Parliament to decide whether law enforcement interests should override individual privacy. We do however believe our industry has a responsibility to ensure Parliament is fully informed about the implications of highly technical measures for the balance between the interests of privacy and those of public authorities.

Question 4: What lessons can be learnt from the approach of other countries to the collection of communications data?

42. We make no submission on this issue.

Question 5: Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

43. There is some overlap between this and question 7 (see below).

Question 6: The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

44. We anticipate that the draft Bill would supersede the current Data Retention Regulations. It would be helpful if that were confirmed.

45. The Data Retention Directive, from which the Regulations are derived, is due for review, and we anticipate the European Commission bringing forward proposals for a new Directive in 2013 or early 2014. Although it is too soon to be sure, early indications are that in at least some respects a new Directive might give greater weight to privacy interests than the existing Directive – for example, we consider it likely that the Commission will propose reducing the maximum retention period under the Directive. It is not clear what impact this might have on the regime proposed under the draft Bill. The current Directive is not a maximum harmonisation measure, but if the draft Bill went ahead, then given that the draft Bill goes so much further than any comparable measure in any other Member State, we would expect the Commission to come under considerable political pressure to respond.

Question 7: If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

46. We do not have a view on this question as stated.

47. That said, if it is concluded that it is essential to provide access to an unlimited range of communications data types, and to provide law enforcement with detailed profiles of communications data on all citizens, there do exist opportunities to introduce other measures in this space that would give greater weight to civil liberties.

a. **Prohibit third party data acquisition**: Provide that the responsibility to collect communications data lies only with the service provider who generates that data. Clarify the law relating to interception to make clear that accessing communications data passing over a network constitutes interception of that data, and is only lawful as provided for (e.g. as necessary for the purpose of conveying the data across the network).

b. **Provide greater distinction in law between different types of communications data with different levels of intrusiveness**, and apply different checks and safeguards to different types.

i. For example, "Reverse Directory Enquiry" information (what is the name and address of the subscriber to a phone number, and the equivalent for an IP address) might be considered the least intrusive, and so could be made available to a wide range of authorities, with little independent oversight and a light touch in auditing/reporting.

ii. By contrast, information about the geolocation of a mobile device – effectively, personal tracking – might be considered a newly available technique that is just as intrusive as the age-old technique of interception of content, and so subject to the highest possible level of safeguards.

iii. Other data types might have different levels of checks and safeguards. In particular, a distinction might be drawn between data that is intended to discover the identity an individual's correspondents and co-conspirators, and data which is intended to establish detailed characteristics about an individual (for example, personal preferences, income level, political views, shopping habits[340]).

c. **Introduce a greater range of authorisation methods**. The Committee has already heard testimony both supporting and opposing a requirement for prior judicial authorisation of

[340] In some cases this information would constitute content interception, and so not be available under the Bill, but in other cases the Bill would provide sufficiently rich information to allow reasonable inferences to be drawn, even if not always accurate ones. For example, whether someone reads www.telegraph.co.uk and www.conservativehome.org or reads www.guardian.co.uk and www.unitetheunion.org is communications data.

access to communications data, but there is no need for a one-size-fits-all approach. For example, prior judicial authorisation could be required for geolocation data but not for other types of communications data.

d. **Prohibit un-targeted searches** ("fishing expeditions") i.e. all searches of the profiling engine that are not limited by reference to an identified person.

e. **Provide that all data obtained by a public authority under the Bill must be sealed when no longer required** for the purpose for which it was sought. In essence, at the conclusion of an enquiry/investigation all data would be destroyed. However, where information might later become relevant again to the same investigation (notably, where it might be required by the Criminal Appeals Board) it should still be available for that purpose; this does not mean that all such information once obtained by the police should be freely available for use within the police in other enquiries, without separate justification, authorisation and audit.

f. **Provide a duty to notify data subjects when their data has been accessed**, as soon as this will no longer compromise the purpose for which it was sought.

    i. This would make the Tribunal a genuine remedy instead of a cipher, as people would know that they might wish to make a complaint.
    ii. This duty would be laid on the public authority that accessed the data, not the communications provider, so that the public authority is able to delay notification by reason of a risk of compromising an ongoing investigation.
    iii. To avoid an undue burden and causing needless concern, certain categories of data with low intrusiveness would need to be exempted.
    iv. It would also be necessary to exempt "collateral" access: for example, a request "Please list all the people from whom X received a phone call last month" would result in X being notified (in due course) but not the people who called him. This would be justified by reason of the fact that the intrusion into X was substantial, whereas that into his callers was more minimal. This exemption could also be statutorily dis-applied when appropriate (for example, when X is a doctor's surgery, or an MP's surgery).

g. **Establish a credible supervisory authority**, with adequate powers and detailed duties. The Interception Commissioner's duties as set out in RIPA are broad but non-specific, which may have led to the Commissioner seeing his role as simply to reassure that there is not widespread misuse of the relevant powers. A strong supervisory authority could be required to do much more:

    i. To draft, consult the public on, and possibly to issue, guidance on the proportionality of intrusion into privacy through access to communications data in common scenarios

    ii. To draft, consult the public on and issue, guidance on application of statutory categories to particular types of communications data (e.g. what is traffic data)

iii. To collect, collate, analyse, comment on and publish statistics on the use of communications data, perhaps by reference to other countries, and by reference to international standards

iv. To make regulations regarding safeguards and protections established under the Bill e.g. notification of data subjects, what constitutes a prohibited fishing expedition etc.

h. **Exempt the Intelligence and Security Services from certain of these safeguards.** The particular requirements and special status of the Intelligence and Security Services might be thought sufficiently important to prevent implementing certain safeguards that might otherwise be justified. That need not be a reason for relieving more quotidian public authorities of such oversight.

48. We do not recommend the above-mentioned options, but simply offer them as a contribution to debate, as examples of things that would give greater weight to the civil liberties interest, if that were thought desirable.

Question 8: Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

49. Yes, these proposals are very likely to make communications service providers see the UK as a less attractive base. They also make it more likely that communications service providers based outside the UK will prevent their service from being accessed from within the UK.

50. The Internet-based sector is one of the most dynamic and innovative parts of the economy.

a. With the whole world teetering on the edge of prolonged recession, low-value primary and manufacturing industries already having largely left for cheaper regions, and the financial services sector in which we thought we excelled having turned out to have inflated its apparent value through the assumption of excessive risk, the UK's prosperity depends as never before on knowledge-based businesses to which the Internet provides essential support.
b. Whether it is in industrial research such as our pharmaceuticals industry, industrial design, high-end manufacturing, the entertainment, fashion and advertising industries, services such as logistics and business support, or the consumer web services most commonly associated with the Internet, all the UK's best and most brightest prospects for economic growth depend on access to the best and most innovative Internet services.
c. The Internet sector therefore has an enormous wealth multiplier factor, especially for a high-value high-skill internationally trading economy like ours.

51. Accordingly, any action that undermines the positive effect of the Internet sector could have serious economic consequences, with implications well beyond the companies directly affected themselves.

52. The government has promised to reimburse those financial costs as can be calculated as directly attributable to the cost of delivering the requirements imposed by the Bill. We strongly welcome this commitment.

53. In our view, despite the government's commitment to cost recovery there will inevitably be unrecoverable costs to telecommunications operators.

    a. The draft Bill would require network operators to construct substantial new systems that do not currently exist:
        i. Network probes, to monitor and process traffic over the network, to acquire, extract and store communications data from third-party communications;
        ii. Data storage facilities (for data types that the network operator does not currently hold)
        iii. Access, search and retrieval mechanisms
        iv. In particular (since this appears to us especially technically challenging), systems to process communications data into standardised formats and make it available in real-time to the "*profiling engine*".
    b. These systems would include not only hardware, but also the creation of a myriad of business processes to support them.
    c. While these direct costs would be recoverable under the government's proposals, we consider that such an extensive creation of new systems would inevitably also incur an incalculable, and hence irrecoverable, opportunity cost, as senior executives and the most talented technical staff are diverted into delivering these requirements and away from commercial goals such as the creation of innovative products and services.

54. The Secretary of State's powers under section are capable of being deployed in a manner that would further exacerbate the irrecoverable costs incurred by telecommunications operators.
    a. Clause 1(3) makes clear that the extensive powers of the Secretary of State under the draft Bill extend to specifying the use of particular techniques, systems and equipments and standards – and, by implication, avoiding the use of others.
    b. This power to micro-manage the telecommunications network operator could in theory be used by the Secretary of State to order the operator to avoid the deployment of systems or the use of techniques that made it impossible to collect communications data, or that resulted in such collection becoming more costly.
    c. The consequence of this power being used in such a fashion would be to impose on the telecommunications operator costs other than direct financial costs. Examples of such cost might include
        i. Performance degradations
        ii. Reductions in network and service resilience
        iii. The inability to offer a particular service to customers (when other, foreign, operators were not so constrained)
    d. Although such costs would not be recoverable as direct financial costs under the draft Bill, they would make the telecommunications operator that incurred them less attractive to its customers and users than other foreign operators.

55. UK-based operators would therefore find themselves at a competitive disadvantage.

56. Foreign operators will accordingly have a significant incentive to avoid exposing themselves to the possibility of incurring such irrecoverable costs, by avoiding establishing themselves in the UK.

QUESTION 9: IS THE ESTIMATED COST OF £1.8BN OVER 10 YEARS REALISTIC?

57. We are not aware of any government-led IT project originally costed at £1.8bn that came in on budget.

58. As we have already noted, there is a wide discretion in how the powers might be applied and the duties that would be laid on telecommunications operators. As a corollary, there is a wide range in the costs that might realistically be expected.

59. We also expect that if this draft Bill is passed the duties of telecommunications operators would be progressively increased over the years to match increasing ambitions of public authorities, as they learn the power of the facility provided and incorporate its use in their everyday activities. This would imply the costs would also rise over time.

Question 10: The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?

60. In relation to the figure of £5bn-£6.2bn of benefits, the government's impact assessment states

> *The largest categories of benefits are direct financial benefits arising mainly from preventing revenue loss through tax fraud and facilitating the seizure of criminal assets*

61. We understand that the Home Office has refused to disclose information about how these anticipated future benefits are made up in response to Freedom of Information Act enquiries, on the grounds that doing so would prejudice the prevention, detection and investigation of crime.

62. Accordingly, we do not know the respective contributions the government expects from recovered proceeds of crime and reduced tax fraud. Given the disappointing results of the Asset Recovery Agency in the former area we assume that majority of the £5-6bn the government hopes to receive will be new tax revenues, equivalent to around 12-14% of corporation tax receipts.

Question 11: Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

63. The definitions are not aligned with the definitions found in other sector-specific legislation, notably "public electronic communications service" and "public electronic communications service provider", from the Communications Act 2003, nor the broader "information society service provider" found in EU legislation.

64. The draft Bill instead refers to "telecommunications operators" and – we emphasise – this is not limited to *public* telecommunications operators.

a. In fact, the definition of telecommunications operator is so broad that any business or household with two computing devices connected together would qualify.

b. We do not mean to suggest that we think the government intends to impose the requirements on practically every household, but simply to point out that there is no limit under the Bill to whom the Secretary of State could choose to select.

65. Although the wording of the definition of "communications data" has not changed from that in Regulation of Investigatory Powers Act 2000, the application of the duties to over-the-top Internet services such as search engines, social networking sites and so forth changes the effect substantially.

66. This effect is particular pronounced in respect of subscriber data, for which the definition essentially means "everything the service provider holds on the data subject". When RIPA was passed, that was loosely translated in most people's estimation (if somewhat inaccurately) to "reverse directory enquiries, plus your itemised billing data". If this Bill is passed, a similarly loose translation will be made: "Everything on your Facebook profile, plus everything Google knows about you". At this point the distinction between "communications data" and "content" becomes rather blurred, if it does not disappear entirely; we note that although the definitions for "traffic data" and "use data" explicitly exclude content information, no such exclusion applies in respect of "subscriber data".

Question 12: Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

67. We have no comment on this issue.

Question 13: How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

68. We do not know the answer to this question and would welcome further clarification from the government.

69. As a matter of principle, we caution against attempting to legislate with extra-territorial effect: even if ineffective it is likely to cause more harm to the UK economy than good, as foreign operators shun the UK. However if it were seen as effective that would give much greater cause for concern, as it would likely lead to other countries seeking to impose their laws extra-territorially too, causing chaos and legal uncertainty in the Internet sector and causing most harm in internationally trading economies like the UK.

Question 14: Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

70. We do not offer an opinion on whether the increased intrusion implied by the draft Bill is justified by the needs of public authorities.

71. We do note, however, that there are certain types of crime that are *inherently* impossible to investigate without use of communications data. Attacks on information systems themselves, for the sake of vandalism, might be one such example. By contrast there are other types of crime for

which investigation might be made much more efficient with the use of communications data, but which prior to the availability of communications data was previously investigated using others means. Criminal conspiracies, or anything involving money laundering, might fall into this category. We would be concerned if any attempt to protect civil liberties were to accidentally foreclose the possibility of investigation into certain types of crime. If Parliament were to respond to the government's proposals by taking the opportunity to tighten the grounds of access to existing communications data significantly, we would hope it would make adequate provision for cases where investigation was inherently impossible without communications data.

72. We note that the government is relying very heavily on the general requirement in the Human Rights Act that public authorities' actions that implicate protected privacy rights be "necessary and proportionate".

73. We acknowledge the importance of this requirement in general, but believe that without appropriately written rules, guidance and training (of which we have seen no evidence) this general prescription cannot bear the weight placed upon it.

74. With the best will in the world, we do not see how officials in a wide range of public authorities will be able to make appropriate or even consistent decisions unless they are able to discuss openly a range of scenarios, some indicating access that would be proportionate, others that would be disproportionate.

75. We recognise the need to conceal the detail of investigation methods in order to protect their efficacy. However the government's current level of reticence is so pronounced, even when testifying before this Joint Committee, as to preclude any reasonable discussion of guidance on what is considered proportionate.

Question 15: Is the proposed 12 month period for the retention of data too long or too short?

76. We do not have a definitive position on the correct storage period, but note that the majority of communications data accessed by public authorities under existing powers is less than 3 months old, and an overwhelming majority of the remainder is less than 6 months old[341].

Question 16: Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

77. We make no submission on these matters.

---

[341] Source: European Commission Experts' Group on the Data Retention Directive, room document.

Question 17: Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

78. We make no submission on these matters.

Question 18: Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

79. We make no submission on this matter.

Question 19: Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

80. No, the level of Parliamentary oversight is wholly unsatisfactory.

81. We do not submit an opinion as to the level of intrusion that is justified in the public interest, but consider it proper that Parliament should determine the necessary balance between the public and private interest, rather than delegating that essential responsibility to the Executive.

82. Although it is inevitable that certain levels of detail must be shielded from the public scrutiny of the Parliamentary process, in our opinion this draft Bill veers too far in favour of Executive discretion.

a. The draft Bill fails to establish any framework for the balance to be struck between the public interest in supporting public authorities and the private interests of the citizen in their privacy and of commercial entities in retaining the confidence of their customers.

b. Instead, the draft Bill provides for sweeping powers that could be exercised in ways that range from simply replicating the current system through other means[342], to the creation of a system of national surveillance and investigation-by-statistical anomaly that is without precedent in the free world, quite possibly in the entire world.

c. In our opinion, if such sweeping changes are required in the relationship between the citizen and the State, as regards their private information, and in the relationship between the telecommunications operator and the customer, as regards the limits of confidentiality, it should be because Parliament has determined that this is so after due deliberation, rather than because the Executive has secretly shifted its policy for administrative convenience.

---

[342] This benign extreme would only occur if the clause 14-16 powers were never activated, and Orders under clause 1 only specified the operator's own data, never third-party data passing over the operator's network.

83. Operators will be subject to substantial but unpredictable new burdens if this draft Bill is carried.

a. The extent to which network operators will be required to acquire, process and store third-party communications data under clause 1 is completely unknown.

b. The government has stressed that in the first instance it would prefer to obtain communications data from the relevant service provider, and would only require the collection of third party data where the service provider is not able or willing to cooperate.

c. However, the government has given no indication at all about the extent to which this "residual" third-party data would be demanded.

d. Nor do we have any real indication of the extent to which this demand will grow over time. All the government's remarks concerning the development of the communications market and its perception of the challenges to law enforcement are consistent with the fear that the government's policy on acquisition of this "residual" third-party data would be "Only as much as we can manage in the first instance, and as much more as we can manage as fast as we can manage it".

e. The nature of the burden is not limited to direct financial costs and the unrecoverable opportunity cost implicit in the need to design networks and services to meet public obligations instead of pursuing private and commercial ends[343]. The burden also encompasses duties that impact on the essential relationship of trust and confidence between the operator and its customers[344].

84. In our opinion, telecommunications operators as well as citizens have a legitimate interest in the reasonable foreseeability of regulation to which they are subject, and a right to make representations to Parliament when fundamental changes to regulation are contemplated. This implies that legal rules that make crucial changes to the business environment ought to originate in clear legislation; legislation ought not to authorise unbounded Executive discretion.

85. The draft Bill does contemplate statutory instruments with Parliamentary oversight (and in some cases positive approval) but we fear it would be rash to expect these to provide the necessary opportunity for democratic scrutiny.

a. Unfortunately, nothing in this draft Bill suggests that such Regulations would provide any more transparency or ability for Parliament to make an informed value judgement than the blank cheque that this draft Bill resembles.

b. Moreover, the government's demeanour in refusing to discuss application of the proposed powers, including its reticence before this Joint Committee, signals an intention to avoid meaningful oversight.

c. If our fears were realised, Parliament would have no effective oversight or control over the real effect of this Bill, the operative parts of which would be contained in notices to operators made by the Secretary of State, addressed to individual operators, at her discretion and cloaked by the Official Secrets Act and commercial confidentiality.

---

[343] See further our reply to Question 8

[344] Some of our members report having already received approaches they received from customers who, reacting to the government's proposals under the mistaken belief that they are already being implemented, expressed concern on this issue.

86. The government has steadfastly refused to show any meaningful transparency with ourselves or with this Committee as to what data would be sought, from whom and in what circumstances. It has shown a remarkable lack of candour in seeking to portray this as a minor technical update of the law with no significant change to the powers available or the overall level of intrusion represented thereby. It has drafted a Bill that appears to leave the Secretary of State with huge discretion in relation to the acquisition of communications data, without any requirement for proportionality except insofar as she is constrained by the Human Rights Act[345]. By far the greatest weight in deciding whether to access communications data lies in the unguided, unsupported and effectively unreviewable interpretation of the subjective term "proportionality" as applied by officers working for the same public authority seeking the information.

Question 20: Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

87. The draft Bill provides a statutory duty on communications service providers enforceable through the courts in the usual manner. Failure to abide by a court order would render the service provider liable to potentially unlimited fines for contempt of court.

88. There is, however, no specific regime for statutory penalties. In our view, given the hugely complex and uncertain nature of the obligations, and in particular the considerable scope for error (such as, for example, the Secretary of State specifying an technical obligation in terms with which it is literally impossible to comply), any more onerous regime for telecommunications operators would be inappropriate.

Question 21: Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

89. We do not make a submission on the administrative law question concerning the most appropriate way to regulate the public authorities under this draft Bill, except to say that effective and dissuasive sanctions for corporate misuse should be found.

90. We believe it should be an offence for an officer of a public authority to request or obtain access to communications data under cloak of pretended authority but without authorisation. It should also be an offence for such an officer to obtain such authorisation fraudulently.

Question 22: Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

91. In respect of network operators capturing third party data, the answer to this question is No. To the extent that anyone thinks the answer is yes, they can only be referring to experimental or prototype systems, or small scale analogues (e.g. organisation-wide, rather than ISP-wide): systems

[345] Although we believe the Secretary of State is technically bound by the Human Rights Act to consider the proportionality of her decisions, given that they would be justified in part by reason of the interests of national security we have doubts as to whether the proportionality test is effectively justiciable.

offering the functionality envisaged in clause 1 and clauses 14-16 have never been deployed and tested on a national-scale before, anywhere in the world.

Question 23: How safely can communications data be stored?

92. Network operators have a good track record in securing data such that it is never accessed except by authorised systems.

93. That said, once the data is outside the direct control of a single network operator it is becomes much harder to secure.

94. The "*profiling engine*" would be an incredibly valuable target for attack by sophisticated criminals, terrorists, and State actors engaged in espionage.

a. Examples of communications data that might be of interest to criminals includes
    i. Contact between their criminal co-conspirators and the police;
    ii. Market-sensitive information of all forms, e.g. the contacts of members of investment banks' and law firms' Mergers and Acquisitions advisory departments.
    iii. Information supporting blackmail, e.g. regular late night phone and text messages might be evidence of an extra-material affair – celebrities and politicians would be especially vulnerable to blackmail in these circumstances.
b. Examples of information that might be of interest to terrorists includes
    i. Geolocation information on prominent persons e.g. the Prime Minister.
    ii. Contacts (e.g. family) of security/bodyguards for prominent people, leading to geolocation of those contacts.
c. Examples of information that might be of interest for espionage includes:
    i. Contacts between business and government during sensitive, high-value negotiations e.g. high-value defence procurement, trade agreements etc
    ii. Contacts between government leaders and leaders of foreign governments (or between the close advisors of such leaders)
    iii. Intelligence on the domestic political situation e.g. full access monitoring of the phones of MPs might be able to predict the date of collapse of the Coalition.

95. Furthermore, as even prominent people transition from relying mainly on the phone to using new communications technologies, existing protective measures (such as ex.Directory) will become less effective. With sufficient access, security through obscurity won't work either: the system will be able to *discover* a target's communications devices.

96. Were the "*profiling engine*" to be compromised by external technical attack ("hacked") the impact would not necessarily even be limited to providing the attacker with the capabilities in use by public authorities: a successful attacker would not be limited by the self-restraint applied by legitimate public authorities in the interests of proportionality, but only by his technical capabilities.

97. It will therefore be vitally important to protect the profiling engine from attack, as if it were compromised it could constitute a serious threat to national security.

98. The "*profiling engine*" would be accessible, as far as can be told from the Bill, to a large number of individuals from a wide range of different organisations. This indicates that it will be challenging to protect the "*profiling engine*" not only from technical attacks, but also from human attacks (social engineering, infiltration of personnel, suborning of authorised users through bribery, blackmail etc, and so forth).

99. This combination of supremely high value to the right people, an enormously sophisticated but poorly understood capability, and broad accessibility, gives considerable cause for concern about the security of the access interface.

Question 24: Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

100. The systems integration challenge implied by the need to connect the communications data of all public communications systems used in the UK (including systems outside the UK accessed from within it) in a manner that all the data can be cross-linked as envisaged in clauses 14-16, can only be described as immense.

101. It should be noted that not only are there a huge number of systems to be linked, but that in most cases the people doing the linking, the network operators supported by CESG, won't be the people who own and control the systems being linked (foreign communications service operators) and in many cases the system controller will be actively trying to thwart the efforts of the systems integrator.

Question 25: How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?

102. We anticipate it will be relatively straightforward for a moderately sophisticated and surveillance-aware criminal to conduct occasional covert communications despite the measures in the draft bill.

103. Maintaining a covert presence on an ongoing basis will require discipline and determination, as well as skill – or alternatively, it could be done with very little skill or effort in a scenario where the use of encryption for online communications becomes commonplace. Unfortunately for the government's aims, the latter is, in our opinion, quite a likely occurrence, and even more likely should the draft Bill become law.

104. As we say below, encryption enables individuals to circumvent the provisions in the draft Bill that envisage the collection of third party communications data by network operators. Indeed, the widespread use of encryption in commonly used software as an essential part of maintaining a secure communications environment[346] means that individuals will circumvent these measures without even realising that they are doing so.

[346] The option of prohibiting the use of encryption is not realistically available as the security of Internet-based communications rests heavily on the use of strong encryption. For this reason, proposed legislation to grant the government a "back door" into all encryption software was abandoned by both the UK and USA in the mid 1990s, when it was realised that the economic harm that would be done outweighed even the interests of the intelligence community. In the UK, the *Regulation of Investigatory Powers Act 2000* was the legislation brought forward in place of the abandoned proposals, to provide an alternative means of addressing the needs of the law enforcement and intelligence communities.

105. There is also a disquieting possibility that some individuals, in an effort to circumvent the measures in the draft Bill, will employ non-standard technical counter-measures that could cause harm to the security, performance and reliability of networks and services.

Question 26: Are there concerns about the consequences of decryption?

106. In the presence of widespread encryption, the intention to co-opt network operators to conduct mass surveillance of third party communications data is in our view doomed to failure.

a. There are only three technical possibilities for defeating widespread encryption
    i. Performing a man-in-the-middle attack;
    ii. Covertly subverting the encryption software;
    iii. A fundamental breakthrough in mathematics
b. We do not believe that any of these could be deployed on a nationwide scale and still remain secret for long
c. The consequence of being discovered using any of these techniques would be very serious for public confidence in the security of online communications, including business communications – not just confidentiality, but also authentication.

August 2012

Alastair Macmillan

It is very easy to drift down the path of totalitarianism in the interests of "security" by only considering the technical aspects of this draft bill. In Great Britain we have a long history of Freedom, Habeas Corpus, and Innocence until Proved Guilty etc. These rights and freedoms are fragile and one would hope that our legislators would work hard to protect them. However, in recent years, this has not been the case and once again we are seeing legislation being proposed that limits the freedom of the overwhelming majority in the name of "security".

A continuing ratcheting up of the legislative framework will not catch those that want to undermine our way of life but will simply provide yet more ways for the state to criminalise the innocent and provide yet more power to petty officialdom.

Whenever legislation of this sort is proposed it is said that those enforcing it will be accountable to Parliament, this as always and from the point of view of the British Subject is naïve bunkum. In reality should I for example be "snooped" upon by an agent of the state, it will be one or more petty official that you or I will have to deal with to clear my name. The law puts power into the hands of these people at the expense of you or I, who will be deemed guilty until we prove ourselves innocent.

In summary it is essential that you raise your eyes from the purely technical aspects of this Bill and look at the overall picture of the balance between Britons and the British State. The last Government was probably one of the most Totalitarian Governments that the UK has ever had out of wartime and the extra powers it gave to the police and security services did little to boost respect for these bodies within Society as a whole. The legislation enacted also encouraged sloppy policing by providing "catchall" clauses , allowing "anti-terror" legislation to be used to limit freedom of expression and the right to demonstrate and question.

Instead of the treadmill of creeping totalitarianism I would suggest that the Police and Security services are made of work with the Public so that we are all encouraged to be responsible for our own and thereby everyone's security. This is the way we have protected ourselves in the past and is the way of Churchill's "small platoons".
Having recently returned from Portugal where one almost needs a licence to breath, I value even more the Freedoms we enjoy in the United Kingdom and I look to you as one of our legislators to work to protect them.

August 2012

Professor Robin Mansell

General:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

1.1 The Home Office is seeking to protect the public by ensuring that communications data necessary to achieve this aim are available to public authorities upon request. This ambition is clear. The evidence base supporting the draft Bill is unfortunately very weak.

1.2 This submission is directed principally to major omissions in the draft Bill and debate about this legislation. These are: a) the absence of evidence of consideration of the costs and risks associated with mandating companies to invest in a 'big data' infrastructure for the purposes of the draft Bill without adequate transparency; and b) insufficient detail as to the means of achieving transparency and adequate scrutiny of the technical means to be employed.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

2.1 No. The Government's case rests on the observation that technical change means that subscriber, use and traffic data that might be of use to authorities are either not collected by communication service providers, or they are, but legislation does not permit authorities to obtain them. Therefore, without action, the authorities will fall increasingly further behind in their ability to access the data they need to protect the public. Whatever the validity of this claim, it focuses disproportionately on accessing data without giving adequate attention to the risks associated with the development of a new 'big data' infrastructure or the transparency of the technical methods used to acquire and process these data.

2.2 A new big data infrastructure: Creating a new data infrastructure for collecting and retaining huge amounts of data, filtering it and processing it, will create new risks that need to be considered **before** these procedures are put in place.

2.3 By creating the incentive for all communications service companies in the UK to build an infrastructure to collect and retain data that they would not normally retain, the Government is legitimizing such practices for all companies, extending the potential for harmful uses of this infrastructure by these companies (purposively or inadvertently), and creating the possibility that these data stores will be breached in ways that may create hazard or harm.

2.4 The potential for data misuse is substantial. In addition to the problem of the use of the infrastructure to intrude into citizens' lives, the existence of such an infrastructure will enlarge the scope for new forms of cyber-crime or inadvertent 'data loss'.

2.5 Estimates about the costs and benefits of the obligations to 2018 are provided, but there is no clear indication of what assumptions have been made about the risks of illegal uses of the new data infrastructure once it is in place.

2.6 It seems to be assumed that only a limited number of companies will build the necessary infrastructure for collecting and retaining data. Yet, this legislation appears to make it legal for any company to develop the data infrastructure in readiness for potential requests for data, raising the risks of data breaches and illegal uses.

2.7 There are likely to be many new risks and costs. There is no basis for reaching a judgment as to the balance between these risks and costs and the benefits claimed as a result of this legislation. **No step should be taken** toward mandating investment in this new data infrastructure until such time as there is better evidence about the risks of hazard or harm.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

3.1 It is claimed that the use of DPI and Request Filter algorithms will ensure that authorities do not capture content. It is not feasible to make a distinction between communications data and content because all electronic communications can be interpreted for their meaning.

3.2 This applies to the interpretation of patterns emerging from the analysis of communications data such as use and transaction data, e.g. the title of a URL link, as much as it does to the analysis of conventionally understood digital content, e.g. the content of a web page or the content of an e-mail.

3.3 Even if conventional content is separated from other forms of information which have meaning, the expansion of opportunities for authorities to draw inferences about citizens' intentions or behavior from patterns emerging from electronic traces of their activities is growing exponentially with increases in the volume of the data that citizens generate through their active and passive (e.g. mobile phones being carried from one place to another) use of digital technologies and networks.

3.4 There is no detail in the draft Bill as to what technical algorithms will be used to extract meaning from communications data or what standard of reliability is acceptable. Legislation should set a standard as an acceptable target for performance subject to review in the same way that standards are set for other public services. There need to be agreed **target benchmarks** against which the proportion of errors can be judged.

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

8.1 The UK communications market is growing. Communication service providers are unlikely to withdraw from the market. They will evaluate the costs and benefits of compliance based on the likely impact on their revenue base.

8.2 It is not only communication service providers that should be considered, however. Customers who are knowledgeable about the increasing scope of communications data monitoring may choose services that appear to offer them greater protection from intrusions such as encrypted service offerings.

8.3 When the construction of a mandated big data infrastructure paid for in part by the state is available to them, some companies are likely to avail themselves of the opportunity.

Scope:

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

13.1 The overseas communication service providers that are often discussed are highly visible companies. It is realistic to envisage their compliance in light of their interest in the UK market **if** their home governments align their legislation with UK legislation. This neglects less visible companies located in countries that already allow State-sponsored monitoring of communications data. Failed states and States that are unlikely to cooperate with the UK for political or economic reasons will not be pursued effectively. At present a few highly visible global companies generate a substantial portion of relevant data. In future, those seeking to engage in serious crime or terrorism are likely to shift to companies that are less prominent and, where feasible, to companies based in uncooperative States.

Safeguards:

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

16.1 The integration of many distributed databases is happening extensively in the 'big data' era. There is no basis at present for believing that the Government or third parties will be able to achieve an acceptable standard for data integrity and security.

16.2 The history of electronic data processing systems shows that error (accidental or with mal-intent) is the main reason for data insecurity. It also shows that efforts to improve the record in this area are not keeping pace with capacities to collect and process data. No evidence has been provided to support a claim that this situation has changed. The extent of potential intrusions into citizen's private lives is unknowable, notwithstanding claims by technical experts who have, historically, been gravely mistaken about such issues.

16.3 Authorisation of data requests must be given by **judicial authority** to ensure citizen rights are protected. In the 'big data' era it is not sufficient to rely on designated senior officers within organisations for such authorization when they have an interest in securing access and use of such data or on retrospective audit of the outcomes. Judicial authority should apply in all cases, and not be limited to local authorities.

16.4 Relying upon a 'designated senior officer' is inconsistent with Article 8 of the ECHR to the extent that it effectively grants judicial authority on issues of 'national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'. Without this authorisation, there is no satisfactory system for preserving the rights of minorities in a majoritarian democracy.

16.5 Transparent means of assessment of the likely risks associated with a ubiquitous big data infrastructure for collecting and retaining data by commercial firms is needed.

16.6 Transparent information is needed about the way the match between the 'plain text' requests for data and the programming of software algorithms will be audited with preset targets and standards for performance.

Technical:

23 How safely can communications data be stored?

23.1 See 2.1-2.7 regarding the risks of creating this new infrastructure for data storage. An important additional issue is the re-transmission of these data to permit processing of data from different decentralised locations. This raises additional security issues because a large number of requesting agencies will be involved.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

24.1 Achieving transparency and scrutiny of technical means: Filtering algorithms are to be employed. It is unclear who will be held accountable for the design of these algorithms. The algorithms (the instructions programmed into the request filters) through which the authorities obtain data and the instructions programmed into the software to aggregate and analyse the data must be available for independent scrutiny.

24.2 Those responsible for public protection may argue that placing this information in the public domain makes it available to those who seek to engage in serious crime or terrorism. The response is that transparency requires independent audit of the inputs with respect to more than whether the Request Filter is 'functioning properly' (Clause 16). It needs to be clear that scrutiny relates to the match between the 'plain text' instructions that are authorized and the actual programming of the technical tools. Independent technical experts (subject to confidentiality restrictions) must be able to verify that the programmed instructions achieve legal ends. In the absence of clarity about this issue, authorities requesting and processing data will be continuously open to charges of bias, i.e. data collection inconsistent with authorized activity.

24.3 Algorithms used to process requested data typically are based on judgments about the 'relevance' of data, just as in the case of commercial search engines. As a consequence, inferences may be made and patterns discovered that are spurious or misleading. There is no detail as to the specific standards to be met through the application of these algorithms.

25 How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?

25.1 As with all technical measures, the ease of circumvention depends upon the technological sophistication of individuals and organisations. The draft Bill creates incentives for improving this sophistication.

August 2012

Lorna Mitchell

General:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?
Not at all, I think we're still chasing terrorists?

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?
No.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?
They fit in with the general loss of privacy. They don't fit in with the beliefs about personal privacy that I believe this government to hold, or the laws that are in effect in my country (i.e. the UK)

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?
Are there any proposals which outline why the government would need this data? I am unclear what we're trying to achieve or what the benefit would be.

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?
Most other legislations allow controlled access to data when there seems like there is grounds for requesting such access. I'm not sure how blanket access to any communications without needing anyone to know about it or grant permission could possibly fit under the same legislation.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?
Not in my opinion. Currently, I have some freedom as a citizen. This data collection produces WAY too much information which could be analyzed at an overall population level and be very valuable to commercial organisations.

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base.
What might be the effect on business?
Digital industries will leave the UK immediately. There will be a large market in selling communication arrangements which bypass the UK for both business and personal communications.
Costs:

9. Is the estimated cost of £1.8bn over 10 years realistic?

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?
I'm not sure that this measure could ever produce a monetary return on investment

Scope:
11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

They are wonderfully vague and the bill provides for them to be redefined at will and without notice. So I'm sure they can be adapted to any scope that this or any future government desires

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?
security agencies only. And no. Please let either the judges or the Lords represent the "man on the street" if changes are needed. They are the only representation he has in this country.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?entirely unrealistic to think that any country can legislate for anything overseas, this is impractical
Use of Communications Data:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?
The circumstances under which communications data can be accessed are wildly disproportional. We have surveillance laws so that, as a country, we can access data and movements of individuals who are suspected of crime. Surveillance of all citizens to identify any atypical behaviour simply isn't in line with british values.

15. Is the proposed 12 month period for the retention of data too long or too short?
Safeguards:

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory?

Are there concerns about compliance with Article 8 ECHR?

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?
Yes, a warrant system would be more appropriate. A non-political person should have final say. And that will be terribly expensive I should think.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?
The information commissioner is horribly under resourced. In principle, it's a great thing. In practice, not so much.

Parliamentary Oversight:

19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?
Enforcement:

20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

Technical:

22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?
This "communications data" of which you speak tells at least as much of the story as the content. In fact, I think I'd prefer you to read the content of my personal and business email rather than have all the meta data that this scheme would give access to - the potential for pattern evaluation and making of assumptions on what constitutes "normal" behaviour is quite frightening (I work in IT)

23. How safely can communications data be stored?
Very safely. The fact that the data exists is the problem.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?
A hassle, but do-able for anyone with reason to do so.

26. Are there concerns about the consequences of decryption?

August 2012

Glynn Moody

1. The UK government's Draft Communications bill is based on two flawed premises. The first is that communications information can be separated from content. That is manifestly not true when dealing with Web sites, since the address is almost invariably descriptive, and provides a great deal of information (and that's assuming that the UK government will not require individual Web page addresses to be stored, which would give even more details.)

2. For example, suppose somebody visited several sites about mental health problems: the mere fact of visiting them would of course give rise to the suspicion that he or she was experiencing some problems in this area. Now imagine that person had a role in government, or some role that required them to make life-or-death decisions: clearly, the fact that they had visited mental health sites could place their careers in jeopardy.

3. The other assumption is even more seriously erroneous: that a series of distributed databases holding local stores of information about individuals is far less problematic than a centralised system. The reason for this is that computing has moved on to such an extent that it is now relatively easy to carry out searches across huge numbers of databases; this means that there is no practical difference between the two.

4. It is these cross-database searches that are the real problem with the proposed surveillance scheme – the "filters" as they are called in the Bill. Computing power is so great now that it is relatively easy to carry out complex cross-database searches that link together apparently disparate information: call it the Googlisation of surveillance. Just as we can find links between areas that might seem quite unrelated, thanks to the power of Google's databases, so all kinds of connections will be found through the use of filters. In particular, it will be possible to map out practically any aspect of anyone's life by framing the right filters. Far from offering a very limited view of what people are doing online, the proposed databases will effectively know everything about everyone.

5. This brings me to perhaps the most problematic issue for the current proposals. In her introduction, the Home Secretary writes: "Communications technologies and services are changing fast. More communications are taking place on the internet using a wider range of services. As criminals make increasing use of internet based communications, we need to ensure that the police and intelligence agencies continue to have the tools they need to do the job we ask of them: investigating crime and terrorism, protecting the vulnerable and bringing criminals to justice." The basic premise is that the current proposals are simply bringing police and intelligence powers "up to date". This is not the case.

6. Instead, the ability to carry out cross-database searches using filters represents a massive and unprecedented extension of powers. It will allow the most intimate corners of people's lives to be interrogated by piecing together tiny scraps of apparently trivial information to form a complete portrait of their daily lives. Once local databases are in place, and can be searched in a unified way, it is inevitable that levels of information will be obtained far beyond the very simple options available today.

7. That is clearly problematic for a democratic society. It potentially gives governments unprecedented information – and hence control – about every citizen at all times, and in near real time. But there are other dangers.

8. As we know from the recent News International scandals, whenever confidential information is available, even to a limited range of vetted personnel, there will always be corruption that allows unauthorised access to that information. Even assuming the databases could be made secure – and in fact that's not possible, as any security expert will tell you – the weakest link remains the human one. Even when people are not corrupt, they may be open to blackmail or threats. Creating these

databases inevitably means that the information they hold will leak out and be abused. The only way to prevent this is not to create the databases in the first place.

9. The case for this huge and unprecedented extension of surveillance to levels way beyond what is available even to oppressive regimes around the world has not been made. Instead, there is a vague, hand-waving argument that it is a simply upgrade of current powers for modern times. As I've noted above, this is simply not true. The onus, therefore, must be on the police and security services to come up with truly compelling reasons for this unprecedented surveillance of a nation's most intimate details – mere convenience is not good enough.

10. It is worth bearing in mind that determined criminals and terrorists will in any case be able to circumvent the proposals, using strong local encryption and non-Internet based communications. So the only people adversely affected by the proposals are law-abiding citizens. Why, then, bring in an extremely costly system (cost overruns are inevitable, as history shows) that will add major new vulnerabilities to the UK's computing infrastructure, for what seems very little benefit? Until that is fully answered, there should be no question about bringing in the proposed system.

August 2012

Barbara Moore

There are only a few questions which I would like to consider in my response and I number the paragraphs accordingly.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

2.1 No. As the London riots revealed there is already sufficient legislation in place to enable the police to operate efficiently when their investigations require the collection of communication traffic data.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

4.1 If by that question you are referring to various African and Middle Eastern nations where there have been recent bloody revolutions and disappearances of the general population or the more historic monitoring in Germany and behind the Iron Curtain then the only lesson that the UK should be learning is that the collection of communication data should be discouraged in a democratic and free society. There should never be any monitoring without prior judicial oversight. Anything else will result in history repeating itself in this fair land.

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

6.1 Data should not be retained other than during an investigation. Access should be limited to those making the investigation and never retained by a commercial entity.

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

8.1 I am not too sure that I understand the first part of this question. For the second part, encryption is already the only way that any business can safely operate in the UK. Already the ISPs are monitoring and selling traffic data between businesses and their customers. Even the UK Government are purchasers of this traffic data. If the draft Bill has the effect of depriving the ISPs of this trade in data then it will be very good for UK businesses. However, the probability is that the draft Bill will make it cost efficient for ISPs to collect and sell even more data than is currently the case which will be a disaster for UK business and innovation.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

12.1 The general public would not expect any such access to extend beyond security services and police investigations. With all such access under court order only and subject to judicial review as to the appropriate use of the powers. It is essential that the people are protected from abuse of powers by Government.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

13.1 This is a laughable proposal. Or, perhaps, very frightening. Would it suggest that overseas governments would have similar 'rights' over the data of UK businesses? Any clause referring to data held outside the UK should be removed from the legislation.

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

14.1 A blanket collection of and access to data is not appropriate in any society which is based on democracy and independent judiciary. It should be up to a judge to determine whether or not a particular crime warrants the collection of communication data to facilitate a conviction. There should never be a list of 'approved' crimes.

15. Is the proposed 12 month period for the retention of data too long or too short?

15.1 This questions becomes meaningless when the blanket collection and retention of data is removed. Data should only be held for as long as is required to process a specific crime.

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

16.1 Another placebo question. If the data is held digitally it should be taken as read that it is not secure and will be compromised. Putting tick boxes to restrict who has access will do nothing to ensure the security of the data.

16.2 I know from my own experience that equipment attached to IP addresses under the control of NASA and The White House has been compromised and used in an attempt to hack into my own equipment. I like to think that my abuse report to NASA helped them to discover the breach which has recently been reported in the public media. I assume that there will never be a public announcement of the breach in the security of The White House network.

16.3 Anyone who offers a 'secure' solution to data collected under the draft Bill is doing so without explaining that digital data is not secure if there is access between LAN and WAN. The collection of data does require the use of WAN.

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

17.1 Anything other than a warrant system for all events should not be considered. As to resources, there seems little point in proposing legislation which will not include funding to provide adequate resources.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

18.1 I have no knowledge of ICC capabilities but have experience of the ICO being under resourced, under staffed and technically without the necessary knowledge to perform any role with any degree of reliability. Lawyers are rarely literate with regard to digital methodologies.

19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

19.1 It is unlikely that parliament will contain sufficient individuals with technical competence to carry out the role of oversight.

22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

22.1 No

23. How safely can communications data be stored?

23.1 There is no safe storage method.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

24.1 Technically the proposals are not feasible.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?

25.1 Exceedingly easy. Such circumvention methods are already widely known and used by people around the world.

26. Are there concerns about the consequences of decryption?

26.1 Encryption is already an essential to any communication due to the amount of commercial exploitation of communication data. When the public become more aware of their data being intercepted for innocent activities they will ask for more secure methods of encryption. Or find alternate methods of communication.

26.2 It is sad to think that it is becoming impossible for two people to communicate in private using any method other than speaking face to face.

August 2012

Alec Muffett

Note

I have read the submission made by Glyn Moody, which he has reprinted in Computerworld [1] and I see no value in addressing the points that have already been covered in that submission, other than to recommend them most highly as correct and worthy of consideration.

On Terminology
Following a cue from other discussion of the bill, I shall use the term Content Service Providers (CSPs) broadly, including firms that would more typically be referred to as Internet Service Providers (ISPs) - as well as including the likes of Google, Yahoo, Microsoft, etc, under that umbrella.

Keyword Summary

- anti-competitive business landscape
- negative impacts of regulation
- small/medium enterprise communications providers
- inhibiting business agility and growth
- conflict of strategic interest
- cybersecurity risk

Evidence
I would like to submit the following evidence:

On the Risks of CCDP Architecture
1. That in abandoning the former architecture suggested by the Interception Modernisation Programme (IMP) - that of building an Orwellian "centralised" database - in favour of a more media-friendly but equally Orwellian "distributed" database, the Communications Capabilities Development Programme (CCDP) greatly magnifies the information security management risks inherent in that system.

2. Therefore the costs are at least equally magnified; where once there was a nominally "single" database with centralised information security management there may now be a hundred with independent management and access controls; therefore the risks are multiplied by at least a hundred, and the cost of managing those risks will increase by a proportional factor.

3. Therefore it seems highly implausible that the Home Office quoted £2bn to implement IMP and yet now quotes a lesser figure of £1.8bn to implement CCDP.

4. So my answer to question 9 (*Is the estimated cost of £1.8bn over 10 years realistic?*) is "No, most definitely not, even allowing for Moore's Law because that will simultaneously be working to aid communicators and interceptors both".

On the Equality of CCDP to its forebear
5. Of course it is facile to sketch the IMP implementation as having ever been designed around a truly centralised database; to do so would require that for every N gigabits of network bandwidth between two arbitrary points in Britain (Glasgow and Edinburgh, say) there would have to be a second, equally-sized, dedicated N gigabits of network bandwidth just to carry a copy of *that* data to Cheltenham

6. So for IMP a copy of the entire British Internet would *also* have to flow to Cheltenham, an architecture which would not be tenable.

7. Therefore IMP must always have been based upon deploying distributed sensors performing data reduction and filtering before passing the data back to a controller, a system structurally identical to CCDP, putting the lie to the suggestion that they are in any way significantly different proposals.

8. So my answer to question 3 (*How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?*) is that "CCDP is the same as IMP, and should be entirely thrown out in

the same way and for the same reasons."

On CCDP's impact upon CSP technical implementation and profit margin
9. So the proposals are now for distributed databases at each Communication Service Provider (CSP), somehow at a reduced cost; the only way to achieve this is to gradually pass costs of the hardware onto the CSPs. This will lead to three obvious scenarios:

10. Large, well-funded CSPs will absorb the costs and manage their responsibilities towards a the interception devices with reasonable care, including locked hardware cages, restricted access to interception equipment hardware, security-cleared staff, etc.

11. Virtual CSPs (for instance, Tesco's ISP service) resell the services of large CSPs and therefore will be "covered" for compliant interception capability somewhat automatically - so long as we can assume that mechanisms exist that can tie a Tesco user's information to the identity of traffic traveling upon the underlying CSP network.

12. Small to Medium CSPs will be faced with a challenge: the cost of obtaining and installing interception hardware and of setting up special controls - hardware cages, restricted access, security clearances - will be a burden on capital and operational expenditure, making significant impact upon business margins.

13. This is because *security costs money to implement properly*.

14. But once installed at the Small/Medium CSP, the interception hardware will also impact upon creative network architecture; in a microcosm of the "Edinburgh/Glasgow" point above, a copy of *all* of the CSP's traffic will have to flow to the interception devices.

15. To an enterprise network architect this is akin to entering a boxing ring with a ball-and-chain secured to one ankle; it impacts your ability to make optimal use of the hardware that you have budgeted for and purchased because you are handicapped by government mandate - always having to bear in mind that one must not *tithe* but in fact wholly *duplicate* traffic flows so that the interception box may have its due; and that you must integrate your shiny new hi-tech network with inherently "legacy" (ie: somewhat archaic) approved interception hardware.

16. Also: Moore's Law does not (yet) stand still, so technology deployed to permit sufficient interception today will be overwhelmed in a year, perhaps three; so the ball-and-chain will have to be regularly replaced even if we quit boxing and instead take up the 4x400m Men's Relay - in which case multiple balls-with-chain will be suddenly required, and *possibly disposed of* if the architecture is backed-out due to failure.

17. So my answer to question 24 (*Are the proposals for the filtering arrangements clear, appropriate and technically feasible?*) is that irrespective of their feasibility the proposals are not appropriate and will negatively impact innovation at some of the places where Britain needs it most, viz: the SME Communications Sector.

18. The large CSPs understand this and are somewhat proof against it by virtue of their maturity and size, and thus are more than happy for the Government to deploy this inherently anti-competitive measure against those who might replace them by virtue of technical innovation in service provision.

On the Cost to the Consumer
19. So it should be clear that the costs of CCDP are eventually borne fourfold by the consumer: in extra service charges, in extra tax upon the same, in lost innovation and in lost competition.

On Intercept Data Remanence and Leakage
20. To return to the many interception devices; even if they become "virtual" devices that are somehow "in the cloud" they must still store their data somewhere, and through this diversity and frequent upgrading and replacement of interception devices it is inevitable that the data will eventually fall into the hands of the general public - either by error (selling old hard disks on Ebay) or malice (paying-off a supposedly trusted employee).

21. It goes without saying that such data is valuable; the fact that a particular IP address - corresponding to a famous footballer - repeatedly visits a particular pornographic website is easily a tabloid headline and

therefore of value.

22. It is possible of course to mitigate some of these risks through encryption, but then the question becomes one of *where are the encryption keys kept?* - if on the same hard disks then the decryption of the footballer's pornography habit is open to any journalist.

23. Or alternately "Hardware Security Modules" and other "Trusted" devices could be deployed to keep the keys, but this pushes up the cost of each interception device, and the complexity of managing it also - so once again we look askance at that £1.8bn figure and wonder where the cost of doing security "properly" is hidden?

24. So my answer to question 22 (*Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?*) is "Perhaps, but my suspicion is 'not at that price point', and "not with this distributed architecture and ownership", and further repeat that it is not necessary to see the actual content in order to write, blog or tweet a story that *Footballer X is visiting Porn Site Y every Friday Night*"

25. And my answer to question 23 (*How safely can communications data be stored?*) is "Very safely, but you'll have to pay rather more than £1.8bn to do it properly, and you would have to inhibit any change, progress or innovation within the CSP industry because the churn of technology will throw up the chaff of disposed interception equipment, ripe for amateur analysis."

On Technical Measures to Crack Encryption on behalf of Snooping

26. My answer to question 26 (*Are there concerns about the consequences of decryption?*) would include "Would Parliament assent to the security services decrypting and taking a copy of all HTTPS/SSL-encrypted web traffic leaving the Houses of Parliament?", but that might be considered flip, so I'll just say "yes" and note that others than members of Parliament might feel similarly; see also the Select Committee report referenced below.

On the capability to circumvent Interception

27. My answer to question 25 (*How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?*) is "Trivially easy; the technologies already exist, are widely deployed, essential tools for the liberty of citizens of repressive regimes, and will only get better and more numerous with time."

28. To ban these tools would be highly retrogressive, technically infeasible, [2] [3] set a bad precedent globally, and be disastrous for liberty.

On New Privacy Technology

29. Thus: because of the two scenarios outlined below I appeal to the committee to please revolt against the notion that there is ever a situation where security measures taken by individuals and organisations can ever be "too good".

31. It is of course very easy to have "too much" security - a suffocating problem that one might encounter at (say) an American airport; but that is not the same as security which is "too good".

32. Security can never be *too good*.

33. Underscoring CCDP (and its brethren) is the assumption that the Government needs to, indeed *must* have visibility not only of the fact of communication between two computers, but also that it needs to / must have visibility of (some) content of that communication, howeverso protected.

34. This assumption is evidenced by the very fact that question 26 (re: *decryption*) was asked in this call for evidence.

35. This assumption is misconceived, and in fact unwise.

36. The Internet - cyberspace - is a digital, on-or-off, one-or-zero, do-or-not-do place, where one's ability to attack another's system is largely a function of knowledge, understanding, competence and luck rather than logistics, and where natural defences such as the English Channel do not exist. In Westminster's cyberspace

one is as far from Tobermory as Moscow, and individual actors may appear as large and relevant as nation states.

37. Thus I am concerned that beyond the Government's helping itself to any data that is now openly available on the Internet, and/or any data which it might coerce from regulation of Internet business, its next logical step would be to prohibit adoption of technologies which restore absolute privacy to individuals and organisations.

38. We have seen such attempts before, with "Mandatory Key Escrow" in the late 1990s, demanding that everyone surrender copies of their SSL keys so that the security services could peep into everyone's encrypted transactions.[4]

39. So it strikes me that the future will contain an either/or scenario:

40. Either the security services learn to adapt to a world where there simply are some forms of data which they are not in a position to know, learn or demand, and thereby evolve alternative strategies to work around this - just as they did previously with the failure of Mandatory Key Escrow, and could do with the abandonment of CCDP.

41. Or else the Government to some extent bans its citizens from having strong security and privacy - from having security that is *too good* - thereby undesirably reducing the resistance of the British populace as a whole to cyberattack from the rest of the world, with the inevitable side-effect that the security services never evolve their skill set beyond "how to demand data from third parties".

42. The third option, of course, is to muddle along somewhere in the middle, trying to ignore the inevitable rise of internet privacy tools that are effectively interception-proof by virtue of being *too good*.

43. But that's what we're currently doing, isn't it?

–

[1] See: The Googlisation of Surveillance blogs.computerworlduk.com/open-enterprise/2012/08/submission-on-uk-governments-snooping-bill/index.htm

[2] See: How the Great Firewall of China is Blocking Tor www.cs.kau.se/philwint/pdf/foci2012.pdf

[3] See: How governments have tried to block Tor www.youtube.com/watch?v=GwMr8Xl7JMQ (video of public lecture)

[4] See: Select Committee on Trade and Industry Seventh Report www.parliament.the-stationery-office.co.uk/pa/cm199899/cmselect/cmtrdind/187/18713.htm which from 1998 strongly reflects much discussion that now surrounds IMP/CCDP

August 2012

Giles Murchiston

I, Giles Murchiston, respectfully submit these observations in a private capacity. I am not a lawyer. This submission had probably best be regarded as "other comments related to the draft Bill" rather than relating directly to the committee's 26 questions.
No doubt the Committee will have received many submissions that the Draft Bill is an outrageous violation of privacy, that the cost is either underestimated and/or disproportionate, and that data collection as required is technically or organisationally infeasible. This submission concentrates rather of what appear to me to be deficiencies in the proposed legal framework. Is is presented as a series of *desiderata*: items which it would be desirable to clarify of amend.

On Ensuring Availability.

Quotation from Draft Bill: 1(1)(a) *[The Secretary of State may by order] ensure that communications data is available to be obtained from telecommunications operators by relevant public authorities.*
Verily, how mighty is the Secretary of State, who can "ensure" anything in the ever-changing world of the internet: how mighty, rather, is the Queen in Parliament to be able to bestow this power. I venture to suggest this may be more difficult to achieve than the Draft Bill suggests.

One evident obstacle is that the telecommunications operator may outright say that it is impossible for them to obtain the required data. Perhaps they do not handle the data at all, or they may handle it but not have the expertise necessary to capture it, or they may say that even if the Secretary of State or other persons engage in activities to facilitate the obtaining, it would involve modifying proprietary software in a manner prohibited by licence provisions. (The statement that "Conduct is lawful for all purposes" if required by the Act doesn't necessarily help here: conduct can contravene a licence even if it is lawful[347].)

Some of these points may be explored by a reference to the Technical Advisory Board, if they can be defined as "technical" (or financial). However it appears that the Secretary of State is not bound by the Board's views and can insist on requiring the impossible. Whether she could persuade a court to grant an injunction to order the impossible is, perhaps, more doubtful (I am not a lawyer). In any case, even with the aid of the courts, she cannot ensure the impossible. Ultimately the operator, trapped between the rock of impossibility and the hard place of court sanctions, could be left with no alternative but to cease his telecommunications activities.

DESIDERATUM: if the Secretary of State envisages forcing out of business such operators who find themselves unable to comply with notices, she should say so during the consultation period.
A more dangerous possibility is that operators may indulge in what I might call "covert non-compliance", that is, accept the notice but take no, or inadequate, action to implement it. As the bill stands, they would not appear to be at risk of any penalty for doing this (unless the notice is backed by an injunction, which will presumably only be sought in exceptional circumstances). They might reason that the chance of being served with a request for Part 2 data is probably fairly low, and if they do receive one they can "minimise the amount of data that needs to be processed" and reply that they hold no data matching the requirement. The requiring authority may find this response implausible, but what can they do about it? – there are no *criminal* offences involved, so they can't get the police to investigate (or investigate it themselves if they are the police).

Well, I say no penalties, but it might be possible to constructively invoke some. If the operator claimed a contribution towards costs of activities which they are not actually carrying out, that

[347] That's sort of why licence conditions exist.

would presumably be fraud. This would mean that *declining* to claim a contribution would be inherently suspicious, perhaps to the point where the Secretary of State might seek to buttress the notice with an injunction. Whether the courts would accept this contorted logic I cannot guess (I am not a lawyer). Again, if the data was sought in support of a criminal investigation, it might be argued that failing to have collected it is tantamount to perverting the course of justice. Then again, on quite a different tack, if the operator is proving a service for which a licence is required, perceived malpractice might provoke withdrawal or restriction of licence with consequent loss of revenue.

DESIDERATUM: if the Secretary of State envisages that malpractice could lead to criminal or administrative penalties, she should say so during the consultation period.

On Enablement.

Quotation from Draft Bill: 1(2)(a)(iii) *[An order under this section may, in particular provide for]* the entering into by such operators of arrangements with the Secretary of State or other persons under or by virtue of which the Secretary of State or other persons engage in activities on behalf of the operators on a commercial or other basis for the purpose of enabling the operators to comply with requirements imposed by virtue of this section.

It seems to me that "Activities for the purpose of enabling the operators to comply with requirements" may be taken with two rather different meanings. It could mean setting up the operator himself to retain and disclose (in accordance with Part 2) the data, or alternatively to contract to provide a complete service of retention and disclosure (and even obtainment) on his behalf. Both are somewhat problematical.

If it is the first, why is it necessary to state it?—it would seem to be normal business practice, and there does not seem to be any prohibition of it even if the order (not, I note, the notice) fails to so provide. I think it is unlikely to be the second, on the grounds that it is unthinkable that the Secretary of State would engage in such an activity (I'm already a bit worried about the apparent suggestion that the Secretary of State can engage in any activity on a commercial basis). There is a potential niche industry here of Providential Data Retainer, and it seems a shame that the Government should fail to leverage the need to spy on its own citizens into a stimulus for private sector growth.

Is the distinction I have drawn between the two levels of involvement even a clear difference? The first level could extend to supplying hardware, and software, and even contract staff to operate these. Just what could the second level provide which would truly set it apart?

DESIDERATUM: to clarify the meaning of "enabling".

On Disclosure.

Quotation from Draft Bill: 5(1) *A telecommunications operator who holds communications data by virtue of this Part must not disclose the data except— (a) in accordance with the provisions of Part 2, or (b) otherwise as authorised by law.*

Now wait a cotton-picking minute, what's with this "otherwise"? Section 1 said "available to ... relevant public authorities in accordance with Part 2". Part 2 provides that only specified authorities can access data, and only for specified purposes[348]. But here is a wide-open back-door in Part 1!

---

[348] although I would quite like to know which body investigates matters "in the interests of the economic well-being of the United Kingdom" and what success they have achieved

I thought this might have been parliamentary draughtsman's force of habit to avoid one statute forbidding actions which another (which one can't immediately call to mind) demands. However this clause is supported by an explanatory note "These (*sic*) may include a request under section 7 of the Data Protection Act 1998 (which provides an individual with the right of access to personal data) or in pursuance of a court order."

I will leave it to the Information Commissioner to provide guidelines as to which Communications Data can be viewed as Personal Data under the DPA, which raises a number of fascinating questions.

The "in pursuance of a court order" bit is altogether more concerning. It appears, for instance, to admit the possibility that a plaintiff in a civil suit could seek a court order for disclosure of communications data. For example, in the ongoing war between copyright owners and piratical fire-sharers, an order might be sought for disclosure of the identity of persons who had accessed a known delinquent web site. It would not take a particularly enterprising legal team to spot an opening which has been flagged up in notes to the Draft Bill. These are areas altogether not covered by the usual "terrorists and paedophiles"[349] justification for this Bill.

DESIDERATA: the Information Commissioner should be asked to provide draft guidelines as to when Communications Data can be viewed as Personal Data, and if necessary this should be explicitly cited in the Bill. Other than for this case, subclause (b) should be deleted.

On Notices.

Quotation from Draft Bill: 7(1) (b) *[A notice of the Secretary of State provided for by an order under section 1 must] specify the person to whom it is given.*

I respectfully suggest that this is not good enough. A person could be involved in the operation of more than one system or service. In fairness, then, he must be left in no doubt what is required of him, so the notice must also specify the telecommunication system or telecommunications service to which it applies. This need requires the specification to be precise, yet it must also be flexible enough that it will not be voided by a trivial change, such as upgrading one of the servers in a system, or rebranding a service from "SplootMail™" to "SplootMail Express™". I also note that specifying a system (including the apparatus comprised in it), even at a single point of time, is going to be a tedious and difficult process, not least because the exact configuration may be commercially confidential.

On Enforcement.

Quotation from Draft Bill: 8 (2) *That duty is enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.*

I am not wholly sure that a remedy grounded in 15th century notions of Equity would be my choice of foundation for building the 21st century surveillance state. Specifically (I refer only to England and Wales), as regards the basic requirement to obtain & retain data, this would require what I understand is termed a "mandatory injunction"—an injunction requiring (rather than forbidding) the performance of some specific act. Which is all very well if it is a clearly defined act, such as delivering up a document or (the old favourite) making safe an unsound dam, for which a deadline

---

[349] the threats that keep giving

can be set (or the "F" word[350] deployed) and performance proved to the satisfaction of the Court. It is likely to prove unworkable if the action ordered is something as complicated as "develop and implement a data retention system", whose adequacy the Court is unlikely to be able to assess, and for which as far as operation goes there is no deadline but rather a requirement for perpetual continuance.

Conversely, as regards the duties to avoid unauthorised processing or disclosure we would be thinking of the more common prohibitory injunction. However it is presumably not the intention to take out injunctions for every notice, but only after an infringement has been reported. In other words, there is no sanction in place against a first infringement.

DESIDERATUM: I hate to say this, but in order to have sanctions against a first infringement, consider making unauthorised disclosure, etc., criminal offences; alternatively enable the Information Commissioner, or some other independent authority, to impose penalties as for breaches of the Data Protection Act.

On Persons, and on Data as Property.

Quotation from Draft Bill: 28 *"person" includes an organisation and any association or combination of persons.*

Now, when Parliament uses a word, it means just what they choose it to mean—neither more nor less.

However, this sort of Humpty-Dumptyism runs risks of forgetting the subtleties of the word's new meaning in a number of ways: Parliament may forget (i) that the extended definition includes the natural meaning; (ii) that the extended definition is greater than the natural meaning; or (iii) that this extended definition conflicts with extensions in other statutes, or legal precedent. I believe the Draft Bill falls into all of these traps.

This extension of meaning interacts with a failure to deal with the nature of communications data as property. A strange sort of property, perhaps, more a liability than an asset, but it is stuff and somebody must own it. Logically the owner would, initially, be the telecommunications operator, who generates and retains it. However it is the nature of property to pass from one owner to another, sometimes in circumstances which the current owner cannot control. (This is not the same as the ownership of any equipment or media on which the data is stored, although it may cause confusion if the rights of the media owner to repossess their property come into conflict with the obligations of the owner of the data to preserve it).

Forgetting that the extended definition includes the natural, that is, that a telecommunications operator can be a natural person. Under Section 4, the operator must retain the data until the end of the period of 12 months, protecting it against destruction and disclosure. If the operator were unfortunately to die, he would be unable to retain the data and carry out the related obligations. It therefore appears that the Bill creates a statutory duty of not dying.

It is not clear what remedy the Secretary of State might seek against an operator who does, unfortunately, die. It seems inherently unlikely (although I am not a lawyer) that a Court would order the executors to have the body brought back to life. A Court might, perhaps, preemptively order an operator to adopt a healthy life style and avoid dangerous sports, but I digress. Companies, too, can die, by going into receivership, or they can be taken over or merged.

---

[350] "*forthwith*"

DESIDERATUM: provision should be made, perhaps in the notices, for the disposition of data in cases where the original operator is no longer capable of retaining or processing it. This may have to involve arranging for its deletion, as it may be technically difficult to make arrangements for any other person to process it. It would of course then escape the Secretary of State's power to "ensure".

Forgetting that the extended definition is greater than the natural meaning; for example that a company is a distinct legal entity from any of its employees (or shareholders, for that matter). Legal persons are good at owning stuff, and making contracts[351], but are really rubbish at writing SQL queries and mounting back-up tapes. They employ natural persons for things like that. There are some sections of the Draft Bill which hint at the distinction, but do not fully address it. This may, for instance, underlie the apparent redundancy of two subtly different duties: under Clause 3(b) "A telecommunications operator must protect the data against ... unauthorised or unlawful[352] retention, processing, access or disclosure"—presumably this includes employees acting on their own volition; while in Clause 5 (1) "A telecommunications operator must not disclose the data except in accordance with the provisions of Part 2" (etc.) presumably means the company acting corporately or the employees acting under proper instruction. However it would seem that a notice or injunction to "protect" could only require best efforts, not be an absolute protection against the action of unruly employees. Employees themselves would not seem to be under any legal sanctions for unauthorised disclosure, although no doubt the company could discipline, or in severe cases even dismiss, them, as provided by employment legislation.

Could an injunction on a company also be taken out on all such of its present and future employees who have physical access to the data? Would this be fair, as they can neither be explicitly named nor consulted? Alternatively can an injunction on a company make it *absolutely* liable for misdeeds of its employees? That hardly seems fair either.

DESIDERATUM: clarification on how duties of companies translate into duties of employees, and how it is envisaged this would be enforced. (This also relates to the section On Enforcement above.)

Forgetting that this extended definition conflicts with other extended senses. Specifically, that it diverges from the concept of a legal personality who could be enjoined in legal actions, such as the injunctions envisaged in 8(2). Natural persons would be fine, as would "organisations" so far as this means companies and similar bodies with a corporate personality. Beyond that it goes a bit pear-shaped. Even if your association is the sort that has members and officers, you cannot usefully take out a permanent injunction on officers *pro tem*, and taking out an injunction on the members at large, without even knowing their names, will at best leave you with an unenforceable piece of paper.

If you try to go even beyond formal unincorporated associations into the vagaries of what might constitute a "combination" of persons, such as those behind peer-to-peer networks like BitTorrent or Gnutella, it pretty much falls apart completely. These "combinations" only exist in the sense that the persons offer the use of apparatus to the system, the membership of the combination is shifting and undisclosed. The combinations cannot be enjoined at law as they have no corporate personality. The persons combined may well be shadowy and anonymous, possibly by design as such systems tend to be involved in communications on or beyond the edge of lawfulness.

---

[351] that's sort of why they exist

[352] surely this is tautologous: if it's authorised it cannot be unlawful, by Clause 8(3).

DESIDERATA: that the definition of "person" be limited to accepted notions of legal personality. That the Secretary of State desist from trying to nail fog to the wall.

August 2012

NAFN

1. I am responding to the call for evidence on behalf of NAFN Data & Intelligence Services (NAFN). My response supports the case for the inclusion of local authorities in the Communications Data Bill and explains the guardian and gatekeeper role provided by NAFN for local authorities applying for communications data.

2. I have copied this response to the Home Office (which has supported the creation of the NAFN SPoC service), the Interception of Communications Commissioner (who has reported to Parliament on the performance of NAFN in providing the SPoC role), the Local Government Association (LGA) and the Convention of Scottish Local Authorities. Key stakeholders including the Association of Chief Trading Standards Officers (England & Wales) and the Society of Chief Officers of Trading Standards in Scotland has been consulted in the preparation of this response and local authorities have supplied the examples used.

The case for including local authorities in the Communications Data Bill

3. The National Fraud Authority (NFA) has estimated that the cost of fraud to local authorities is £2.2 billion per year. They state that *"improved prevention and detection of fraud will assist in reducing the financial pressures on local authorities, protect front line services and instil public confidence".*

4. Local authorities acquire communications data lawfully for relevant statutory enforcement and use it effectively in the investigation and prosecution of a broad range of criminal offences including serious crime.

5. Local authorities make effective use of communications data to enforce numerous statutes and to identify criminals who persistently rip off consumers, cheat the taxpayer, deal in counterfeit goods, and prey on the elderly and vulnerable. In addition to welfare fraud investigations, trading standards teams make increasing use of communications data. Environmental health departments principally use this data to identify fly-tippers.
6. It is important to note that in many cases the police are unable or unwilling to investigate local authority cases. Failure to investigate these cases will undermine public confidence and send the wrong message to perpetrators and their victims. The power to acquire communications data is a cornerstone of local authority investigations. The impact of not having access to communications data would be that many serious crimes and criminals would be harder to detect and convict.

NAFN's Current Role and Performance

7. NAFN is an unincorporated, not for profit organisation created and managed by local authorities to provide specialist data and intelligence services including the RIPA Telecommunications Single Point of Contact (SPoC) service. NAFN is hosted by Tameside Metropolitan Borough Council and Brighton & Hove City Council.

8. Communications data is a key source of intelligence which can be obtained quickly. As the government looks to extend intelligence sharing between government agencies locally, regionally and nationally NAFN's communications data service will be instrumental as part of the local authority intelligence hub envisioned by the NFA.

9. Assurance that local authorities' acquisition and use of communications data is compliant with the law is provided by the requirement to separate the roles within the local authority. To that assurance NAFN

adds independence, expertise, effectiveness and adherence to national processes with full audit trails and checks by experienced team leaders and an additional Senior Responsible Officer.

10. NAFN provides a robust guardian and gatekeeper role which is independently verified by the Interception of Communications Commissioner. The assurance arrangements are stronger for local authorities than for other agencies. Local authorities accessing communications data using the NAFN also have the assurance of our independence and expertise.

11. The Freedom Act 2012 requires that local authorities present requests for communications data to a magistrate or Sheriff. Their decision will be based on the written evidence alone. The NAFN system ensures that the documentation is of the highest standard. Additionally, NAFN has proposed (for England & Wales) that the presentation of applications might be enhanced by centralisation. Her Majesty's Courts and Tribunals Service are considering the proposal which would, in our view, quickly build a high level of expertise which could be made available to magistrates considering applications not made via NAFN.

12. The Interception of Communications Commissioner's inspection team has inspected the NAFN service every six months and has reported to Parliament that the service is of an excellent standard*. Sir Paul Kennedy and his inspectors have encouraged local authorities to use the NAFN service and have commented positively on the support given to investigators. NAFN has found that local authorities quickly gain confidence in the service and extend the use of communications data to enforce statutes and regulations.
*(see IOCCO Report 2011; pages 38 – 45 relate to local authorities
http://www.intelligencecommissioners.com/docs/0496.pdf).

Supporting Information

13. I have included additional information as follows:

- **Appendix 1**: Statistical analysis of local authorities' use of communications data since January 2009.

- **Appendix 2**: Examples provided by local authorities showing how communications data has been used successfully to assist in the detection, investigation and prosecution of criminals engaged in organised crime.

- **APPENDIX 1: Local Authority use of RIPA powers to acquire communications data**

- The table below shows the number of requests made by local authorities under both the Regulation of Investigatory Powers Act 2000 and Social Security Fraud Act 2001 powers*.
-
- * - SSFA figures do not include local authority use of SSFA powers which were not dealt with by NAFN
- ** - The 2009 RIPA "via NAFN" figure excludes the January to May period as the NAFN service was not available until June
- *** - These figures are taken from the annual IoCCO reports

Period	RIPA total***	Via NAFN	Percentage via NAFN	SSFA via NAFN *	Total
Jan 2009 – Dec 2009	1756	91**	5%	1625*	3381
Jan 2010 – Dec 2010	1809	615	34%	1686*	3494
Jan 2011 – Dec 2011	2130	1491	70%	1445*	3575
Jan 2012 – 19th July	Not available	1241	N/A	911*	N/A

APPENDIX 2:

Examples of Local Authority Use of Communications Data

The examples below represent just a small selection of the type of offences where communications data has been used by local authorities. They show how access to this data is vital to support the investigation and successful prosecution of a wide range of criminal activity. Several examples demonstrate that had the local authority not had access to communications data the criminal would not have been brought to account.

1. Money Laundering

One example involves serious and organised crime committed against elderly and vulnerable people involving money laundering to a value of £700,000. Telephone analysis was vital in identifying the money launderer's connections to the conspirators. The perpetrators have been prosecuted and given prison sentences varying from 9-13 months.

Another example involves a large scale investigation into the theft of funds from the Rent Deposits Scheme at one member local authority. An employee of the authority and several other suspects were responsible for setting up a large number of fictitious landlords and stealing £150,000 from the local authority. Communications data identified suspects who used mobile phones to coordinate the withdrawal of funds from ten bank accounts.

2. Land Sales Scam

The scale of this fraud is estimated by the FSA to be around £15 million. The organisation under investigation attempted to cover their tracks by registering their company in Panama with bank accounts in Germany and the Isle of Man and outsourcing their sales team to Spain.

The company purchased a parcel of land which they subdivided into smaller development sites selling to members of the public for up to £20,000 per plot. In their literature and website it was claimed that the land has been 'earmarked for development' and as such would rise in value but this is not the case. Owing to the arrangement, location and size of the plots owners were unlikely to secure planning permission for development purposes. The company were making false claims as to the expected or guaranteed profit and the timeframe in which purchasers would see their investment mature.

Communications data obtained using RIPA provided evidence identifying company premises and connections to suspects corroborating information already held by the local authority.

3. Rogue Traders

The first example relates to a business which had stolen a large sum of money from a vulnerable person. Communications data supported further investigations in order to successfully identify the offender and other victims and witnesses to support a prosecution.
Further examples where the use of communications data assisted in successful prosecutions includes two cases involving vulnerable consumers who had been defrauded. In one case the offender received an 18 months concurrent custodial sentence for the two fraud counts and in the other case the offender was convicted on two counts of fraud and received a ten week prison sentence (suspended for 12 months), 100 hours community order and was required to pay compensation to the victim.

4. Trade Marks Act and Copyright, Designs and Patents Act.

This case involved offences in relation to the Trade Marks Act and acts of conspiracy. Communications data linked the defendants and confirmed the fraud leading to custodial sentences of 8 and 12 months custodial suspended for two years with £1500 costs.

5. Tenancy Fraud

This investigation related to a former agency worker based within a local authority housing department. The individual acquired 13 council properties following calls from care homes and relatives who advised that the former tenant was no longer at the property or had passed away. Subsequently details were altered on the councils system and the properties rented privately for personal gain.

Communications data assisted in linking the offender to landline phones at all of the council properties, provided a residential address, bank records and identified witnesses and other parties affected by the fraud.

6. Car Clocking Scam

This case involved the purchase of high mileage cars at vehicle auctions and the subsequent reduction of their odometer readings using bespoke mileage correction equipment. These vehicles were sold to unsuspecting private buyers together with altered MOT certificates and falsified service histories.

An array of names, addresses and telephone numbers were provided by the defendants in advertisements, auction records and sales invoices. Communications data enabled investigators to link both defendants to the purchase and sale of around 40 vehicles. The co-conspirators received 12 and 18 month prison sentences with the confiscation of assets to compensate fraud victims

In a similar case using communications data a defendant was prosecuted for offences under the Trade Descriptions Act 1968 and the Fraud Act 2006 for clocking, advertising, and supplying vehicles. The offender pleaded guilty to all charges and was given a 12 month Community Order and ordered to pay costs of £1500.

7. Benefit Fraud

There are numerous examples where communications data is used routinely to detect fraudulent claims. These include:

- Email subscriber checks identifying undeclared partners linked to a benefit claim address
- Subscriber and itemised billing identifying undeclared partners, relationships between landlords and tenants and undeclared employment
- Identifying alternative residential addresses for the claimant
- Establishing that a benefit claimant has undeclared property
- Redirection of mail or PO Box ownership
- Identification of bank accounts to assist in Proceeds of Crime Act financial investigations.

August 2012

the Newspaper Society

The Newspaper Society represents regional media companies which publish around 1100 local and regional newspaper titles, 1600 associated websites and hundreds of niche and ultra local publications. The local press is the UK's most popular print medium, read by 33 million people a week and 42 million unique users a month relying upon their local newspaper websites.

At the time of the passage of RIPA, the NS and other media organisations expressed concern about the breadth of the legislation, the potential threat to confidential journalistic sources which can be revealed by communications data and the lack of adequate safeguards against any potential misuse. We understand that attempts might well have been made by local authorities to trace the source of leaks and the confidential sources of local newspaper journalists.

The Draft Communications Data Bill poses the same concerns. We question whether adequate justification has been given for the new powers or their breadth and consider the safeguards inadequate.

In respect of specific media concerns, the draft Bill's wide definitions and scope would give far reaching powers to the relevant public authorities to grant themselves access (in many cases) to communications data, on a very wide range of grounds each capable very broad interpretation.

Such data could reveal confidential sources, including whistleblowers. The Home Office memorandum does not consider whether the draft bill conforms with Article 10 ECHR freedom of expression rights, including the protection of confidential sources. Nor is any explanation given for the absence of longstanding media/freedom of expression safeguards, such as court orders and hearings at which such applications can be contested and orders granted appealed, which are explicitly intended to protect confidential journalistic sources and material against unjustified access by the law enforcement agencies.

The minimum safeguards in all cases should be prior independent judicial scrutiny and approval, subject to fast track review. In cases where confidential journalistic material such as sources might revealed, irrespective of whether this was the purpose of the investigation or not, a court order granted by a Crown Court Judge should be required for access to such communications data, with the provisions and procedures at the very least mirroring the production order provisions applicable to confidential journalistic material, (including advance notification and contested hearings, plus appeals), under the Police and Criminal Evidence Act 1984.

August 2012

No2ID

1. This submission has been prepared by for NO2ID, a campaign group. NO2ID was founded in 2004 in response to the then government's attempt to introduce the compulsory registration and lifelong tracking of UK citizens by means of a centralised biometric database held by the Home Office. It has continued in existence because it quickly became apparent during our campaign that the National Identity Register was only one of a multiplicity of official schemes to monitor and manage the citizen using the new power of networked computing -- many of which are threats to individual privacy and liberty, We coined the term "the database state" to describe that fashion in administration.

2. NO2ID is a non-partisan organisation supported by people from all parts of the political spectrum. More than 30,000 individuals have registered their support. We are currently entirely funded by individual and collective donations and membership subscriptions.

3. We are neutral on most political questions. Our concern is the threat to privacy and liberty posed by mass surveillance, the collection, retention and collation of information that can be tied to individuals, whatever the ostensible or intended purpose. Information sharing or matching used to generate files on individuals without specific and reasonable cause and independent oversight is a special case of the broader problem.

4. We opposed the previous administration's plans for surveillance of communications data, which (though more vague) it is hard to distinguish from those in the Draft Bill. We oppose the Draft Bill in its entirety.

5. Our submission is in two parts. Part I deals with the broader context and the proposals as a whole. Part II briefly addresses the questions which the Joint Committee has asked in its public call for evidence. There are two numbering sequences to avoid confusion in Part 2. Part 1 uses sequential paragraph numbers. Part 2 presents answers to Committee questions numbered Q1 – Q25

6. Definitions In what follows:
"Draft Bill" refers to the Draft Communications Data Bill (Cm 8359) of June 2012.
"RIPA" refers to the Regulation of Investigatory Powers Act 2000 and orders made under it.

Part I: General considerations

7. Our submission is that the narrow context of the ostensible purpose of the legislation is insufficient. Broader effects should also be considered. What does it enable, how does it change the practical capacity to use surveillance powers? What legal and structural foundations are laid?

Existing problems with over-broad RIPA powers exacerbated
8. Cl.9(6) – which seeks to define "necessity" into the fact of exercise -- gives an extraordinarily broad range of purposes for which the powers may be exercised. It is hard to think of an official purpose, anything a government might want to do to its people, that is left out. (Though tracing lost children appears to have been.) If that were not enough they can be arbitrarily extended by order cl.9(7). This carries forward the presumption of RIPA that officials should always have a legal basis available.

9. It is a current objection to RIPA that powers are self-authorised by the bodies using them, in their own interests, with no external check. This is not changed by the Draft Bill. It is made worse - because a broad-based default "necessity" is vested in the system rather than limited to specified bodies in the exercise of their specific powers. And there is still no external check.

10. This problem should be addressed by limiting the list of grounds for use to those where there is broad agreement the powers are justified, rather than drawing up a catch-all list.

Easier surveillance means more surveillance

11. It is not necessarily a good thing to make investigative powers cheaper and simpler to use. That just ensures that they will be used more. We suggest the real constraint on the use of official powers is the convenience of users within a bureaucratic system, not moral or legal constraints nor actual utility. That they **are** used does not mean they are always necessary.

12. The scheme of the Draft Bill is to make surveillance easier and cheaper to use. That means it will be used more. It is not clear whether it is used too much already. Given that the current authorisation process is not independent, it may well be.

13. It is our contention that surveillance powers as significant as the capture of communications data **ought** to cause the investigating authorities some time and trouble to use, and that is a strong barrier to their being overused. An independent check on use by way of a system of judicial warrants would create the further barrier of having to make a substantive case.

Centralisation, automation

14. The scheme intends one central system, one means of access to all the multifarious information that it proposes to collect. This vests vast power in a single organisation. which would be the gatekeeper for **all** the numerous public authorities that may have use for the scheme. (Compare under RIPA: for all its faults, a dispersion of power to individual bodies who may only look at some things and are exposed to question if they attempt to look at others.) It also presents a single point of failure.

15. By automating access to the data concerned, the scheme removes a key practical check on the abuse of power—visibility. Currently, infrequently but significantly, ISPs and telcos can and do question RIPA requests, if they seem unreasonable or ill-posed. That check is removed. As (we can guess, though the details are obscure) the sanity checks involved in detailed human authorisation and human data-processing.

16. The scheme promises easier faster, less supervised access to communications data, reliant on a single powerful but largely hidden organisation to extract it – and vastly more of it…

Scope of surveillance greatly widened

17. The new power to define a Communications Service Provider and demand access to data on their service users is extremely broad, and potentially brings under direct mass surveillance whole areas of life that have hitherto not been watched. Anyone providing a communications service could be subject to rules that would not only make them open customer information to authorities, but collect customer information they've never before kept.

18. Unlike telcos and ISPs, hotels, companies and educational institutions with mailservers, intranets, and telephone systems for their own use, travel and courier services do not necessarily need detailed information on users provided they get paid. Operators of forums, mailing lists and bulletin boards often avoid keeping logs or don't know where they are. This is a huge extension from public telecommunications systems to all communications systems, on the face of the Draft Bill.

Misleading presentation

19. The draft Bill states "Communications data is very different from communications content". This contrives to be both untrue and misleading.

20. Untrue: The distinction is not obvious. It is very hard philosophically or technically to distinguish the wrapping of information from the information contained in it. An obvious example is in web browsing: how much of a url is merely communications data? If you know I looked at a particular page, then you don't need a copy of what I saw to reconstruct what I did see.

21. Misleading: Promoters of the scheme have made much of the idea that **only** communications data will be open to such routine inspection, not content – the implication being that somehow content is more intimate.

That is not true. A timeline of all your contacts and interests, phone calls, reading and browsing, purchases, financial worries, patterns of movement, of waking and sleeping, build a more complete picture of you than you ever explicitly write down for anyone, perhaps more complete than you have yourself – and opens that to interpretation in a way that the contextualised statements in an email exchange would not. I have no idea what I was reading online last Thursday lunchtime, or what a third party might believe it says about me.

Finding more uses

22. The scheme creates an infrastructure both legal and technical that lends itself to the extension of surveillance and to other approaches to surveillance. The 'filter' concept of searching for data within a mass of collected details from the general population lends itself not just to finding data on identified targets, but to fishing expeditions, to mapping networks of association (and therefore attributing guilt by association), and to ideas of pattern recognition that have been popular in intelligence circles for some time.

23. There are persistent ideas that data-mining can deliver intelligence through searching for repeated constellations of characteristics to which meaning can be attributed. This data-astrology conception was behind the US Total (later Terrorist) Awareness System of a decade ago, and has enjoyed a vogue in the attempt to predict young offenders in this country. Given a fully comprehensive data-set and the ready means of access to it, these ideas are likely to return, perhaps with the suggestion they are a 'free' additional benefit of a system that is already paid for.

24. We should not build a system that by its structure passes great power to one cluster of organisations. Nor should we create one that offers incentives and opportunities to expand surveillance further. Surveillance systems should be designed instead to be self-limiting.

Part II – Response to Committee's questions

Q1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

No. and it has given grounds for belief that the ostensible aims and actual purposes may differ. The Home Secretary introduces the Draft Bill saying "The purpose of this Bill, therefore, is to protect the public and bring offenders to justice by ensuring that communications data is available to the police and security and intelligence agencies in future **as it has been in the past**. [Our emphasis] Previous versions have also been sold on the basis that they are 'maintaining capacity'.

It is hard to describe this as anything but a barefaced lie, in the face of the radical alterations in scope and procedure contained in the Draft Bill. Data would not be available as it has been in the past. Much more data including new sorts and new sources, will be available, more easily, under different terms, and new surveillance capacities will be created. It is not unreasonable to suppose that what the Home Office hopes to achieve is not what it says it wants but what is provided in the Draft Bill: greater surveillance power, centralised in the Home Office and associated intelligence agencies, with scope for expansion.

Q2 Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

The case offered isn't really a case at all. We are invited to trust the authorities that what they want is what's needed. One does not wisely buy insurance on the basis of trusting the salesman. One needs to know what one is insuring against – and evaluation of any new threats is absent. No new threats have been identified, let alone adequately quantified. Adversion to cases that have already been dealt with under existing powers certainly doesn't convince.

A huge institutional change and a big sacrifice in liberties and privacy requires more than that. What's being offered is a 'solution' to a problem that we only have vague assurances even exists, but which has significant risks in itself.

Q3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?
See Part I for partial discussion

Q4. What lessons can be learnt from the approach of other countries to the collection of communications data?
There are many differences in countries' approaches, and discussion could fill a book. The clearest lesson to be drawn is that there are advanced countries that limit surveillance, and ones that permit it easily, and this produces no obvious causal difference in their ability to deal with crime. That in turn suggests the scheme is less "essential" than its proponents insist.

Q5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?
Yes. There is no reason why a court order issued to a communications service provider, with suitable compensation for its costs, should not serve the same purposes as those claimed for the scheme. If that won't do, then a clear explanation why not should be presented. "It would be inconvenient," (or words to that effect) won't do. It should be inconvenient to invade the privacy of members of the public.

Q6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?
The Bill is essentially an overlay on the Data Retention Regulations (DRR) and aims to be that overarching regulation (and to provide more by order). That is not desirable, precisely because of the function creep and infrastructural effects. The DRR exist primarily because the Home Office demanded the Data Retention Directive (see, e.g. '*UK urging e-mail data retention*' – BBC News Monday, 11 July, 2005). The directive was opposed by several EU member states, and is currently being reviewed. If the directive is reduced in scope, which remains a possibility, the Bill enables HMG to keep the full effects of the Directive in domestic law.

Q7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?
The question contains petitio principii. It suggests it is common ground that civil liberties are a limited quantitative entitlement and that there are (and it is fine for there to be) unnecessary restrictions on them that the authorities may legitimately use as bargaining chips. We do not accept that. If any of the provisions in the draft Bill are genuinely *essential* (though we argue that NONE of them are) then they clearly ought to be enacted regardless of other *essential* restrictions on liberty and privacy. IF there are other measures that interfere with privacy or liberty unnecessarily, then that is a problem in itself.

Q8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?
It is a mistake to limit such discussion to "communications service providers". Many of Britain's key export businesses are in knowledge sectors – financial services and markets, law, and technology being pre-eminent – where communications confidentiality and the privacy/anonymity of activities are paramount concerns. Quantity of communications data itself is potentially market-sensitive information, without the possibility that individual firms or their clients might be targeted. Any loss of trust in British e-commerce, would not only affect our leading providers of those services directly, but would retard the development of the web economy. If customers are less sure of privacy it may affect all internet businesses.

Q9. Is the estimated cost of £1.8bn over 10 years realistic?
In the absence of any technical detail, it is quite impossible to tell. It is even unclear whether this would be the cost borne by the exchequer directly or whether it includes any uncompensated costs to business that would reduce economic growth and/or tax receipts.

Forecasting internet costs is difficult. The rate of change of IT and communications is such that to purport to have a 10-year plan seems odd. Cisco Systems' 'Visual Networking Index' attempts to forecast internet traffic 5

years in advance and reckons on an annual compound traffic increase of 27% in Western Europe up to 2016. The same index shows internet growth over the last 10 years (since the dotcom bust) of 13,950%

Yet the Home Office's record in more straightforward areas of financial management, and forecasting does not inspire confidence. The budget for the National ID scheme –also shielded from critical examination, began for "entitlement cards" in 2002 at 1.3Bn, became 3.1Bn for the draft bill and was £5bn during the final passage of legislation. It remained mysteriously stable at around £5bn until abandonment 3 years later, even though the scheme underwent fundamental restructuring.

Is there any point to the Home Office giving costs estimate that cannot be challenged, and that because of the secret nature of the scheme, cannot be checked against actual performance?

Q10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?

Likewise it is impossible to tell. The Home Office needs to explain the benefits coherently and with real figures before they can be evaluated. One hopes that they are not secret too.

Q11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?
See Part I

Q12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?
The issue is less which public authorities, but to what purposes. We would want to see it limited to criminal investigation and emergency services, with separate provision for intelligence, and no administrative bodies having any such powers. Provided the purposes are radically limited then the public authorities concerned can be too. There is certainly no need for the Secretary of State to have such order making powers. If a new body needs the powers, provision can be debated and expressly made by parliament in primary legislation creating that body.

Q13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?
We have no opinion.

Q14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?
We regard the whole framework created by the Draft Bill, and that of RIPA before it as being overbroad, unchecked and arbitrary. We have no objection to communications data being used for national security intelligence, or for the investigation of actual crime, or in emergencies for the protection of people and property from immediate harm. But with the exception of emergency use we would expect a process requiring a warrant on reasonable suspicion of crime put before a judicial authority, or for national security purposes issued by a Secretary of State.

Q15. Is the proposed 12 month period for the retention of data too long or too short?
We have no opinion. Under a warrant-based selective system, specified data might be captured and held for the duration of the investigation.

Q16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

We regard it as nonsensical to describe these as safeguards, since all actors in the system necessarily have parallel incentives and a common culture. A properly designed system would leave no doubt as to Article 8 rights. There is a great danger of designing a system merely for formal human rights compliance – how much can the Home Office get away with? We hope that the parliament seeks to maximise liberty and privacy, and that our standards would be somewhat higher than the safety-valve of the ECHR,

Q17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?
As we have argued throughout. Yes. A warrant should always be required except in an emergency to prevent immediate harm to people or property.

Q18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?
Their remit is limited so that they effectively supervise only process, or in limited circumstances comment on it. Their powers do not therefore mitigate the problems with the proposed system. It should be noted that reports of the Interception of Communications Commissioner are subject to censorship before being laid before parliament.

Q19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?
No. The Draft Bill contains a vast scope for order-making powers. It is a traditional Whitehall trope that the affirmative resolution procedure is a parliamentary safeguard against untoward extension by secondary legislation. Members of the committee will know how rarely secondary legislation is withdrawn. We submit that nothing should be in secondary legislation that could practicably be on the face of the Bill, and subject to debate and amendment in parliament.

Q20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?
We have no opinion. We would rather CSPs resist all requirements, save a proper court order for specified data.

Q21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?
The penalties are meaningless without a realistic chance of being caught. And the offences themselves are inevitably rather difficult to prove. The better approach is to set up a system in which there are third party gatekeepers who have incentives not to provide data unless they can verify the validity of the request.

Q22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?
We have no opinion.

Q23. How safely can communications data be stored?
If 'safely' refers to security against unauthorised access, it is at first sight completely contradictory to suppose it can be stored safely AND made available in a standardised format for ad hoc direct access.

Q24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?
No. What they are supposed to do is far from clear, and the technical feasibility depends on what exactly they are supposed to do.

The term "filtering" is misleading, and calculated to suggest reduction of access to data, whereas in fact it is plainly conceived as described as a means of facilitating it. There are objections of principle concerning the use of a rule-based system to decide who may access what data, and further ones concerning the conception of "filtering" which term appears to represent something more like a search engine – what would more commonly be called data-mining.

It is extremely dubious that they are appropriate – or even rational. The scheme implies that an algorithmic system (that cannot be legally questioned and gives no reasons for its decisions) can make judgements about arbitrary data in accordance with the Human Rights Act, and implicitly sanction the actions of an interested human investigator. Such investigators will inevitably learn to tune their responses to maximise the yield of what they want from the system, even when acting properly and in good faith.

Q25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?
It will clearly be extremely easy for those with actual discretion: for the Home Office, police and intelligence services to exceed their powers, and for authorising officers to use them improperly. Abuse by staff at lower levels (whether for personal, criminal or espionage purposes) will depend entirely on the organisational procedures and controls that prevent or detect such techniques as (say) issuing a false request, or (say) deliberately mis-stating a request in process. Opportunities for abuse also lie within the providers of software or hardware for the scheme, and with data management staff at individual CSPs.

There may on the other hand be very simple techniques available for those who wish to communicate clandestinely that would be difficult to block or trace. Coded unencrypted messages exchanged by posting on open forums and comment systems is one obvious method. There will be dozens of others.

Q26. Are there concerns about the consequences of decryption?
If there is any intention by the promoters of this scheme generally to crack or falsify basic web services routed through Britain (which seems to be hinted at, but not clearly communicated) then that could have significant effects on the confidence in the web economy and provide new opportunities for cyber-attackers.

August 2012

Zoe O'Connell

Qualifications

1. I have worked in the service provider industry continuously since graduating from Brunel University with a degree in Computer Science in 2000 and have maintained an interest in digital policy since that time, starting with the passage of the Regulation of Investigatory Powers Act. I am also qualified as Cisco Certified Internetwork Expert (#8174), a top-level qualification in the networking industry.

2. I currently work for a medium-sized AIM-listed managed service provider in South East England, where my role as the senior networking professional includes dealing with requests under the existing Regulation of Powers Act. In that capacity, I was also involved as a witness in what I believe to be the first conviction for "inciting terrorist murder via the internet". (R v Tsouli, Mughal & Al-Daour, 2007)

3. I am also author of the blog "Complicity". All answers in this submission are my personal opinion.

QUESTION 1: Has the Home Office made it clear what it hopes to achieve through the draft Bill?

4. Considering the draft bill itself, there is no apparent restriction on the powers that are granted by it, which does not give any way of assessing exactly what the intentions are. The powers could be used for deployment of "black boxes" en mass throughout the UK, could be used to just to target known hotspots, or could just be used to attempt to intercept information to and from non-cooperative web site owners. They may even be no deployment of interception, with the bill just being used to retain. additional information.

5. In it's publicity surrounding the bill, the Home Office (HO) stated legislation was needed because "*New communications technologies are generating communications data in different ways and communications data is* ***no longer always retained*** *by communications service providers."* (Emphasis added) In oral evidence to the committee, Charles Farr and Richard Alcock also concentrated on the "data retention" aspect of the bill as being primary, rather than obtaining data via interception. (This is discussed further in answer to question 2)

6. It would therefore seem that the HO are publicly trying to state that the bill is about retention. However, the powers being asked for include obtaining data via interception, and the use of these powers has not been made clear or publicly discussed in any detail by the HO.

7. The Home Office (HO) has also stated that it has spoken to a number of service providers who do understand their aims here. However, it is certainly not clear to myself or to anyone else I have spoken to in the industry what the aims are. It may be that those who have been spoken to are not themselves technical, but instead managers in effect bidding for a slice of the £1.8bn on offer. As a result, without knowing who the HO have been communicating with, one should be wary of accepting assurance that the concerned service providers are happy (technically or otherwise) with the HO proposals. Even if the HO genuinely believes the assurances given to it by service providers, the assurances it has received may not be entirely have been made in good faith and from a disinterested position.

8. Multiple Freedom of Information requests have been made to the Home Office on the topic of who they have spoken to, both for the draft bill and existing data retention regimes, and also enquiring as how they arrived at the costs stated. All have been entirely or mostly refused[353], so there is no clarification available via that route as to either the value of any assurances apparently given by service providers or the aspirations of the bill in general.

---

353 http://www.whatdotheyknow.com/request/external_organisations_consulted
,http://www.whatdotheyknow.com/request/data_retention_ec_directive_regu_3
http://www.whatdotheyknow.com/request/reimbursements_to_csps_for_data
,http://www.whatdotheyknow.com/request/payments_under_regulation_of_inv
http://www.whatdotheyknow.com/request/internet_monitoring_systems

9. Other potentially useful information on the bill has also been suppressed by the HO. For example, they attended a conference run by the London Internet Exchange (LINX) and presented a half hour slot to Internet Service Providers (ISPs) on the bill. The conference attendees were not security cleared and include foreign nationals, but despite this the HO refused permission to allow LINX to release the video for download to members who were not present at the meeting and additionally stated that they would never disclose who in the industry they had talked top in order to stop people simply switching ISPs.

10. The above facts combined - overly broad content in the bill, concentration on "data retention" in evidence to the committee, refusal to answer Freedom of Information requests and limiting circulation of information would suggest that the HO simply does not want more than vague details of it's aims to be public knowledge for security reasons. That approach makes any useful, democratic assessment of their request a practical impossibility and also seriously damages any prospect of meaningful oversight.

QUESTION 2: Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

11. In evidence given orally to the committee by Charles Farr, Director General of the Office for Security and Counter-Terrorism, states that much of the current problem is down to "ambiguity" in the Data Retention Directive (Q7) and also goes on (Q9) to state that he believes the draft bill will increase the proportion of successful requests for data from 75% to 85%. This concentration on data retention (Versus data acquisition) is further reiterated, including in a response to Question 74 by Richard Alcock (Director of Communications Capability Directorate) in his answer to Q74, who states that the costs are around data retention.

12. What is not addressed is why simply updating the UK implementation of the data retention directive would not be sufficient to achieve the stated 10% uplift if this is simply a data retention issue.

13. There is mention in the same session of cooperating with European, not UK, providers in retaining this data and that differences in the implementation of the Data Retention Directive (DRD) across Europe were part of the problem. It is not explained how a bill passed in the United Kingdom could be used to require European providers to retain data: Either the providers somehow fall under UK law by virtue of doing business here (In which case they would be subject to a UK "clarification" or update of the Data Retention Regulations 2009) or they are not subject to UK law, in which case any agreement with them would not be influenced by new legislation.

14. Although effort has been made to justify retention of additional data, no serious attempt appears to have been made by the Home Office for additional powers of interception and obtaining additional data.

QUESTION 3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

And:

QUESTION 4. What lessons can be learnt from the approach of other countries to the collection of communications data?

15. Based on an analysis of data released by Google[354], the UK has per capita the population most investigated via data communications in the world. Other countries may engage in snooping directly on their citizens, rather than requesting data from countries such as Google, but the UK would be unique amongst western democracies should it engage in such practices and this would largely be uncharted territory.

---

354 http://www.complicity.co.uk/blog/2012/06/google-data-shows-uk-back-as-most-snooped-on-population/

QUESTION 5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

16. As discussed previously, updating the Data Retention (EC Directive) Regulations 2009 to cover more data should be considered. However, the HO have been reluctant to release enough information on what they hope to achieve which makes proper consideration of any alternatives difficult.

QUESTION 6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

17. It would appear that, as written, the bill would supersede the Data Retention Regulations in all respects. There would appear to be no circumstances under which it would be worthwhile for the Secretary of State to issue further notices to service providers under section 10 of the regulations should the bill be passed. As a result, the regulations would cease to have any real world effect once all current providers are notified of their new obligations under the proposed bill.

QUESTION 7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

18. The draft bill gives the potential for near-total omniscience to the state within the communications world. Given that people's lives are increasingly integrated with electronic devices and the Internet, the scale of any scrapping of existing powers outside of the bill itself to rebalance liberties would have to be staggering in it's scope.

QUESTION 9. Is the estimated cost of £1.8bn over 10 years realistic?

19. Despite multiple Freedom of Information requests, as noted in the answer to Question 1, the HO has yet to produce any breakdown of it's costs beyond simply stating around half the cost is retention. As it has also not been made clear what the aims and objectives of the bill is, it is not possible to determine if this is realistic.

QUESTION 10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5□6bn. Is this figure realistic?

20. The HO have not released any breakdown of this benefit, so it is hard to analyse. It would appear some of these benefits, based on evidence given orally by Charles Farr, is based on notional values of human life etc, for which we do not have numbers.

21. However, a basic sanity check can be performed. There were 414,400 successful requests in 2010 (75% of 552,550) and the HO have stated in oral evidence to the committee that they hope for a 10% increase in successful requests as a result of the bill, meaning an additional 55,255 requests. This would mean that the current Data Retention regime is delivering a value of £3.75bn per year, or £9k per request. That number seems large and I would have expected to see more publicity surrounding the benefits of the existing system, but is a feasible figure given that the HO aims to *"prevent revenue loss through tax fraud and facilitating the seizure of criminal assets"*.

QUESTION 13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

22. The UK would appear to have no legal recourse against foreign service providers who do not, entirely voluntarily, comply with the proposed bill. If the HO did attempt to find a way to pursue foreign service providers with no UK base, this would set a very unwelcome precedent. UK service providers may then have the burden of complying with laws and regulations in every other country connected to the Internet, in case a user from that country visits their site.

QUESTION 16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How

should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

And

QUESTION 17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

23. Independent oversight of requests is certainly desirable, but a "warrant" could be granted by the Secretary of State or their nominated representative, which lacks sufficient independence. It would be more appropriate to specify that a judicial warrant is required.

24. The main objection to requiring warrants by the HO has been time, in critical cases, and cost. On the topic of time, there is no reason why the vast majority of non-time-critical (Priority Grade 3, under the current RIPA system) should not require warrants. Such a system must mandate retrospective judicial approval of any high priority (Grade 1) requests to prevent abuse, with automatic reporting of any failed retrospective requests and investigation by the commissioner. The commissioner has already identified "serious non-compliance
" by a number police forces under the current oral approval system[355] which is a major cause for concern if not addressed.

25. For cost, the overall cost of the proposed system amounts to £3,257 per successful request[356]. The cost of applying for a warrant does not appear to constitute a major additional burden in light of this.

QUESTION 18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

26. The roles in theory are welcome, but the commissioners have proven themselves to be relatively toothless and do not properly investigate problems. A much stronger system of oversight is required.

QUESTION 19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

27. As noted previously the HO have been extremely reluctant to provide any information to the committee in evidence to support the bill. There is no reason at this stage to believe they would be any more cooperative when it comes to future oversight. The draft bill should enforce tough, thorough and public reporting by the HO and all organisations granted powers or obligations under the bill.

28. It is notable that the proposed system of interception involves the secretary of state mandating the equipment and configuration to be used by service providers, meaning it is unlikely that service providers will have any meaningful insight into the operation of the system. This will mean that the only organisations who really know what is going on are the HO and the (So far unidentified) suppliers of the equipment. This potentially means that no independent oversight of the technical implementation of the bill will exist at any level.

QUESTION 21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

29. It should be a criminal offence to wilfully disregard any communications data provisions, to prevent managers and staff refusing to take responsibility for the significant powers granted to them, in a similar

355 2011 Annual Report of the Interception of Communications Commissioner
, Page 35
356 http://www.complicity.co.uk/blog/2012/07/comparative-costs-of-ccdp-requests/

way to the driver of a vehicle - and not his employer - being liable for offences committed behind the wheel. However, history has shown that prosecutions for such offences rarely take place as they are deemed not to in the public interest and this is as critical a problem as the penalties themselves. Mandating investigation by the commissioner with a strong presumption of prosecution on behalf of the CPS would go some way to solving this issue.

QUESTION 22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

30. On the scale required by the HO, no. No evidence has been presented by the HO to suggest otherwise, or how they would handle non-standard and ever-evolving protocols used by many sites.

31. As an example, in the 2010 film "Four Lions", the jihadists converse over a web site that appears to be based on Disney's "Club Penguin", an online game for children. The protocol used for communication between such sites and the client software running on the users computer will be completely proprietary and change entirely at the whim of the developers.

QUESTION 23. How safely can communications data be stored?

32. Security is a trade-off between usability and accessibility of the data versus it's value and the impact if it is compromised. The value of the data held by Service Providers will be huge, representing a valuable asset in corporate espionage potentially funded by foreign governments.

33. Such a high-value asset needs to be protected very robustly and although service providers generally have a good track record in keeping critical data secure, breaches do happen. This is a significant risk, the impact of which should be properly and fully investigated and reported on by the HO and accepted as being necessary prior to the bill being passed.

QUESTION 25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?

34. It would seem to be trivial to circumvent, unless the HO has some mechanism of decrypting all traffic that is not known to the rest of the world. (See discussion in answer to Q26 for more on this)

35. The government of China, which has thrown significant resources at it's "Great Firewall of China" project, has been trying to simply block - not even intercept - unapproved internet sites. Despite this, it remains the case today that people are able to bypass this system using technologies such as "tor". There is no reason to believe the HO would be significantly more successful at interception than other governments would be at the simpler task of blocking.

QUESTION 26. Are there concerns about the consequences of decryption?

36. Potentially, yes, as we do not know how the HO intends to break decryption other than a simple statement that they can. There is a real danger that "man-in-the-middle" attacks on encryption might expose UK users to additional security risks or generally destabilise the internet in unwelcome ways[357]. To avoid security and stability problems created by interception, it should be a requirement of the bill that interception may only be passive and not alter the contents of the communication in transit.

37. Worse, in a nightmare scenario, whatever technology is deployed at the service provider level by the HO to decrypt traffic is stolen from a data centre by criminals or members of foreign intelligence agencies, potentially exposing very large number of users to security risks and huge financial implications.

August 2012

---

357 http://www.complicity.co.uk/blog/2012/06/spooks-in-the-middle/

Open Rights Group

Introduction

1. We believe the powers contained in the draft Communications Data Bill are too broad and will result in a generalised surveillance of the population. Law enforcement access to communications data for specific purposes is not wrong in principle. But we do not believe the generalised collection of communications data about the population by the government and law enforcement bodies is acceptable in a liberal democracy.

2. Where incursions into the public's private lives are proposed, and justified with reference to competing rights such as security, the benefits case must be made openly and trade-offs must be established via a clear and robust democratic process. We are concerned the Joint Committee is being asked to make recommendations based on incomplete or inaccurate information.

3. In this submission we argue that there has not been sufficient opportunity for the public or Parliamentarians to properly scrutinise the proposals. We set out concerns about the scope of the information likely to be collected and the safeguards governing access to it. Quite clearly this Bill amounts to more than a proposal to maintain existing powers. Too much information will be collected about too many people.

4. We argue that 'new' kinds of communications data, from social media for example, are simply not comparable to phone record data. They can be far more intrusive and revealing and, of course, far more useful. This is especially so when data is combined to create a broader picture of an individual's movements, personality and social circles. So we refute the suggestion that communications data does not somehow convey substantive content about a person's life. We believe that the term 'communications data' is being stretched to breaking point, and can not adequately contain the variously intrusive and revealing types of data now potentially available to law enforcement. It has reached its limit as the useful basis for a single regime of information storage and access.

5. We set out why we believe the proposed safeguards around access to communications data are too weak, which will result in both the accidental and deliberate misuse of the data leading to significant privacy harms. That will likely include risks to journalists and their sources, the undermining of legal privilege and a chilling effect on whistleblowers. We also note how information provided by the Interception of Communications Commissioner about the error rate in RIPA requests seems to be based on a flawed reporting process, and there is insufficient data to make informed, independent analysis of the regime.

6. We recommend the current draft Bill is rejected. We suggest there are alternatives to these proposals that would involve less intrusive and harmful powers but which have seemingly not been considered, for example a form of properly managed directed (rather than general) collection, with court approval for access, in cases where suspicion exists. We suggest a more detailed, and public, consideration of the various types of information potentially available to law enforcement, how useful and intrusive that information may be, and what collection, storage and access regimes are appropriate.

7. We include in our submission a legal opinion from Eric Metcalfe of Monckton Chambers, former director of JUSTICE, in which he considers the consistency of the draft Communications Bill with human rights law. He concludes that the Bill is incompatible with the UK's obligations under Article 8 of the European Convention on Human Rights. The full opinion is attached to this submission. We also include in Annex B evidence from Public Concern at Work, detailing case studies of recent threats to whistleblowers.

Summary of key points

- We recommend that the draft Bill as it is written is rejected. The powers to order the collection and storage of information are too broad, and the safeguards over access are too weak.

- The Government has not run an adequate policy making process. The proposals seem built to *withstand* public scrutiny and debate rather than be subject to and improved by it. There has been no consultation and they have not provided sufficient detail regarding how the powers will work in practice, nor the associated costs and benefits. We recommend a full review of, and consultation on, communications data collection and access.
- The powers amount to a general surveillance of the population. We recommend an analysis of how a properly regulated regime of targeted collection would be more appropriate.
- Drawing on the attached legal opinion, we consider the proposals to be incompatible with the UK's obligations under Article 8 of the European Convention on Human Rights.
- We recommend court approval for all access to communications data.
- We recommend a system of notification for people whose data is accessed.

Issues with the policy making process

8. We welcome the scrutiny that the Joint Committee has given the draft Bill thus far. We also believe that the lack of a full public consultation and the paucity of detail available to the public and the Committee have undermined the policy making process and led to an inadequate public debate.

9. The government have not 'built in' to this process an opportunity for a democratic debate about a broader range of options for addressing the 'capabilities gap' identified by the Home Office.

10. The proposals and the process that led to their creation appear to have been built to avoid and withstand public scrutiny, rather than to be subjected to and improved by it.

The lack of detail

11. Part 1 of the Bill sets out extremely broad powers. As a result, it has been difficult to establish with any clarity how collection and storage of information will work in practice.

12. For example, there is no detail on what the orders may look like. On 9th July both Rt Hon Simon Hughes MP and Dr Julian Huppert MP asked for more detail on the orders that may be written under the powers of the Bill358. It is fair to say the answers were not comprehensive:

> **Simon Hughes:** I am grateful to the Minister for his answer. He will know that the draft Bill, particularly in clause 1, gives very wide powers to the Secretary of State by order. Will he tell us whether the Secretary of State has yet written those orders? In any event, will he give the undertaking that they will be published at the earliest available date?
>
> **James Brokenshire:** It is worth underlining that communications data are an essential tool in solving and prosecuting crime. It is important that that is not eroded by changing technologies, which is why we need the flexibility to respond to change. We are working closely with the Joint Committee. We are absolutely committed to the pre-legislative scrutiny and to ensuring that the Committee can conduct robust scrutiny of the Bill.
>
> **Dr Julian Huppert (Cambridge) (LD):** The Minister said that he was working with the Joint Committee on which I serve. He will be aware that the Joint Committee has not been given sight of the order. Will he promise that we will have a chance to see it while we are carrying out the pre-legislative scrutiny?

---

358 http://www.publications.parliament.uk/pa/cm201213/cmhansrd/cm120709/debtext/120709-0001.htm#1207099000621

> **James Brokenshire:** As my hon. Friend will know, scrutiny of the draft legislation is only just starting. I understand that the first sitting of the Joint Committee is due to take place this week. Officials from the Department will consider this matter and give evidence to the Committee. I will commit to keeping the issue under review as the legislative process develops, because we recognise the need to ensure that the Bill and the scrutiny that we will respond to are effective. We need to recognise that this is an important matter in ensuring that crimes continue to be prosecuted.

13. We are not aware of the Joint Committee receiving further detail along these lines, nor are we aware of the Home Office releasing such details publicly. As a result, it is difficult to examine in great detail exactly what the Home Office have in mind.

14. One consequence of this is that the Home Office has focused simply on whether communications data is useful in principle, or whether using communications data to solve crime is a good idea. Communications data is obviously extremely powerful and useful data. The important debate is about the types of information potentially available, the means of collecting and storing it, the relative levels of intrusiveness and usefulness and the suitable regimes for access to it. The decision making process focused on that should take place through democratic fora involving a public consultation.

15. These proposals have been presented as *the* possible option for addressing the issue of access to new types of 'communications data'. In her introduction to the draft Bill, the Home Secretary begins by telling a story of the capability gap and why closing it is vital to maintaining the ability of law enforcement to deal with serious crime. However, absent from the introduction is a consideration of what information is and is not available, to whom, the power of that information and any possible harms that may come about from the misuse of it. Focusing on the in principle, top level benefits of communications data without a consideration of these further issues can only lead to a one-sided debate.

16. The options presented in the Impact Assessment offer a further example of this issue, presenting a simple binary choice between 'doing nothing' and the Bill as written. This suggests either that there is only one way to address the capability gap, or that the Home Office has not considered alternatives.

17. The Privacy Impact Assessment does not offer much more detail, nor does it give a full consideration of the privacy issues. It is largely a description of some of the privacy risks and a statement that the safeguards are adequate, with no real analysis or explanation.

Lack of a public consultation

18. We regret that there has been no public consultation for this draft Bill. Whilst the Joint Committee have kindly called for written evidence, we are now significantly 'downstream' in the policy making process.

19. There was a consultation run by the previous Government on what is in its practical effects and implications the same proposal. Following this, and significant opposition to the ideas, the proposals were dropped before a draft Bill was published.

20. The current proposals may be argued to be substantially different from those developed by previous government, in which case they should be subject to a consultation. Or the proposals may be very similar, in which case there should be an explanation about why the Home Office has now drawn a different conclusion from the responses to the previous consultation. The Government appears to see this as a different proposal from the one put forward by the previous government. For example, Foreign Secretary Hague stated in Parliament:

> *"It differs enormously, because the previous Government's proposal was to hold all data in a central database. Our proposal would require providers to hold on to their data."*359

21. First, this is to downplay the functionality of a distributed database across services providers done to a design specified by GCHQ, which will in practice be no less insecure or intrusive than a centralised store. Second, as Privacy international and others have noted360, the previous Government dropped proposals for a central database. Furthermore, Section 20 appears to allow for the creation of centralised services. So this is not a point of differentiation.

22. In the recent Demos report "#Intelligence", the authors (former director of GCHQ Sir David Omand, Jamie Bartlett and Carl Miller) make a similar point - that the regulation of the use of social media information (which they term 'SOCMINT') requires a more fundamental debate about what is appropriate:

> *The Government should publish a green paper as soon as possible on how it plans to manage over the next few years the opportunities offered by social media analysis and the moral and legal hazards that the generation and use of SOCMINT raises. This needs to include definition of the potential harms that SOCMINT pose, how harm can be judged and measured, and how these risks can be balanced and managed. It is important that the Government provides a position on the practicalities and specifics involved, including information on the relationship between the Government, ISPs and social network providers, the scope of information collected, the bodies authorised to collect it, who will have access to certain capabilities and with what safeguards.*361

23. The paper discusses the differences between private and public social media information. It can be seen as a broad argument that any changes in the types of data gathered and used for intelligence purposes must be accompanied by a wide public consultation, because of the different levels of intrusion that new types of communications data bring. In skipping to a draft Bill that focuses on the highly intrusive matter of communications data in such limited detail, albeit with the scrutiny of the Joint Committee, the government is short circuiting that broader public debate. We are also concerned that this places the Joint Committee in an extremely difficult position.

24. We believe that ahead of a draft Bill, the Home Office should have produced a Green Paper to allow for a full public debate, about acceptable surveillance in the contemporary information society, through a more open democratic process.

Unanswered questions

25. A number of questions remain unanswered due to the lack of detail published about the draft Bill. For example:

- To what extent will any "black boxes" be used to collect information? Even though the law specifies only communications data, will the black boxes not be able to routinely gather content as well? If not, how will they work?

---

359 http://www.theyworkforyou.com/debate/?id=2012-06-20a.863.1

360 https://www.privacyinternational.org/blog/the-draft-communications-bill-is-a-wasted-opportunity

361 Page 69, http://demos.co.uk/files/_Intelligence_-_web.pdf?1335197327

24. How many services genuinely will not co-operate? Where are they located? The government may attempt to impose collection or access duties on companies located overseas. There are legal arrangements for such access, so the government should consider what sort of changes might resolve this issue. Furthermore, it is unclear to what extent such duties can be imposed by the UK or in what circumstances.

    This is a wider legal question than just those relating to communications data. Is there evidence that international legal agreements are not functioning? Has such an analysis been undertaken?

    Twitter is an example that does not seem to support the Home Office's case. Twitter already hands over data following an appropriate legal request, including to UK police362. 11 user information requests were issued between 1st January 2012 and 30th June 2012. Only 18% of these were complied with363. Rejections may arise from the requesting authority failing to identify a Twitter account, requests that are overly broad, or where users challenge requests after being notified. US court orders can be obtained by UK police, at which point the data is handed over. It would be useful to examine why the success rate for these requests is 18%.

    Google operates via a different model. They do not require court orders but largely comply with local standards, publishing a transparency report of their handling of request. The transparency report reveals they complied with 64% of requests for user data from the UK Government. Would the discretion that saw 36% of requests refused disappear under these proposals? The current model, which lacks a legal process in the handing over of user data, is not ideal. But we are concerned that the draft Bill proposes to replace this not with a court process but a model of self-certification by requesting law enforcement bodies with no meaningful judicial oversight.364

25. Frequently, data is retained on devices as well as companies, and can also be accessed that way. To what extent would this address the capability shortfall?

26. How will encrypted data be treated? Does the effectiveness of the proposals depend on breaking the encryption on which we routinely depend for online transactions, including banking and e-commerce? If so is that a net gain or a net loss to business confidence and to security in the UK?

Costs and benefits

26. Hardly any information on the costs or benefits has been published. We have been provided with ball park figures with no justification made public. In the Impact Assessment accompanying the Bill, the details of the costs and benefits are listed as 'optional'. The Home Office's Office for Security and Counter Terrorism has rejected our requests under the Freedom of Information Act for any useful level of data about the costs and benefits analysis. On 23rd July we asked them to supply us with the "summary of workings made to create that estimate, as used to create the figure used in the Impact Assessment, giving breakdowns for the savings categories mentioned above." In reply, the OSCT turned down the request. In their explanation of the public interest test, they set out the following justification:

---

362 *Treaty between the Government of Bermuda and the Government of the United States of America relating to Mutual Legal Assistance in Criminal Matters* (http://www.official-documents.gov.uk/document/cm76/7613/7613.pdf)

363 https://support.twitter.com/articles/20170002#

364 See http://www.google.com/transparencyreport/userdatarequests/GB/?p=2011-12

"Sensitive operational benefits expected as a result of the draft Communications Data Bill would prevent the publication of the information requested. We consider that release of this information would aid individuals and/or groups seeking to plan or carry out an attack or commit a crime.

The information withheld includes who we have worked with which would highlight operational capability issues. Disclosure of these details would limit the effectiveness of the law enforcement agencies to prevent and detect crime.

The information which relates to UK capabilities is considered to pose an unacceptable risk to the ability of the UK to safeguard national security; the disclosure of this information could be used to avoid detection.

We have determined that safeguarding national security interests and law enforcement is of paramount importance and that in all circumstances of the case it is our opinion that the public interest clearly favours the non-disclosure of information covered by section 31(1)(a)."

27. We have requested an internal review of this decision. On June 21st, we asked the Home Office the following, again under the Freedom of Information Act for "the likely costs or estimates of costs for the programmes of collection and storage of communications data expected to be created under the Communications Data Bill, and analysis made by or for the Home Office of the available technologies to fulfil the new programmes of collection and storage of communications data under the same Bill". In reply, we were told that the request was being rejected on costs grounds. We are working to narrow the request.

28. We are particularly concerned that the withholding of information on the basis of national security is inhibiting a legitimate debate, by the public or Parliamentarians about the detail of this draft Bill. While this approach may be reasonable for certain specific details and issues, it is not appropriate for general obligations imposed on companies that involve data collection potentially affecting every citizen, innocent or not. It again makes understanding the proportionality of the proposal very difficult.

29. There are two key issues to consider when judging whether the current process is a sufficient mechanism for scrutinising the proposals. First, have the public been provided with enough information and detail to enable a proper public debate about the proposals? Second, is the Joint Committee being supplied with the required information by the Home Office and relevant bodies to make a proper and informed judgement?

30. Taken together, the answer to these questions determine whether the scrutiny process constitutes the requisite level of public deliberation about the use of the Bill's proposed powers and associated technologies.

31. The Joint Committee's findings are likely to be taken by the Government as a conclusive judgement on the acceptability of the proposals. It is one thing to withhold potentially sensitive information from the public. It is another to withhold it from the Committee set up to scrutinise the proposals in Parliament.

32. With reference in particular to the lack of a full consultation, the paucity of information concerning the details of the Bill and the rejection of Freedom of Information requests, we would argue that this has been an insufficient process of scrutiny and public debate.

Privacy and consent

33. It has been argued that people care less about privacy now, evidenced by the proliferation of social networks on which people share all manner of personal details. Building on this, some may argue either that the Government should be able to benefit from this information to the same extent that Tesco or Facebook can, or that people will not mind if the Government shares in the usefulness of this trove of data. In his evidence to the Joint Committee, for example, Professor Anthony Glees made a similar point:

> *"...there is a philosophical point here, where you have people putting all sorts of intimate details about themselves quite freely on to the internet. What is private and what is public no longer means what it meant when I was a student 40 years ago. One does have to have that debate."*365

34. It hardly needs pointing out that people now share more of their everyday life than ever before, both voluntarily and involuntarily. This interest in sharing often personal details is enabled by technologies that give people new ways to connect with each other, carry out everyday tasks and organise their lives. Much of this change in behaviour is driven by a combination of our social instincts, consumer habits and the business models of many digital businesses. In return for sharing more information about ourselves, we often get something in return – whether it is cheaper goods, apparently 'free' online services or more fulfilling social lives.

35. The fact that people have taken to sharing more about themselves does not mean that the government can feel empowered to appropriate that information. It does not imply an automatic right or need for that information. Nor does it suggest a fundamental shift in attitudes towards a more general reckless or relaxed attitude towards privacy – certainly not to the extent that it would permit institutions to assume rights to access or use information. The use of information is based on an individual's context specific consent. People often lack knowledge or clarity of how information will be used or the terms of an agreement, with research demonstrating that people often make 'imperfect' decisions that do not fit with a perception of perfectly rational privacy decisions.366

36. The general direction of data protection legislation has been to address such issues through emphasising minimisation of data collection and requiring consent to be as clear and informed as possible. The proposals in the draft Communications Data Bill are heading in the exact opposite direction.

37. Sometimes people will not be able to make individual direct decisions about use of personal information. Access to communications data by public bodies would be one example. In those situations, law enforcement bodies exercise their authority through the use of personal information. To the extent that this is an intrusion into the private sphere, the rules governing this use need to be created through democratic, public debate.

The scope of information collection and access

38. The Home Office argues that the draft Bill is needed to maintain existing powers. This is not credible. The scope and nature of information collected make the proposals far more than a simple maintenance of existing capability.

39. The Home Office argue that they want to close the capability gap from 75% to 85% data availability. We argue that this must be placed in the context of the general orders-of-magnitude proliferation of data, personal and otherwise. In their report on 'big data' in 2011, McKinsey predicted a 40% growth in global data generated per year, arguing that "we are generating so much data today it is physically impossible to store it all"367. The

---

365 Uncorrected evidence, page 25 http://www.parliament.uk/documents/joint-committees/communications-data/uc170712ev4HC479iv.pdf

366 See for example "Does it help or hinder? Promotion of Innovation on the Internet and Citizens' Right To Privacy", Directorate General for Internal Policies, Policy Development: Economic and scientific policy, 2011 http://www.europarl.europa.eu/committees/fr/studiesdownload.html?languageDocument=EN&file=65871 and Ian Brown, "Privacy Attitudes, Incentives and Behaviours", 2011 at: http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1866299_code892424.pdf?abstractid=1866299

367 McKinsey Global Institute, Big data: The next frontier for innovation, competition, and productivity, 2011 available at

Home Office impact assessment for the draft Bill assumes that the 'total volume of internet traffic increases by a factor of ten over the 10 year period."

40. No doubt this poses challenges to law enforcement. But it is not accurate to say that the insights law enforcement may gain from available communications data has reduced, even if the percentage of the amount of data available has reduced. We question the notion of a capability gap couched in percentage terms, and see this as much a qualitative issue.

41. Data generated now is of a markedly different type to phone records and other traditional types of communications data. A record of a phone call tells an investigator who called whom, when, and where. Even this 'traditional' communications data is intrusive. The Article 29 Working Party of European data protection commissioners argued that the Data Retention Directive (Directive 2006/24/EC) involved "an inherently high risk level that requires appropriate technical and organisational security measures. This is due to the circumstance that availability of traffic data allows disclosing preferences, opinions, and attitudes and may interfere accordingly with the users' private lives and impact significantly on the confidentiality of communications and fundamental rights such as freedom of expression."368

42. The new kinds of 'communications data' the Bill is aimed at collecting can paint a more intimate picture of our lives. Details of social media communications reveals likely political opinions, lifestyle preferences, social circles, habits and patterns of behaviour. Although only the fact that a particular website was accessed, and not the specific page, is to be recorded, such information can still speak volumes. The fact that someone repeatedly contacted Narcotics Anonymous, or Gaydar, or a political website goes some way to indicate significant aspects of their identity or personality.

43. By combining email, telephone and web access data, and mobile phone location history, one can deduce a detailed picture of an individual's movements, habits and thoughts to a greater degree than phone records alone could offer.

44. Additionally, the same "heuristic" techniques used to identify spam e-mail could potentially be applied to large-enough bodies of communications meta-data to identify common patterns. Heuristics for spam say, for example: "these 100 messages are spam. Is this new message like them statistically". Consider a similar scenario: "these 100 messages related to a given political party. Is this message like them statistically"?

45. The distinction between 'content' and 'communications data' does not, in practice, easily hold. This is partially because of the difficulty of separating out content from 'communications data.'369, but also because the category 'communications data' does not adequately account for the variety of types of data, and the possible intrusiveness of it – which ranges from Oyster card user data to Facebook likes and comments, LinkedIn groups, Twitter Direct Messages and so on. Separating out content does not necessarily reduce the intrusiveness of data to the degree that blanket collection and weaker safeguards are acceptable or proportionate.

The move to general surveillance of the population

---

http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_innovation

368 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf page 1

369 For a discussion of this issue see "Briefing on the Interception Modernisation Programme", LSE, 2009, http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf

46. The government is giving itself extremely broad powers to order any communications provider to collect and disclose communications data. The government hasn't said how collection might work, even though the way the data is collected is critical.

47. The Committee has heard that this is most likely to involve collection duties on Communications Service Providers and 'black boxes' being installed on ISPs networks, which will harvest communications data that can then be access by relevant government bodies. This will involve organisations collecting information that they otherwise would not because it goes beyond their normal business needs. The proposals represent a fundamental shift to general, mass surveillance of the population.

48. The collection and storage of data is outsourced to the privacy sector, making CSPs the servants of the state rather then of their customers. It creates the liability for substantial payments by Government to service providers, introducing costs that may escalate and prove hard to control. This happens just at the time where elsewhere Government is making huge and to some extent successful efforts to bring HMG's out-of-control spending on IT and services back under control.

49. The result will be the creation of a distributed370 database of a wide range of information about everybody's communication.

Filters and data mining

50. The clauses on "filtering" (clauses 14-16) appear from the drafting notes to relate to identifying data associated with an individual from a query across datasets or databases. However, the technical ability to search and identify people will go much further, and will be hard to regulate.

51. Filtering arrangements, described as a 'search engine'371 for the collected communications data, would allow complex questions to be asked of the database relating to suspects' social networks.

52. Combined with large-scale data collection it could completely change the economics of mass surveillance. For instance, the data could identify a protester who posts to a radical politics site, and their location at any given time. Their favoured contacts, those likely to be politicised and their locations could be identified. The data could in effect be used to monitor political activity, or any activity deemed unusual or deviant, to a finely grained level.

53. At present, the police make sparing use of mobile phone location data because they get charged by the phone companies – typically several hundred pounds per subject. Once the data are all collected into connected databases, the per-use cost will approach zero. Investigative methods that are at present only used for serious crimes like rape and murder will be available to investigate minor issues too.

54. Given the nature of the communications data involved and the volume of data available, the scale of the likely collection and the provisions for filtering, we do not believe that it is creditable to claim this is simply a case of maintaining of existing powers to collect communications data. This is a significant extension of capability to create something qualitatively different.

Mission creep

---

370 Meaning simply 'it's not all in one place'

371 http://www.parliament.uk/documents/joint-committees/communications-data/uc170712ev4HC479iv.pdf page 35

55. We are concerned about the inevitability of 'mission creep', and the risk that this new cache of communications data will be used for an increasingly broad range of purposes. Home Office officials were pressed by the Committee about whether the data would be used to investigate speeding or dog fouling. They were reluctant to rule anything out. Dr Julian Huppert asked in the Joint Committee evidence session372:

> *"The Chief Constable of Derbyshire, Mr Creedon, who is the ACPO lead in the area, said last month that he would consider it perfectly appropriate if he saw somebody texting or using a mobile phone while driving to use the communications data for that."*

56. In reply, Charles Farr did not rule this use of the data out, saying: "I think you would have to demonstrate necessity and proportionality; let me put it like that."

57. We do not believe that the primary check on the purposes for which communications data can be used should be the judgement of the law enforcement bodies themselves of what is 'proportionate and necessary'. The broad questions about the proportionality and necessity of the collection and use of this data for different purposes are better discussed in a forum that can make democratically legitimate judgements about the trade-offs between public interest, security and privacy. This is a job for Parliament.

58. We note the recommendation in the Demos report #Intelligence, which suggests that use of 'SOCMINT' – their broad term for information generated through social media – be limited:

> "As UK legislation at present limits the work of the intelligence agencies to national security, the detection and prevention of serious crime, and the economic wellbeing of the nation, we believe this narrower 'sufficient and sustainable cause' restriction should apply to their use of SOCMINT as well."373

59. The purposes for which the draft Bill suggests communications data can be used are far too broad and vague. This is another reason the draft Bill should be axed.

Wrongful access and the security of the data

60. In addition to overly broad access under the law, through mission creep for example, there is a risk of unlawful access through the insecurity of the data.

61. Sensitive private information has, in the past, fallen victim to 'blagging'. From obtaining NHS records374 to accessing the Police National Computer375, it is clear that no store of information is completely safe. Given enough time, private data can – and, likely, will – be accessed unlawfully by someone who is sufficiently determined or unscrupulous. It is worth reflecting on the fact that for some twenty years, "everyone knew" that journalists working for News International (and some other firms) were unlawfully obtaining information by bribing police officers, blagging information from official databases, and conducting unlawful interception.

---

372 See page 5 http://www.parliament.uk/documents/joint-committees/communications-data/ucJCDCD100712Ev1.pdf

373 http://demos.co.uk/files/_Intelligence_-_web.pdf?1335197327 page 43

374 Leveson Inquiry, Statement of Matt Driscoll, News of the World - 21st March 2012

375 Leveson Inquiry, Statement of Assistant Chief Constable Jerry Kirkby - 21st March 2012 pp.22-23.

62. We are concerned about the security of the data that will be captured and stored under these powers. The extent to which the security of the data can be maintained is an important factor in considerations of how proportionate and necessary these powers are. As such, we would expect an analysis of the likely security issues should be part of the public debate about the Bill.

63. However, we have not seen any such public-facing analysis. We are concerned that there has not been a full independent analysis of the technology involved and the security of the collection and storage of data.

64. Whenever data is stored by a company there will be a risk that it will be lost, stolen, or damaged. Normally, that risk of loss or theft is offset by the importance of the business purpose for which the company is retaining the data. The more valuable the data, the more likely it will be that individuals or groups will attempt to obtain it. Lawful points of access to information provide an attractive target for unlawful activity. In 2005, more than 100 mobile phones belonging to members of the Greek government were unlawfully tapped, through an exploitation of lawfully placed backdoors in the devices376. In 2009 it emerged that former US President Bill Clinton's personal emails – lawfully collected – were unlawfully accessed by an intelligence analyst377.

Risks of misuse

65. The phone hacking scandal and the revelations from the Leveson Inquiry help to demonstrate that the ability to access personal information will be exploited for a variety of reasons. There are many ways that the data involved could be misused in a manner that would affect whistleblowers, journalists and their sources, legal privilege and activists.

66. For example, the Bill would facilitate relatively easy access to the contact histories of possible suspected leaks or sources that matched with those of a particular journalist. The Bill attempts to make searches easier, and automated. The searches could also extend to location histories.

67. A government wishing to know which of twelve civil servants had leaked evidence of serious wrongdoing to a journalist might ask each CSP for a list of everyone these thirteen people had communicated with last week, and when. The data would be taken to a central point (assumed to be NTAC at GCHQ) and studied, from which it might emerge that civil servant number 3 had called the mobile phone of Professor X at 7 on Tuesday evening, and Professor X had then made a Skype call to the journalist.

68. In short, the data matching and sorting provisions within the Bill would make anonymity extraordinarily difficult to maintain, whilst placing surveillance tools into the hands of an extremely large number of police, intelligence and other operatives who work under insufficient scrutiny.

69. See Annex B for a briefing from Public Concern at Work (PCaW) regarding these powers and the possible dangers for whistleblowers. This helps demonstrate that access to information can be used for the purposes of malicious or personal vendettas or certainly reactions that are not in the public interest. PCaW detail cases of whistleblowers and leaks that have involved an overzealous reaction from authorities including the case of HMRC tax lawyer Osita Mba378, who had raised concerns about special deals between HMRC and those with large outstanding tax bills:

---

376 http://www.guardian.co.uk/business/2006/feb/07/newmedia.media?INTCMP=ILCNETTXT348 7

377 http://www.wired.com/threatlevel/2009/06/pinwale

378 http://www.guardian.co.uk/politics/2012/jun/07/information-commissioner-hmrc-whistleblower

"In early part of June this year the Guardian reported that the Information Commissioner's Office (ICO) has launched an inquiry into the way HMRC investigators obtained the personal information of Mba and his wife.

The ICO received documents that show in October 2011 HMRC managers sent personal information, including Claudia Mba's address and four phones' numbers to the Department's Criminal Investigations Unit."

70. Trust in public institutions and those in them is important. Most public servants and officials and those involved in law enforcement are likely trustworthy. However, a desire to trust institutions does not mean ignoring the possible motivations, incentives and vulnerabilities of the people working in them.

Problems with safeguards governing access

71. The Impact Assessment asserts (page 5) that 'RIPA place strict rules on when, and by whom, access can be obtained to communications data retained and stored by industry", which is designed to prevent unauthorised access. However, RIPA does not place strict enough rules on access.

72. The Bill promises the same 'safeguards' as provided in RIPA. This means that (with the exception of local authorities, who must now seek judicial approval) organisations such as the police will continue to nominate an internal 'designated person' to authorise access to the collected data of millions of people.

73. For law enforcement purposes, access to the data will simply require designated senior officers at those bodies to believe that it's "necessary to obtain the data" and that it is "proportionate to what is sought to be achieved."

74. We are concerned that this effectively means that there will be no external, meaningful and direct oversight of access requests. We believe this will be ripe for abuse and exploitation379. The safeguards over access need to be tightened up rather than used as a model for access to a much broader store of information.

The Interception of Communications Commissioner

75. The oversight of such 'internal authorisation' is performed through the retrospective analysis of a sample of authorised requests. Each year the Interception of Communications Commissioner (IoCC) and his inspectors review a subset of the applications to ensure that policy is being applied correctly. We welcome the increasing amounts of information that the inspector has published year on year.

The 'error percentage'

76. However, we are concerned about the figures purportedly identifying the error rate of RIPA requests. The IoCC report states that the error percentage is 0.18% in 2011380. This looks to us to be incorrect, and the report lacks important basic details about when, where and how often errors happen. As a result the IoCC report does not facilitate a proper independent analysis of how the oversight and sign-off regime is working.381

---

379 For more information on weaknesses in the current regime, we note the Big Brother Watch report 'A legacy of suspicion', available at http://www.bigbrotherwatch.org.uk//files/ripa/RIPA_Aug12_final.pdf

380 Page 30, IoCC report 2011

381 This issue was initially noted by Caspar Bowden

77. In 2011, the IoCC identified 895 authorisation errors. On page 30, the report states that this is the number reported to the Commissioner's office. Page 32 clarifies that 99 of the 895 errors were 'identified by my inspectors during the inspections', rather than having been reported to them.

78. Seventy seven of those discovered errors appear to have been discovered in local authorities. Local authorities account for .5% of the total number of RIPA requests in 2011 (the total being 494,078 requests).

79. On page 30 of his report the Inspector states that the 'error percentage' is 0.18%. This appears to have been calculated by dividing the number of reported and discovered errors by the total number of RIPA requests.

80. However, the total number of inspections undertaken – the sample size - is not published. We do not know what percentage of the 494,078 requests the IoCC team inspected. That means that the reported error figure of 0.18% means very little, if anything.

81. The cited figure of 0.18% would only identify the error percentage rate for the total number of RIPA requests if the IoCC team inspected every single request or they are confident that there are zero further errors in the uninspected requests.

82. To determine the necessity and proportionality of powers to collect and access communications data, it is critical to have a clear picture of the error percentage. First, because it facilitates a proper understanding of the likely 'collateral intrusion'. Second, because it helps us to understand the likely frequency of false positives.

83. The error percentage has been used as evidence of how robust the current oversight regime is. For example, the figure from 2010 (0.3%) is cited on page 11 of the Home Office's Privacy Impact Assessment for the draft Bill. The IoCC himself states on page 30 of his report that he is 'satisfied that the overall error rate is still low when compared to the number of requests that were made during the course of the reporting year'.

84. Errors can have serious consequences. We know that two members of the public were wrongfully detained in 2011 as a result of RIPA related errors382. A certain number of mistakes are inevitable, but it is clear that the police occasionally use retained data to conduct invasive operations without sufficient verification.

85. In his evidence to the Joint Committee, Charles Farr makes the point that understanding the effectiveness of the authorisation regime is critical to examining how appropriate the powers are:

> *"the trivialisation of the use of communications data is therefore better tackled through an examination of the application process and the extent to which necessity and proportionality are, indeed, ingrained in the system. That feels, to me, a more likely route to avoiding trivialisation than defining or redefining serious crime, which, as you rightly say, is fraught with hazard. I personally believe that the necessity and proportionality tests are met by the users who use most of this data—the police—but you will come to a view on that."*383

86. It is crucial that the issue of sample size and error percentage is clarified. It is only possible to examine how appropriate such powers are when there is transparent oversight that inspires the full confidence of stakeholders.

87. We have written to the Commissioner to ask them to publish the sample size (ie the number of requests inspected), and to clarify the error percentage calculation. So far, their response has been to confirm that the

382 http://www.guardian.co.uk/uk/2012/jul/13/snooping-errors-wrongful-detention-watchdog

383 http://www.parliament.uk/documents/joint-committees/communications-data/ucJCDCD100712Ev1.pdf page 5

number of requests inspected cannot be published. We have written a further open letter, which will be published on our website, highlighting the apparent calculation error and requesting an explanation. We will supply details of any reply to the Committee.

88. We recommend a review of the oversight of the access regime, for example looking at whether the IoCC has the required technical and legal staff, and the extent to which it relies on the police and agencies for advice. We also recommend an analysis of what information the IoCC should disclose to ensure full and transparent oversight of the access regime. This should be designed from the 'outside in', starting from the perspective of trying to ensure proper democratic oversight.

89. We recommend that, in addition to increased transparency of the workings of the oversight and inspection regime, those whose data is accessed are informed. This could be limited in cases where there are potential operational problems with informing the data subject.

90. As it stands, the safeguards are not transparent, and they do not command our confidence or the confidence of other knowledgeable observers. We are concerned therefore that the Home Office plans to step up to blanket data collection and retention with the same unsatisfactory oversight.

Incompatibility with human rights law

91. Annex A contains a legal opinion from Eric Metcalfe of Monckton Chambers regarding the compatibility of the draft Communications Data Bill. Metcalfe concludes that the Bill is incompatible with the UK's obligations under Article 8 ECHR on the basis that it fails to improve on the authorisation and oversight regime under RIPA and imposes a 'further requirement on CSPs and others to retain, make available and filter communications data for the purposes of lawful surveillance. In the absence of sufficient safeguards, this constitutes a further, disproportionate interference with the right to privacy".

92. Explaining the position on the insufficiency of the current safeguards, Metcalfe sets out that Article 8 requires access to communications data be governed by legislation the provides "adequate and effective safeguards against abuse" (para 15). He argues that the senior figure responsible for authorising access under RIPA 'cannot be credibly described as sufficiently independent or objective to provide an effective safeguard against arbitrariness or abuse" (para 16).

93. On the new powers to order collection and access to more communications data, Metcalfe argues that "the Bill's power to require CSPs to store, make available and filter their customers' private communications data in a particular manner for the sake of making covert surveillance easier" is "plainly disproportionate" (para 29).

94. The full opinion can be found at Annex A.

Retention is being challenged in many jurisdictions

95. The Data Retention Directive and its implementation are subject to legal challenges across Europe. In January of this year, Digital Rights Ireland asked the European Court of Justice to consider whether the Data Retention Directive is consistent with EU law384. The implementation of the Data Retention Directive is also being challenged in various forms in Germany385, Bulgaria386, Romania387, Cyprus388 and Czech

384 See http://www.thejournal.ie/ecj-asked-to-rule-on-mandatory-retention-of-phone-and-internet-data-339434-Jan2012/ and for the document submitted to the Court, see http://www.scribd.com/doc/97936957/Digital-Rights-Ireland-data-retention-challenge-Preliminary-Reference-Questions

385 http://www.totaltele.com/view.aspx?ID=473999

Republic389. We consider it unwise to propose further collection and retention measures when the scope and implementation of the current Directive are being challenged across Europe.

96. The Article 29 Working Group published a report in 2010 on the implementation of the Data Retention Directive and were critical of the implementation of the Directive across Member States. They recommended that the categories of data retainable under the Directive be considered exhaustive, and that "the list of serious crimes justifying retention under the directive should be laid down at domestic level based on national law, taking into account the considerations...as for the need to clearly define and delineate what is meant by "serious crime.""

97. The Working Party were also very critical of the lack of statistics from Member States on the implementation of the Data Retention Directive, which meant a full review of the implementation of the directive was impossible. It seems unwise to propose an extension of the types and amount of information collected and stored whilst the impact of the current Directive is unclear.

August 2012

386 http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention

387 http://www.edri.org/edrigram/number10.1/romanian-senate-rejects-data-retention

388 http://www.pcadvisor.co.uk/news/mobile-phone/3362812/czechs-consider-reintroducing-eu-data-retention-rules/

389 http://jurist.org/paperchase/2011/03/czech-constitutional-court-overturns-parts-of-data-retention-law.php

Open rights Group – supplementary evidence

A note on storage of third-party encrypted data by CSPs and "Perfect Forward Security"
For the Joint Committee on the draft Communications Data Billi
Questioning in the closed sessions has suggested a scenario under which a network CSP (i.e. ISP, such as BT) would be requested to store encrypted data-streams between their customers and third-party CSPs (such as Google). The implication that, under RIPA or equivalent, third-party CSPs would be requested to retrospectively decrypt this captured data.
(Q435-440, Q464-467, Q505-507, Q589-Q597. Q595 in particular)

We believe this scenario will be found to be unworkable for technical reasons. (With particular reference to point 5.)
1) Requirement that the entire stream be captured will influence the way in which this data can be captured. The determination to capture a communication must be made at the very beginning of the connection. This would have implications in terms of cost and technical architecture.
2) Requirement that the third-party CSP still has the key in question. It must be possible to identify and retrieve appropriate private key to decrypt. CSPs may have a large number of keys (e.g. some certificate signing authorities require a different certificate for each server, and hence a different key for each server.) Keys may only be kept during the lifetime of a specific server - hardware turnover rates may be quite high on larger sites. Indeed key certificates may expire and be replaced within the time period between capture and the request to decrypt.
3) Retrospective decryption of TLS-encrypted streams is not a standard business function. If the appropriate procedure to do so is not available, time would need to be spent developing it. Regardless, it is likely an additional expense to the third-party CSP.ii
4) Security policies may require any key used for this purpose be retired from active use. This would incur additional expenses in replacing them, and additionally the change in key would be publicly observable (potentially signalling that an order to decrypt has taken place).
5) Even with access to the key, it may be possible that the stream cannot be decoded. Current technical implementations of the technology can use Diffie–Hellmaniii key exchange to establish the use of a cipher which cannot be retrospectively decoded. Sessions that use a cipher-suite that provide Perfect Forward Secrecy (PFS) are not believed possible to decrypt since the key used to encrypt the session is not derived from the key held on the server.iv This technology exists precisely to protect encrypted streams from being decrypted in the event of the private key being compromised.
As an example: any encrypted stream between Google and a browser with PFS capacity (which now includes all widely used browsers), if stored, could then not be retrospectively decrypted by Google.
We anticipate wider adoption of PFS, especially by sites motivated to provide better privacy of their user's communications. At best, any order for CSPs to store encrypted streams at public expense would accelerate adoption.

[1] Joint Committee on the draft Communications Data Bill http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/news/call-for-evidence/
[1] There are companies offering retrospective decryption tools for TLS (where Diffie-Hellman exchange is not used) which might be why it is imagined feasible. For example Wireshark and Network Instruments Observer offer this facility.
http://www.networkinstruments.com/support/html_doc/current/index.html#page/Observer/decoding_encrypted_network_traffic.html
http://wiki.wireshark.org/SSL

[1] Diffie–Hellman key exchange, Wikipedia https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange
[1] Perfect Forward Secrecy, Wikipedia and Google Blog
https://en.wikipedia.org/wiki/Perfect_forward_secrecy
http://googleonlinesecurity.blogspot.co.uk/2011/11/protecting-data-for-long-term-with.html

Anne Palmer

General:
1) Has the Home Office made it clear what it hopes to achieve through the draft Bill? I understand that the Home Office has to implement EU Legislation and that it has to monitor all its own British Citizens and then to forward the information it has gathered, to the European Union.

2) Has the Government made a convincing case for the need for the new powers proposed in the draft Bill? There is no way any BRITISH Government can make a "Convincing Case" for the need of these EU "NEW POWERS" for the proposed Draft Bill. For the people that were not around in the last war, legislation such as this was not even thought about. Letters were opened and certain words blocked out-but that was in war time and many might have been killed by a thoughtless remark in print. Although this legislation is being brought about allegedly because of 'Terrorism' and 'Terrorists', and sadly, the USA and the UK are well aware that thousands of people can be killed through such despicable terrorists acts. But many millions were killed in the last World War to prevent such as this kind of legislation being thought of and brought about by foreigners. That war was won to prevent this kind of legislation and to bring FREEDOM for ALL. There will always be terrorism in this world of "today", with or without this legislation, yet if our Government allows this Bill to go through, the terrorists will have won. Nothing will be gained by this proposed Legislation except to alienate the people even further away from this present Coalition Government as well as the European Union. Exactly WHO will be the next EU Leader and what will that leader require? I never would have thought the EU would have brought this legislation out, and never the slightest thought that a British Government would even think of passing it.

3) How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy? This Bill can never "fit in" and, with the greatest respect to you all, I doubt any one of you will ever be forgiven for the despicable intrusion into the people's individual privacy. They will have no privacy if this Bill goes through, and never will anyone that went through the last war. People and friends were being bombed to bits, with houses gone and people cowering in Bomb Shelters. Men folk were away at war giving their lives for your FREEDOM today; between you, you are all letting this sacrifice slip and it appears all you can do is obey the directives (orders) of foreigners, for that is what this legislation is all about. Yet we vote and contribute to your pay for Governing this Country according to its very long standing Common Law Constitution.

4) What lessons can be learnt from the approach of other countries to the collection of communications data? They may learn, all too late that this EU Directive should have been torn up.

5). Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider? What this piece of EU Legislation costs this Country if this is accepted will be beyond price.

6). The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data? It is already just one EU Directive, the intrusive Directive 2006/24/EC,
No matter how this once sovereign National Government try's to dress it up.

7). If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties? Can you really rebalance Civil Liberties? To make them what they once used to be?

8). Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base? What might be the effect on business? As most EU Countries the UK deals with will have exactly the same legislation, they will be in exactly the same position. On the other hand, if this Country liberates itself from foreign rule, perhaps a great deal of business will come our way. All will know we are FREE for our people will throw off their sense of defeat and depression and bells will ring out across the land. It has happened before for it is the golden thread of British history.

Costs:

9) Is the estimated cost of £1.8bn over 10 years realistic? That £1.8bn is nothing compared to the loss of freedom the people will feel if this legislation goes ahead. All through a British Government wanting to snoop and snitch on a once FREE people and then sending the information gathered to strangers on the Continent. A people that fought and yes many gave their lives so that there would always be a freely elected British Government in that wonderful House of Commons that would always be guided by its own long standing Common Law Constitution. Yet in a note to Germany re this Data Retention, which had taken a critical stance against this Bill and wanted an "opt out" from it, was told in writing, "In this context, it must be recalled that Union Law prevails over national law, including national constitutional law". Yet I remember one Prime Minister of GREAT BRITAIN stating quite clearly "There is no question of eroding any national sovereignty" in joining the European Community. Yet we have permanent laws on treason protecting our Constitution, so how can that statement be right? How can EU Law over-ride our "National Constitution" that has lasted hundreds of years and has been saved by fighting and winning two World Wars? It is undoubtedly high time for this Country to remove itself from the federalist European Union with haste. There has been a growing stench of betrayal in the air for a long while now and people know it.

10). The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-£6bn. Is this figure realistic? Benefits? Absolute nonsense.

Scope:
11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill? This Bill should be scrapped and deep down, I believe with all my heart, you all know it too.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order? No one should. This is one piece of EU legislation that should be consigned to the bin-permanently.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty? I hope there are no such plans. Is the latter worth trying?

14. Use of Communications Data: 14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect? (a) There are no circumstances at all. (b) If this EU Directive is put into action, which countries will not access any or all communications in the UK?

15. Is the proposed 12-month period for the retention of data too long or too short? The whole EU Proposals for this legislation should be scrapped. I would like to believe that most of those that have been freely elected, know that too.

Safeguards:
16. (a) Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. a) No one can guarantee any kind of "safeguard" when any information gathered is to go to the European Union. The information will also be shared with the USA. (b) How should "designated senior officer" be defined? (b) There will be no need of such an'Officer' if commonsense reigns. (c) Is this system satisfactory? (c) Obviously the answer is "NO". (d) Are there concerns about compliance with Article 8 ECHR? (d) 1. "Everyone has the right to respect for his private and family life, his home and his correspondence". (d) 2. "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the

prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". You can remake the law to fit part two but it will not and never be a democratic society again. The last war was fought for FREEDOM and it is that you will all lose forever. Even now you are obeying foreign laws rather than looking to your own Common law Constitution and all that my generation fought and gave their lives for.

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be? In view of my previous answers, there is no need for an answer to this.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible? This EU Proposal should be rejected.
Parliamentary Oversight: 19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory? The Draft Bill should be rejected.

Enforcement:
20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill? If the Government decides to implement this Bill, it will be the greatest mistake any British Government has made thus far. It should be remembered that the people contribute to what this Government does. Why should they contribute to any EU Fine when all the people can do is obey their own Common law Constitution for they had no hand in allowing foreigners to make the laws even their own Governments have to obey.

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence? Answer as at 20.

Technical:
22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content? None of the Communications are meant to be 'stored safely', they are meant to be shared with others that this Government cannot possibly 'vouch' for. The EU and the USA and possible others.

23. How safely can communications data be stored? As above, they cannot. How can e-mails captured not be read? It was in fact Edward Heath who made it very clear that in joining the then EEC, that "there would be no loss of essential Sovereignty" and people voted to remain in the EEC in 1975 because they believed what he said. He lied and admitted that lie on Television. Admission of that lie did not put the matter right. The people have never been asked since that date whether they want to remain in the EU, yet this Government is asking the people now (that know about this (EU) legislation), if we should allow this Draft Communication's Bill, known by such as myself as, "The Snoopers Bill" if they want to be spied on for the rest of their lives, which is exactly what this Bill will allow. The vast majority of people's freedoms and privacy will be gone forever including your own.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible? No. A wise Government would reject this EU Directive.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill? It may not come to this at this time, because people in other countries-(namely Germany) are aware of this proposal- do not like it either, but, as we have found out to our cost before, what the EU decides it wants, it will have, one way or another. It really is time to put this Country out of its reach.

26. Are there concerns about the consequences of decryption? I doubt anyone could prevent Governments from tracking e-mails – but there are ways of course where nothing is kept on or in the Computer. The Fifth Amendment to the United States Constitution protects some people under criminal investigation from having to

reveal passwords provided access to the encrypted content of storage devices. Perhaps we should have some kind of that protection here.

August 2012

Public Concern at Work

INTRODUCTION

1. We are providing this response to the Joint Committee on the Draft Communications Data Bill as part of the call for written evidence. Our response focusses on issues where the draft bill may affect whistleblowing and the legal protection for whistleblowers, set out in the Public Interest Disclosure Act (PIDA). We begin by setting out a brief introduction to Public Concern at Work to provide context for our submission. We suggest 'function creep' within the proposed powers could mean the bill is used by investigating authorities to track communications between a whistleblower and third parties, such as regulators, MPs or journalists resulting in a chilling effect on the likelihood that regulatory or wider disclosures which are already protected by law wil be raised. As we explain below, we believe there is a real risk that these powers set out in the bill will be abused, by those undertaking leak inquiries under the offence of misconduct in public office. We also raise concerns over the effect this may have on the legal protection for whistleblowers under PIDA. We recommend that investigations concerning misconduct in public office be excluded from the communication data that investigating authorities can obtain for the purposes of detecting crime or preventing disorder, or that there is an additional arms length oversight mechanism when such investigations are being undertaken or contemplated.[390] We also suggest that where the communication data of a whistleblower is accessed but no prosecution is pursued that the individual is informed that this access request was made and obtained.

2. We have limited this submission to our particular area of expertise – namely the protection of whistleblowers - but we would also endorse the concerns raised by other civil society organisations particularly Big Brother Watch, Open Rights Group, Liberty and Justice about the very broad powers contained within the draft bill. We agree that the nature and breadth of communications data being collected, stored and mined means that the distinction between communications data and communications content will necessarily become blurred so that there are real risks to individuals' privacy rights as a result of these provisions. [391]

3. As stated in evidence by Angela Patrick of Justice: "It is particularly important for parliamentarians to be aware of the need for effective controls and safeguards to ensure that surveillance is only used in those circumstances where it is strictly necessary and justifiable. Individuals in most cases, if surveillance is effective, will never know that it has happened and so will never have access to an effective challenge or a remedy." [392]We would wholly endorse this statement and urge the committee to consider the question of appropriate checks and balances very carefully.

4. We would also urge the committee to consider the implications for communications involving lawyer client privilege, the protection of jounalists' sources and the confidentiality of communications between constituents and their MPs, as part of this consultation and suggest that either such communications should be excluded from the reach of this bill, or additional arms length safeguards are introduced where such communications are going to be monitored.

Background to Public Concern at Work

5. Public Concern at Work (PCaW) is an independent charity and legal advice centre. Launched in 1993, we have helped lead developments on whistleblowing as a good governance and risk management tool in the UK and abroad. We provide a confidential advice line for individuals with whistleblowing dilemmas; professional support to organisations , policy advice to Governments and international

---

[390] Part 2, Subsection (6) (b) of the Draft Communications Bill

[391] http://www.parliament.uk/documents/joint-committees/communications-data/uc170712ev4HC479iv.pdf

[392] Q222 Uncorrected Transcript of Oral Evidence, Joint Committee, Draft Communications Bill 17 July 2012

organisations andpublic education programme, that promote whistleblowing and good workplace cultures.

6. By way of brief background, PCaW was set up in response to a series of scandals and tragedies in the late 1980s and early 1990s which included the sinking of the Herald of Free Enterprise in 1987, the Piper Alpha oil rig explosion and the collapse of the BCCI amidst widespread fraud in 1990. The various official Inquiries after these disasters revealed that all too often staff had known of the danger but were too scared to speak up or, if they did, that they did so in the wrong way or to the wrong person, only to be ignored and/or dismissed.

7. Our work to address whistleblowing effectively as a matter of accountability and good governance means that we have unrivalled practical experience in the field - both in operating an advice line service for individuals and in providing professional support for organisations on whistleblowing.

The Public Interest Disclosure Act

8. When enacted, PIDA was praised "for so skilfully achieving the essential but delicate balance…between the public interest and the interests of employers".[393] The Act most readily protects concerns raised with an employer, but also gives protection to individuals who go outside their employer such as to a regulator, or MP/ journalist in certain circumstances when the concern has been covered up or not addressed. PIDA is ultimately about accountability and it follows that for this to work it must be possible for those responsible to be held to account for their conduct. This provides an incentive for organisations to deal openly and well with any potential wrongdoing when first raised by a worker. As stated below, we believe that one of the potential unintended consequences of this bill will be that legitimate whistleblowers working in public authorities will be discouraged from raising concerns openly or confidentially and will use anonymous leaking as an alternative if they believe that their communications are being or could be tracked.

Response to the Consultation

9. We note that the Committee has discussed 'function creep' with the bill appearing to cover more areas of investigation than originally indicated when proposed by the Home Secretary. [394] We are concerned the new powers could be used to pursue leakers and whistleblowers via the offence of misconduct in public office.

10. Whistleblowing is now seen in the UK as a positive and necessary function of our democracy. Disclosures under PIDA to any level of internal management within an orginisation can be protected as can disclosures to a regulator, MP and to the media. There is often going to be a tension between wider disclosures (ie outside the regulatory framework to the media) and leaking confidential information about the political movements and policy discussions within Government. Leaks have long been described as damaging for effective government as they can erode the trust between a Minister and their civil servants .[395] The line between whether someone is leaking information or whistleblowing in the public interest is not always a clear one for someone at the heart of this dilemma, and controversy has followed where the government has tried to pursue people they believe to have leaked information with criminal sanctions. Our concern is that powers proposed in this Bill may push whistleblowers into using anonymous online leaking platforms or other anonymous means of communication rather than the open and confidential options encouraged by best practice and protected under PIDA.

---

[393] Hansard HL, 5 June 1998 Col. 614

[394] Q183 Uncorrected Transcript of Oral Evidence, Joint Committee, Draft Communications Bill 12 July 2012

[395] P.g. 7 Leaks and Whistleblowing, 10th Report of the 2008-09 Session of The Public Administration Select Committee

11. Leaking information can be a criminal offence if it breaches the official secrets act which outlaws disclosures of information related to national security, national defence or relations with a foreign power. [396] How to deal with a situation where information leaked falls below this threshold has proven controversial, in recent years the police have unsuccessfully pursued individuals using the offence of misconduct in public office.

12. The Crown Prosecution Service (CPS) describes misconduct in public office as follows-
    - a public officer acting as such;
    - wilfully neglects to perform his duty and/or wilfully misconducts himself;
    - to such a degree as to amount to an abuse of the public's trust in the office holder;
    - without reasonable excuse or justification.[397]

13. There are two recent cases that demonstrate this tension and provide an insight into how 'function creep' towards the offence of misconduct in public office could occur. The first is the aborted investigation into Damian Green MP and Christopher Galley in 2008 and the second is the collapsed prosecution of journalist Sally Murrer in 2007. Both cases revolved around the investigation of misconduct in public office as the information disclosed did not fall within the scope of the official secrets act. Questions were asked in both cases as to whether it was in the public interest to pursue the cases. We have summmarised the circumstances in each of these cases below and provided a more thorough case study of both cases at Annex A attached to this submission.

14. In Galley and Green's case, there had been press coverage about a number of problems within the Home Office and a leak investigation ensued resulting in a raid of Damian Green MP's Westminster Office and the arrest of a junior home office civil servant (Chris Galley) and Mr Green. In the end the CPS dropped the case against both men on the basis that the case had no reasonable prospect of success.

15. In the Murrer case a journalist and a police sergeant were prosecuted for the same offence over a number of stories that appeared in a local paper which included the arrest of the local football team's star striker. The case was thrown out when the trial judge ruled a taped conversation between Murrer and the sergeant was inadmissible as evidence due to legal protection forjournalistic sources under European law. Both cases demonstrate a concern we share with oral evidence put before the committee that under the proposed system a disclosure of the confidential information only requires a senior officer to approve its use. [398] The proposed powers would make it possible for an MP or a journalist who has received information from a whistleblower to have their email and electronic correspondence tracked without having any knowledge that this is happening. The potential for abuse can be seen in the Home Affairs Select Committee report into the Green and Galley investigation where the committee criticised the Home Office and the Cabinet Office for exaggerating the actual and potential damage the leaks would do to national security when they approached the Police asking them to investigate.

16. A cautionary tale can also be seen in the US where two cases have been brought against the US government centering on a secret presidential order signed by President Bush in October 2001, which was then exposed in 2005 via whistleblowers and media reports.[399] The order allowed the US law enforcement agencies to secretly store email and telephone data via thetelecommunications companies

[396] Official Secrets Act 1989

[397] Misconduct in Public Office- CPS- http://www.cps.gov.uk/legal/l_to_o/misconduct_in_public_office/#a04

[398] Q117 Joint Committee on the Draft Communications Bill, Uncorrected Transcript of Written Evidence, The Draft Communications Bill 11 July 2012

[399] http://www.nytimes.com/2012/08/23/opinion/the-national-security-agencys-domestic-spying-program.html?_r=1&ref=opinion

under the guise of national security in the wake of 9/11. Security services were allowed access to this data without prior approval from an outside court, this situation continues today. When this was uncovered and questions were asked as to whether the presidential orders were constitutional, a class action suit was brought against the telecommunication companies by the Electronic Frontier Foundation and the US Government in response, passed laws exonerating the relevant companies from liability. This in turn led to a further class action suit this time against the US Government and the politicians responsible for creating the current system, namely former President George W. Bush, then Vice President Dick Cheney and the administration's Attorney General. Though the case is still to be decided, the decision by the US Government to create a system of electronic surveillance without any warrant or judicial oversight has caused considerable controversy and a lengthy legal battle. The Committee should look at this situation as an example of the unintended consequences of such an initiative and ask the government to ensure that proper safeguards are in place so that similar legal actions in the UK are not necessary.

17. We recommend that more thought is given to what criminal offences are included under provisions that allow communications data to be obtained in the pursuit of detecting crime or preventing disorder. We suggest that the bill either excludes misconduct in public office from Part 2 section 6(b), or that additional arms length oversight is required outside of the investigating authority where such a charge is being contemplated. We also recommend that a warrant or judicial oversight system is brought in to monitor the use of the new powers to ensure requests are necessary and used in an appropriate and proportionate way. [400]

18. We are also concerned about the use of the proposed powers as 'fishing expedition' against an individual who is known to have raised concerns with a body external to the orgnisation within which they work, under the pretence that the individual might commit a criminal offence but in reality it is an attempt to intimidate the individual.

19. We draw the Committee's attention to the treatment of HMRC whistleblower Osita Mba who raised concerns about the inappropriate tax deal that had been struck between the tax authorities and large corporations. [401] Mr Mba raised his concerns with the Public Accounts Committee, the Treasury Select Committee and with the National Audit Office, each of these avenues of disclosure is protected under PIDA. The Guardian reported in June that a complaint had been issued in relation Mr Mba and that his wife's personal details had been passed by HMRC managers to the Department's criminal investigation department.[402] Mr Mba has not been charged with any criminal offence, in fact his concerns led to critical reports on the governance arrangements at the HMRC and praise from the chair of the Public Accounts Select Committee and its members.

20. Our concern is that without adequate safeguards there is a very real risk that the powers provided by this piece of legislation will be misused by those charged with undertaking a leak investigation which will only serve to intimidate people like Mr Mba, which in turn will mean that it is very much less likely that government whistleblowers (like Mr Mba) will ever come forward. Alternatively the likelihood is that such whistleblowers will anonymously leak the information for fear of communication data tracking. Leading to a weakening of public trust and confidence, making it harder for wrongdoing to be addressed and more difficult to protect an individual or even to thank them.

21. We are also concerned that this has the potential to undermine the legal protection for whistleblowers. PIDA requires the claimant to demonstrate that there is a link between the protected disclosure (the

[400] Part 2, Subsection (6) (b) of the Draft Communications Bill

[401] See Annex A for the full case study.

[402] Audit Office Attacks Tax Deals for Corporations, Rajeev Syal and Shiv Malik, The Guardian, Thursday 14 June 2012

whistleblowing) and the detriment suffered (the victimsation or dismissal suffered) but under the proposed powers there is no way an individual would be aware they were subject to such an investigation. This request could well be a key part of any PIDA case this individual may want to take forward as it could demonstrate a line of causation from the concerns raised to any detriment or victimisation suffered as a result.

22. Our recommendation would be that where a request for communication data is granted in relation to an investigation into a whistleblower, but no prosecution has been brought forward, the requesting authority notifies the target of this request.

23. We trust that this short response is helpful to the committee. We would be pleased to provide any further assistance deemed necessary by the Committee or to expand upon our submission if this would be of help.

August 2012

Privacy International

The current Draft Communications Data Bill is a vague framework that grants the Secretary of State significant powers for future, as yet unspecified, actions. The purpose of this briefing is to match currently available technology against the draft bill in order to better understand what this bill as drafted could enable.[403]

Summary

- In this briefing we address the Committee's Questions 3, 4, 22, 23, 24, 25, 26.

- Q3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy? They fundamentally reverse this Government's stated position on restoring civil liberties.

- Q4. What lessons can be learnt from the approach of other countries to the collection of communications data? The technology for the proposed scheme is primarily used in dictatorships. The details of such approaches and abuses tends only to emerge once these dictatorships are overthrown, for example, in the aftermath of the Arab Spring. Detailed evidence is now emerging revealing the technologies and techniques used by the previous Libyan government against its citizens,[404] and some information about surveillance and censorship systems in Tunisia (which also edits email in transmission[405]) and Egypt has also come to light.[406]

- Q22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content? Any communications service provider (CSP) that did this would be at a fundamental disadvantage within the international market of the internet.

- Q23. How safely can communications data be stored? Stored communications data can never be perfectly secure.

- Q24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible? The proposals for the filtering arrangements are neither clear, nor appropriate, nor technically feasible. Even minimal discussion with a representative cross-section of industry would have demonstrated this, but such discussion has not taken place.

- Q25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill? It will be an extremely simple matter, even for most schoolchildren, to evade the measures in this bill.

- Q26. Are there concerns about the consequences of decryption? This Government (and the previous one) has pushed the development of a "digital economy" in the UK. For such development to be successful, secure communications for payments etc are absolutely crucial. The measures in this bill would fundamentally undermine the digital economy in Britain.

Overview

---

[403] For a detailed discussion of the policy aspects of this technology, we strongly recommend Susan Landau's book "Surveillance or Security - The Risks Posed by New Wiretapping Technologies". ISBN: 978-0262015301, MIT Press, 2011; and her blogpost on https://www.privacyinternational.org/opinion-pieces/surveillance-and-security-securing-whom-and-at-what-cost

[404] http://owni.eu/2011/12/01/exclusive-how-gaddafi-spied-on-the-fathers-of-the-new-libya/

[405] http://www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html

[406] http://online.wsj.com/article/SB10001424052702304520804576345970862420038.html

- Privacy International has been investigating the global surveillance industry for several years. Surveillance companies are innovating at a rapid pace, and expanding their markets in undemocratic regimes. Many of these companies are British, and some sell their technologies and services in Britain as well.

- In 2008, Detica gave a presentation[407] at the ISS World trade show for surveillance equipment, commonly nicknamed 'the Wiretappers' Ball',[408] discussing the potential for national surveillance systems similar to what is now being proposed by the Home Office.

- The presentation highlighted the contemporary obstacles, to achieving such a surveillance system. The issues were not just technical, they were also social and legal; such a system would not be lawful in democratic societies, and would not be accepted by the public. The Home Office is now attempting to change the legal situation, but is ignoring the social and technical issues.

- Q3 & Q4: Intrusion and collection

- The police already have access to data in a way that was unforeseeable when the Regulation of Investigatory Powers Act 2000 (RIPA) was drafted. For example, at the time neither the Transport for London Oyster card nor the Congestion Charge existed.

- The police have "routine access to data from the cameras used for Congestion Charging",[409] and request access to Oyster data under the Data Protection Act. For Oyster data, 5-10% of requests are rejected by Transport for London (TfL) as the requests do not have acceptable levels of detail or are excessive.[410] While TfL review requests for Oyster data with a dedicated team, and can therefore determine whether requests are excessive or unacceptable, the nature of the access to Congestion Charge data is such that TfL cannot review each request, and thus cannot reject excessive requests. The "technical detail"[411] of implementation therefore matters a great deal. If we take the Oyster case as representative, up to 10% of police requests could be illegal but access would nevertheless be granted because the filtering component of the draft bill would create a system of automated access. Automated access almost always results in more requests than manual review; there is a moderation effect that comes from knowing requests will be reviewed before fulfillment.

- "I readily acknowledge that communication data records are highly intrusive as they may give an insight into the everyday activities of the user of a communications device." [412]

- While the 2009 ACPO submission on communications data referred only to phone calls, text messages and cell sites, other submissions to this committee have stated that[413] the draft bill additionally requires the collection and retention of social media traffic data, email and other traffic.[414]

---

[407] Source: Dealing with the retained communications data explosion: https://www.documentcloud.org/documents/409138-23-200810-iss-prg-detica.html

[408] http://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_story.html?tid=pm_pop

[409] What do I need to know about the central London Congestion Charge camera system? p1

http://www.tfl.gov.uk/assets/downloads/CC-Cameras.pdf

[410] http://www.tfl.gov.uk/termsandconditions/12321.aspx#page-link-does-tfl-receive-requests-from-the-police-for-disclosure-of-information-about-the-use-of-individual-oyster-cards-

[411] Home Affairs Committee - Minutes of Evidence, HC 1939-i, Q79, Theresa May to Julian Huppert: http://www.publications.parliament.uk/pa/cm201213/cmselect/cmhaff/1939/120424.htm

[412] ACPO Data Communications Group 2009 response to "Protecting the Public in a Changing Communications Environment – A Public Consultation – Government Proposals to EnsureCommunications Data Remains Available for Future Electronic Communication Services":

http://www.scribd.com/doc/34921616/ACPO-Data-Communications-Group-Submission

- This Bill proposes an extension of current capability to cover all internet services by all devices, with the Secretary of State able to direct services to collect and retain particular data. Bringing together data from such a wide variety of sources, including Facebook sessions and email inboxes, provides an intimate mapping, allowing law enforcement to identify a person's associates, friends, family and daily habits, even when and where that person sleeps.

- Home Office statements claiming that the police have access to less data nowadays than they once did are misleading. Facebook, for example, makes public at least the name and profile photograph of each user. To discover the identity of the owner of Facebook account number 347071695348056, police need only visit http://facebook.com/profile.php?id=347071695348056. When Privacy International submitted Freedom of Information Act requests to the Metropolitan Police[415] and other police forces[416] about their use of social media in investigations, our requests were refused.

- Another source of information readily available to the police is 'Open Source Intelligence' (OSInt) - information that is freely available on the internet. The growth of OSInt monitoring is not something the Home Office has been willing to comment upon, perhaps because it gives the lie to the claim that the police are increasingly deprived of data, but is often highlighted by companies that provide relevant services to the police.[417]

- In one sales brochure, the power of open source intelligence analysis is illustrated with a diagram of the social network of London technology workers (you may spot some names referenced in testimony to the committee, from television, or from the House Staff List).[418]

- The bill provides for the amalgamation of all these techniques to monitor small and large populations, based on orders issued by the Secretary of State. No other functioning democracy monitors its citizens in this way.

- Q22 Capture and storage

- The bill requires the collection of the data of all UK communications users. Anyone in the UK who uses a telephone, mobile phone or domestic email service is already subject to the surveillance regime requiring the retention of data for up to a year. The bill not only proposes to extend collection and storage to other forms of information, but is unprecedented in ordering the collection of additional information not required for commercial purposes.

- In practice, the equipment may collect a complete copy of all internet streams, all email and all webpages, and will then determine which parts to retain. As far as we can see, this is a necessary process if the technology is to function. Privacy International has published a worked example on this topic,[419] looking at

---

[413] HC 479-iv Transcript of Oral Evidence taken before the Joint Committee on the Draft Communications BIll, Tuesday 17 July 2012. Q221- http://www.parliament.uk/documents/joint-committees/communications-data/uc170712ev4HC479iv.pdf

[414] http://www.liberty-human-rights.org.uk/campaigns/no-snoopers-charter/no-snoopers-charter.php

[415] http://www.whatdotheyknow.com/request/social_media_monitoring_policies#incoming-250931

[416] http://www.whatdotheyknow.com/request/social_media_monitoring_policies_2#incoming-257392

[417] ntpreid sales presentation, Gathering Open Source Intelligence Anonymously.
https://www.documentcloud.org/documents/409185-76-201110-iss-iad-t6-ntrepid.html

[418] ntpreid sales presentation, p8 and 9: https://www.documentcloud.org/documents/409179-70-201110-iss-iad-t5-ntrepid.html

[419] https://www.privacyinternational.org/blog/facebook-message-anatomy

the anatomy of a Facebook message and demonstrating that the technical gymnastics the draft law would require would actually be prima facie illegal.

- Technology capable of capturing communications data reliably, separating it from content and storing it safely does not exist. There are a number of approaches, all of which have drawbacks and benefits, and all require tradeoffs between coverage, speed and retention. The stated plans seem impractical, inefficient and complex, and the fact that the Home Office has refused to divulge any technical details does not inspire confidence.

- The definition of "collection" is essential to understanding the implications of the bill. In the United States, “collection” only occurs when an individual views information - for example, when whistleblowers reported that the NSA was “collecting” all emails inside the US,[420] the NSA denied that this was the case, as the emails were not necessarily read.[421] However, in the UK the mere collection (in the normal sense of the word) of information is in itself an interference with the right to privacy enshrined in Article 8 of the Human Rights Act 1998, and therefore must be done in proportionate manner. The Home Office wrongly believes that the US military definition is applicable in the UK.

- Q24 The Filter

- The Filter appears to be designed to operate as a single unified search interface across multiple CSPs’ data sets. Within evidence, it was stated that this is akin to a "search engine for the police".[422]

- The police may also obtain tools that that offer an enhanced view of Facebook activity,[423] showing the network of people an individual is connected with and who he or she exchanges messages with (and how often). In no way can this be considered targeted surveillance. The information of a person who happens to have some connection to someone under suspicion would become visible to the police.

- The Filter may be able to predict the future. A mobile phone company holds enough information to guess where an individual will be tomorrow at a certain time to within a 20 metre radius.[424] The Filter would be able to match time and locations across networks and services, correlate who was where at the same time, and then, by design, step backwards and forwards in time to see who was communicating beforehand or afterwards. The power of this capability is significant and intrusive.[425]

- The Filter may know who you called, what you searched for, and with whom you communicated. Even without content, knowing which Google searches are run during a phone call gives a strong indication of the content of the call, without the content of the call itself being recorded.

- Q25 & Q26: Circumvention and decryption

---

[420] https://www.eff.org/issues/nsa-spying/

[421] See the analysis here: https://www.eff.org/deeplinks/2012/03/nsa-chief-denies-ability-warrantlessly-wiretap-despite-evidence and the Regulation C2.2.1: http://www.fas.org/irp/doddir/dod/d5240_1_r.pdf

[422] Q307 of Oral Evidence taken before the Joint Committee on the Draft Communications Bill http://www.parliament.uk/documents/joint-committees/communications-data/uc170712ev4HC479iv.pdf

[423] Glimmerglass: pg 10 https://www.documentcloud.org/documents/409165-55-201110-iss-iad-t1-glimmerglass.html

[424] http://www.thestar.com/business/article/1224211--where-will-you-be-this-time-tomorrow-smartphone-data-can-guess-within-20-metres

[425] George Danezis and Richard Clayton, Introduction to Traffic Analysis: http://research.microsoft.com/en-us/um/people/gdane/papers/TAIntro-book.pdf

- Circumventing this policy is simple - how simple depends on how far the Home Secretary is willing to extend his/her powers as enabled by the draft bill. In order to improve information security, businesses have begun to use secure networking techniques and outsourced their services in ways that will render the 'black boxes' ineffective. Increasingly, individuals are also seeking out such solutions.

- One timely circumvention example is the geographic limiting of online coverage of the Olympic Games. Due to the low quality of coverage by US network NBC, there have been a proliferation of articles, advice and comment in the US mainstream media explaining how to access the BBC's internet services.[426] Another example is the history of spam email on the internet - a circumvention arms race has been underway for almost 20 years, yet a glance at anyone's email inbox shows there is still no effective prevention mechanism.[427]

- The suggestion of "spoofing" SSL implied in some language in the Bill will simply give criminals an easily detectable sign of active monitoring, being routinely checked by web browsers. This may not be the Bill's intent.

- The bill also fails to cope with technologies that allow for anonymous routing of traffic, i.e. Tor.[428] Developed by the US Navy to protect Government communications, Tor would certainly evade the measures in the draft Bill.[429] We understand that Tor have been asked to give evidence to the committee, and so we refer you to their submission.

- Once 'back door' capabilities are designed into communications networks, they can be used by criminals as well as law enforcement. In 2004, the capabilities built into the Vodafone network in Greece were accessed illegitimately, permitting an unknown entity to monitor the communications of the Greek Cabinet, US embassy officials and journalists. Vodafone was eventually fined 76 million euros.[430]

- Does the committee and this Parliament, by your actions, endorse requiring CSPs to only purchase equipment, where it is capable of handling 100,000 simultaneous connections, it must also be capable of tapping every individual connection[431], each to 6 agencies,[432] and without the CSP knowing? In effect, that is the position of the Bill.

- Much of the pre-publication rhetoric of the bill focused on obtaining access to Skype calls. However, Skype is now owned by Microsoft,which rebuilt the internal structure of the Skype network in a way that allows lawful access a few months after purchase.[433]

- However, the Home Office maintains that it wants the ability to not only order a foreign provider to respond to information requests, but also to require structural changes to their practices and services, e.g. to order a provider to collect new categories of information. If a national Government can mandate technical interference on private services, it may limit the economy's ability to adapt to a changing market and put the country at a competitive disadvantage.

---

426 http://articles.latimes.com/2012/aug/01/business/la-fi-tech-savvy-olympics-20120801

427 for more details, see the SpamHaus.org project which has been working on this since 1998.

428 https://www.torproject.org

429 https://www.torproject.org/about/overview.html.en#inception

430 http://www.ft.com/cms/4791e25e-8be1-11db-a61f-0000779e2340.html

431 http://www.telesoft-technologies.com/products/network-monitoring-security-control/abis-probe

432 https://www.documentcloud.org/documents/409319-182-vastech-201110-brochures.html

433 http://www.skype.com/intl/en-us/legal/privacy/general/

- Less invasive technologies

- This bill proposes a vast expansion of communications surveillance and would create a situation in which everyone communicating in the UK would effectively be treated as a potential criminal suspect.

- There are numerous examples of other technologies for targeting mobile phones, broadband connections[434] and other communications that are more effective than these measures would be. News reports on undercover police officer Mark Kennedy's infiltration of networks of environmental activists[435] demonstrate that surveillance technologies are already in use. Whether the police are using modified mobile phones and watches,[436] or the more esoteric modified lightbulbs or children's car seats[437] is unknown.

- Though these tools are unfortunately used without oversight, they are not only cheaper but also more targeted - and thus more proportionate - than the proposed law.

- While the precise details of the equipment used in surveillance, under this Bill and under RIPA, may be a mere "technical detail" according to the Home Secretary[438], we invite Parliament to take a greater interest in how the mass surveillance of citizens will operate in practice.

August 2012

---

[434] TraceSpan ADSL intercept solution -- taps a single ADSL line

[435] http://www.guardian.co.uk/environment/mark-kennedy

[436] Griff Communications https://www.documentcloud.org/documents/409250-127-griffcomm-flex8f.html

[437] Elaman https://www.documentcloud.org/documents/409323-186-201106-iss-elaman1.html#document/p21/a69092

[438] Home Affairs Committee - Minutes of Evidence, HC 1939-i, Q79, Theresa May to Julian Huppert: http://www.publications.parliament.uk/pa/cm201213/cmselect/cmhaff/1939/120424.htm

Supplementary Privacy International

Q1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

1. To some extent, the Home Office has been clear about what it hopes to achieve: future-proof legislation that ensures easy access to communications data and is applicable to any form of communication infrastructure that may come to be. It is ostensibly for this reason that the Home Office has proposed the most ambitious communications surveillance legislation we have seen to date, anywhere in the world. PI has been researching communications surveillance policies internationally since 1990, so we are in a relatively unique situation to make such a statement.

2. However, in some respects the Home Office has been extremely unclear. For example, while Part 1 of the Bill would allow the Home Secretary to issue orders to telecommunications operators, we do not have any clarity about what these orders will look like, who they will be issued against, how they will be enforced, how this will affect the technologies and services the orders are applied against, and how this might affect the rights of individuals in the UK and abroad.

Q2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

3. We agree that there is a need to reconsider the powers of government agencies to gain access to data stored by service providers. We also agree that, as technology changes, it is important to continually re-engage in this discussion. We also agree that the fact that communications service providers are not always based within the United Kingdom poses challenges to government agencies wishing to obtain the data they hold.

4. We disagree with the Home Office's choice of policy. We do not believe that the Home Office has made a convincing case for this specific policy. We do not believe that the Home Office has carefully considered the ramifications of this policy from a technological, legal or economic perspective.

Q3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

5. The Home Office has a rich history of proposing technologically advanced surveillance measures that are poorly regulated and technically problematic. In the mid-1990s, the Home Office promoted a policy of restricting the use of encryption - something that is now considered essential to the emerging digital economy in the UK. The Home Office funded the widespread deployment of poorly regulated visual surveillance techniques in that period as well, despite Home Office research revealing that the use of CCTV was failing to reduce crime.[439]

6. The Home Office ensured that Britain was one of the first countries to require the deployment of intercept capability at CSPs, and one of the only countries to do so under a regime of ministerial warrants. The Home Office promoted the policy of communications data retention as a voluntary option in Parliament, only to then pursue a mandatory data retention policy at the European Parliament in the mid 2000s (later brought back to Parliament as an EU Directive). The Home Office also pursued the world's most ambitious identity card programme, ignoring all international and technological expertise, while accusing its critics of being "technically inept".[440]

7. When it comes to surveillance, the Home Office does not have a good track record of pursuing technologically efficient or proportionate policies. We had hoped that, with the shifts in Government rhetoric on civil liberties, the direction of the Home Office would change. However, we see no change in Home Office discourse since this policy was last promoted in 2009 as the 'Interception Modernisation Programme'. Nothing in the draft bill would prevent the implementation of an exact replica of the 2009 policy, with the assistance of a few orders from the Home Secretary. The Home Office had previously

---

[439] Home Office Research Study 292, 'Assessing the impact of CCTV', Martin Gill and Angela Spriggs, February 2005; also see 'CCTV and its effectiveness in tackling crime', House of Commons Library, July 1, 2010.

[440] 'Defence expert undermines Blair on safety of ID cards', David Hencke and Vikram Dodd, Feruary 13, 2006, http://www.guardian.co.uk/politics/2006/feb/13/idcards.immigrationpolicy

proposed a centralised database of information, though this was abandoned in 2009 on privacy grounds. Yet the filtering arrangements within the draft bill appear to create a single interface for widespread access across distributed databases - the fundamental nature of the storage model is the same, whether it is centralised or distributed.

8. This proposal comes at a time when increasing amounts of information is potentially accessible through traditional means. Mobile phone usage has expanded dramatically, and now mobile phone providers hold intimate information on the entire population. When RIPA was still being debated in Parliament, we never imagined a day when the police would be able to identify everyone who has been in a specific geographic area by accessing data held by mobile phone service providers. Open source information is now much more widely accessible because there are greater stores of personal information, gathered both with and without the consent of individuals.

9. It is particularly distressing that while new techniques of surveillance are being devised and deployed in this country, the Home Office is not only failing to properly regulate the use of these techniques, but in fact refuses to discuss them at all. Despite this draft bill being characterized as essential for improving responses to security threats, there is no mention or discussion of the surveillance techniques that are being developed and potentially used domestically without any Parliamentary or judicial oversight. All the Freedom of Information requests we have made to the police about their use of these techniques have been rejected. Such techniques include:

    - The ability of police to remotely access your computing and phone devices. Techniques and products exist that permit the police to infect a computer or a mobile phone with a trojan that allows the microphone and camera to be remotely and covertly switched on, and all activity on the device to be recorded. In essence, this permits the police to maliciously hack a device. We are uncertain as to the legal basis for any such conduct, as prima facie this would likely breach the Computer Misuse Act. In 2008, the German Constitutional Court ruled against the use of trojans by the state of North Rhine-Westphalia, asserting that not only was it a breach of the right to privacy, but a breach of "a guarantee of confidentiality and integrity in information-technology systems."[441]

    - The ability of the authorities to access information on all mobile devices in a given area. Using a device called an 'IMSI-catcher', the police can create a fake cell tower to which all nearby mobile phones will connect. The device would then be able to access the unique identifiers of all the devices, and cross reference them against databases of account-holders. This technique is advertised by the companies who develop the technologies as being particularly helpful for use at large public events and protests. Our request for information regarding the legal status and polices around their use from the Metropolitan Police Service was rejected.[442]

    - The ability of authorities to track individuals by GPS. The use of GPS by police in the US led to the US Supreme Court to rule (United States v. Jones, decided January 23 2012) that the deployment of this technique on an individual's car required a judicial warrant. Our request for information from the Metropolitan Police Service regarding simply the number of GPS devices and the use of this technique, was rejected.[443]

    - The ability of authorities to infiltrate and monitor online social media. A number of police organisations outside the UK have been procuring social media analysis software and this has led to policy responses requiring clear articulation of how this type of surveillance is undertaken, and the

---

[441] Quotation taken from 'Germany's New Right to Online Privacy', Der Spiegel, February 28, 2008, available at http://www.spiegel.de/international/germany/the-world-from-berlin-germany-s-new-right-to-online-privacy-a-538378.html

[442] http://www.whatdotheyknow.com/request/imsi_catcher_guidance#incoming-246590

[443] http://www.whatdotheyknow.com/request/gps_tracker_statistics#incoming-270219

necessary levels of oversight.[444] Our request to the Metropolitan Police Service again asking questions regarding the legal status and polices around the use of social media monitoring was rejected.[445]

10. There are many other techniques for which the Home Office has still not provided any guidance. We await, for instance, the results of our request for information from police agencies about their use of unmanned aerial drones.[446]

Q4. What lessons can be learnt from the approach of other countries to the collection of communications data?

11. Many governments are struggling with updating their laws for the current telecommunications environment, but no democratic country has openly pursued the policy currently being promoted by the Home Office. This could be for a number of reasons:

    - this policy would be against the law in many countries because it allows the monitoring of non-targeted individuals;
    - other countries have not yet held discussions about the modernisation of surveillance techniques for the contemporary and future technological environments;
    - governments have been quietly pursuing the policy without open discussion and debate;
    - some governments already have jurisdiction over the relevant internet services and thus do not require additional surveillance capabilities.

12. Any attempt to compare and contrast policies around the world is fraught with challenges. One could argue that a judicial warrant in one country does not qualify as a judicial warrant in another country. However, it should be noted that some governments have already been rebuked by their courts for not applying the highest standards of protection over the types of data being discussed here, and that no democratic government has pursued the 'black box' DPI policy at ISPs for constant monitoring of data streams in order to identify specific forms of interactions without suspicion. These black boxes were (and still are) used across the Middle East and Northern Africa, more specifically in China, Iran, Kazakhstan, Syria and Tunisia.

13. With respect to the best practices and standards set for rigorous, fair and effective communications policies around the world, such policies generally include:

    - No policy of data retention - in fact, most democracies have rejected or failed to implement data retention policies (e.g. United States has repeatedly debated but not implemented the policy; Australia and Canada have introduced laws to update surveillance techniques but all have excluded the option of data retention; the courts of Bulgaria, the Czech Republic, Germany, and Romania have ruled against data retention laws and there is a case pending at the European Court of Justice, while a number of countries have failed to implement the Directive on Data Retention and there is increasing uncertainty surrounding its value and future.[447]).
    - Due process involving judicial authorities who are competent to review and capable to reject access requests.

---

[444] The Federal Bureau of Investigation decided that its use of social media monitoring will in future be vetted by the agency's Privacy and Civil Liberties Unit. See 'FBI says social media monitoring won't infringe privacy rights', Computerworld, February 14, 2012.

[445] http://www.whatdotheyknow.com/request/social_media_monitoring_policies#incoming-259481

[446] See our request to the Greater Manchester Police, available at http://www.whatdotheyknow.com/request/drone_documenation#incoming-304248

[447] See a report from the Council of the European Union, 'Consultation on reform of Data Retention Directive: emerging themes and next steps', December 15 2011, available at http://quintessenz.org/doqs/000100011699/2011_12_15,Eu_Commission_data_retention_reform.pd f

- A clear and transparent regime of cost and liability distribution that does not insulate institutions from individuals seeking redress.
- Provisions for the service provider to contest requests before a court; this is particularly important when the requests come from other countries.
- Transparency and democratic oversight with annual reports disclosing meaningful information about the extent to which a power is used and under what conditions.
- Notification of individuals when their data has been accessed.

14. This is why other countries have court warrants, judicial authorisations, and notification of surveillance after the fact. The UK remains one of the only democratic countries with ministerial interception warrants. The UK's self-authorising access regime for communications data continues to surprise experts around the world.

15. All this data should lead us to conclude that we must improve our regime for communications surveillance. The situation has never been more urgent: we are seeing many developing countries directly replicating UK surveillance laws. It is essential that the UK not act as an enabler of poorly regulated surveillance and technologically ambitious schemes. We have already seen indications of abuses of such powers both in the UK and internationally, including:

- in 2008, Liverpool Council was investigated after officials went through the mobile phone records of the opposition leader (monitoring links between police and journalists for leaks)[448]
- in 2006 Suffolk Police accessed the mobile phone records of a journalist to find out how he had obtained information regarding a historic inquiry[449]

16. However, because there is a general lack of transparency and notification, we are unable to properly identify all the cases of abuse. The international experience indicates that the frequency of abuses may be significantly higher. As examples:

- an Albertan regulatory board was caught spying on opponents[450]
- Azerbaijan used communications data to identify everyone who had voted for Armenia in the Eurovision song contest[451]
- DeutscheBahn executives resigned after being caught monitoring employees' communications to see who was speaking with journalists and members of Parliament;[452]
- Deutsche Telecom was also caught spying on journalists' communications with senior executives[453]
- Vodafone was caught monitoring its directors' communications[454]

---

[448] 'Phone records search investigated', BBC News, June 18, 2008, available at http://news.bbc.co.uk/1/hi/england/merseyside/7461819.stm

[449] 'Reporter's telephone calls probed', BBC News, December 1 2006, available at http://news.bbc.co.uk/1/hi/england/norfolk/6200410.stm

[450] Montana investigating Alberta energy board spying allegations, CBC News, August 23 2007, available at http://www.cbc.ca/news/canada/edmonton/story/2007/08/23/montana-spying.html?ref=rss

[451] 'Azerbaijan authorities interrogate music fans in Eurovision probe', 18 August, 2009, http://www.guardian.co.uk/music/2009/aug/18/azerbaijan-authorities-interrogate-music-fans

[452] 'German rail boss quits over spying claims', Daily Telegraph, March 31 2009, http://www.telegraph.co.uk/news/worldnews/europe/germany/5079165/German-rail-boss-quits-over-spying-claims.html

[453] 'Telekom Accused of Tracking Journalists' Mobile Phone Signals', Der Speiegel, May 30, 2008, http://www.spiegel.de/international/business/spy-scandal-grows-telekom-accused-of-tracking-journalists-mobile-phone-signals-a-556741.html

[454] 'Vodafone spied on its top bosses', ThisisMoney, June 1, 2008, available at http://www.thisismoney.co.uk/money/markets/article-1632040/Vodafone-spied-on-its-top-bosses.html

- the German foreign intelligence service spied on reporters' communications[455]

17. Most telling are cases in which the data was accessed without adequate oversight. When the US decided to exceptionally grant the FBI powers of self-authorised access to communications data solely for the purpose of national security investigations, many problems ensued. According to the FBI's Inspector General, these included failing to report accurate numbers to Congress,[456] single 'letters' actually requesting information on large numbers of people (9 such requests accessed the subscriber information of 11,100 different telephone numbers),[457] and significant and numerous abuses and errors, even more than reported by the FBI.[458]

18. This US surveillance regime was repeatedly revisited and debated in Congress, and has been curtailed to some extent. Most distressing is that the National Security Letter regime still has stronger oversight than the general policing approach to communications data retention in the UK; the NSL regime is now restricted to national security cases and has some processes for internal review, which led to extensive debates in Congress. Despite significantly lower standards in the UK and the use of similar powers for all forms of surveillance, RIPA has not seen similar legislative review and oversight.

Q5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

19. Direct requests to the service providers for their customers' data is always a preferred approach. We accept that many of these may be based outside of the UK. A legal process must be developed that matches the needs of international service providers. They require that requests are compliant both with UK and their own domestic laws. The standards for requests in the United States, for instance, are significantly higher in general and serious crime policing, and we should, at a minimum, match these standards.

20. We are working closely with international industry leaders, technology, legal and security experts to devise best practices on the processes for cooperating with government requests. It is a long and thorough consultation process. Meanwhile, this draft bill is evidence of what happens when there is a lack of consultation -- in our discussions with various sectors of industry in the UK and abroad, they all contend that they had not been contacted by the Home Office at any point about this policy prior to this draft bill.

21. Not getting this process right will stunt our communications abilities for the future. When information exists that is directly relevant to an ongoing investigation just measures must be applied to allow for access, and this access may indeed be across borders using faster mutual legal assistance processes that are able to ensure compliance with the laws in both jurisdictions. These are not new problems -- from lex mercatoria to anti-terrorism policy, we have all been struggling to find new and equitable solutions across jurisdictions. The Home Office is currently proposing to railroad these conventions and redesign communications infrastructure in their own interests.

Q6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

22. An overarching piece of legislation has drawbacks. The Data Retention Regulations relate to the EU Directive which will be reviewed imminently. Once that review is complete, changing the regulations would be far easier than revisiting the legal framework in its totality.

---

[455] 'BND Agents 'Knew what they were doing'', Der Spiegel, March 25, 2008 http://www.spiegel.de/international/germany/the-world-from-berlin-bnd-agents-knew-what-they-were-doing-a-549765.html

[456] As many as 4600 requests were not reported according to the Office of the Inspector General Report, March 9, 2007.

[457] 'Report Details Missteps in Data Collection', R. Jeffrey Smith, Washington Post, March 10, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/03/09/AR2007030902353.html

[458] See p 95 of the Department of Justice, Office of Inspector General, A review of the FBI's use of National Security Letters in 2006, March 2008. For a helpful analysis of the problems, please see http://www.aclu.org/files/images/nationalsecurityletters/asset_upload_file41_34805.pdf

23. But the advantage of a single framework is that it will combat political uncertainty. One of the challenges that arose with the Anti-Terrorism Crime and Security Act, and later the Data Retention Directive, was that the purpose of communications data retention was to combat serious crime and terrorism, but access to the data was governed by RIPA, which allows generalised access to data held by communications service providers. This created an uncertain regime of law in which a pool of information intended for the purposes of combatting terrorism, was accessed under a law drafted for more general purposes, one subject to less stringent constraints. Policy deliberation for data retention was focused on serious crime and anti-terrorism, and ignored the use of this information for broader purposes.

Q7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

24. No. Considering the evidence given to the committee to date, there has already been so much discussion about the existing problems within RIPA that only a root-and-branch review of RIPA would fix the problems with the vast data stores that the authorities already access, so any consideration of new information sources is immediately problematic.

25. Of course, one could argue that if RIPA is redrafted to require judicial authorisation for requests for traffic data, then this would go some way to fixing the problems with communications surveillance in this country.

Q8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

26. We strongly recommend that the Committee reviews the responses from organisations such as COADEC - the Coalition for A Digital Economy. If a new service provider based in this country develops a new form of communication, it faces a significant risk of being placed under an order from the Home Secretary to change key components of that service. Failure to do so will mean that all their customers' communications will be interfered with by UK ISPs. This is not a reasonable choice for small organisations with limited capacity to meet the legal and technical requirements of the Home Secretary.

27. However, this legislation would not only have implications within the United Kingdom. If the Home Secretary wished to place an order on a foreign provider of communications services, that provider would have to perform the same calculations regarding their UK user base.

Q12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

28. The focus should not be on which agencies, but rather on which purposes and which authorisation and oversight regime applies. Any government agency could have a reason to access communications data, perhaps even better reasons than the police. The focus should be on the locus of the decision-making on whether the request is proportionate and necessary in a democratic society. Our current regime is wholly inadequate for making these decisions, and this is in large part due to Parliament failing adequately to address these questions, leaving it to the authorities to self-authorise.

Q13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

29. The problem isn't just that it is unrealistic; it also places UK users at a disadvantage over users from other countries. As it is, many of these foreign service providers are not necessarily aware that their users are based in the UK. Under this draft bill, they would have to identify all their UK users and then place additional surveillance measures against them, e.g. collect and retain additional information just on UK users. If they failed to do so, the service providers would risk their users' information being collected and processed in ways that are beyond their control.

Q14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

30. The nature of the access sanctioned by this legislation is neither appropriate nor proportionate.

31. In our review of the surveillance technology industry,[459] we have found many 'black boxes' that are capable of conducting directed surveillance of large numbers of people simultaneously. Some companies are selling black boxes designed to conduct illegal mass surveillance. What the Home Office envisions is in the same vein: technology that is capable of monitoring all streams of data in order to identify specific types of communications that must then be picked apart to identify specific communications data.

32. As an example, consider Facebook (or any other type of social media service). The structure of users' interactions with Facebook's servers is such that the black boxes will necessarily have to intercept all communications data in order to gain access to traffic data. RIPA currently states that when a user is surfing to //www.facebook.com/ajax/messaging/send.php, the 'communications data' is 'http://www.facebook.com', but for the police to gain access to anything after the first '/' would require an interception warrant. What the Home Office is proposing would involve self-authorised access extending well beyond that first '/'.

33. Moreover, the black boxes would have to monitor all traffic to Facebook.com and go into detail about the content of the communications between the user's browser and the Facebook servers in order to identify when that user is messaging someone else. In order to identify the relevant information of who is messaging who, the black boxes would have to read across various interactions with Facebook servers because they are not always easily accessible within a single set of communications. The Home Office does not believe that this would amount to interception of communications, as it maintains that the authorities are capable of ignoring anything that looks like the content of the direct message while the technology delves into the details of the interactions with the server. In effect, we have to accept a promise that, while law enforcement is collecting and reconstructing the totality of our interactions with Facebook, they will scrupulously ignore the content of the message, and that no change to Facebook, operating independently without knowledge of what the UK Government is doing, will break this assumption and cause illegal monitoring.[460]

34. Again, the issue is not about 'what kind of crimes', nor 'which kind of agencies'. The question is: who makes the decision about what is proportionate and necessary? At the moment the very people who want to gain access to this information are the ones doing so. We cannot believe that in the 12 years since RIPA was approved, and even under previous legal regimes, this situation has been deemed acceptable by Parliament. Even the introduction of independent authorisation is only a first step - magistrates and judges need to be provided with sufficient training, information and a clear legal regime upon which to base their adjudication of what is necessary and proportionate. Transparency in reporting and review must also be more thorough, and include notification to the individual when the investigation is complete. The fact that we can't even identify how many people have had their information accessed by various agencies under RIPA over the years is unacceptable in a democratic society.

Q15. Is the proposed 12 month period for the retention of data too long or too short?

35. The indiscriminate retention of any information on innocent individuals beyond the time period required for delivering a communications service is too long.

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

36. As discussed above, this is not satisfactory. The assent of a single police officer does not classify as a safeguard. Independent authorisation by an informed, empowered and accountable body is necessary to ensure that the request is necessary in a democratic society and proportionate. We are not as concerned about compliance with Article 8 as we are concerned that the UK Parliament has thus far failed to implement safeguards that have been called for since the 1930s. According to the history of surveillance in

---

[459] See our separate submission to the Joint Committee entitled 'Implementation Briefing', August 23, 2012.

[460] See https://www.privacyinternational.org/blog/facebook-message-anatomy for a longer discussion of this point.

the UK provided by the Birkett Committee report (a Privy Council Committee report written in 1957), the Home Secretary in 1937 decided that ministerial warrants should be required for communications data. In the Malone case in 1979, the judge asked that Parliament come up with a better system for communications surveillance regulation, stating: "I would have thought that in any civilised system of law the claims of liberty and justice would require that telephone users should have effective and independent safeguards against possible abuses." When Malone arrived the European Court of Human Rights, the court ruled that "the exercise of such powers, because of its inherent secrecy, carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole. This being so, the resultant interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse." We do not believe that our current framework, nor the one proposed by the Home Office, achieves these objectives.

Q17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

37. Yes a warrant system applied to RIPA would be more appropriate. Yes it should apply to all agencies, and necessary in all circumstances. We do not understand why it has taken so long to even ask this question.

Q18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

38. The two Commissioners should be thought of as a final set of safeguards once we have a clear and open communications surveillance regime and a clear delineation of which services it applies to, in which companies can contest the orders and requests, orders are deliberated upon openly and requests for access authorised by independent and knowledgeable bodies.

Q19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

39. No. We do not understand how Parliament can meaningfully review this draft Bill without understanding what an order from the Home Secretary may actually look like, particularly as we have no idea which new communications technologies we will be using in the near future.

40. Whether the police should be able to routinely access company databases is a question that should be debated and discussed in public and in Parliament. It should not be done behind the scenes in clause 2 of a bill without public consultation. The Home Office is proposing a system that would allow a police constable to generate a list of every owner of a mobile telephone in Glasgow, Manchester and London at particular times. The records of anyone who happened to fall into this category would be accessed. Parliament should not deceive itself that it will have any oversight over such processes.

Q25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?

41. It's not a matter of circumvention alone. The internet is not being built for the sole purposes of the Home Office; it is being built upon every day to create a more secure environment where individuals and organisations can find the various levels of protection, assurance and confidence they require for particular transactions. Businesses are routinely using encryption services because of due diligence requirements, and these same services that frustrate malicious entities seeking unlawful access to sensitive information may also frustrate the Home Office. Similarly, individuals are increasingly using security techniques, sometimes unknowingly, to protect their information. The Home Office either wants to undo all these security and privacy developments, create back-doors into them, or strip them out in ways that will reduce everyone's confidence in these services. At the moment, when an individual transacts over a service with a specific provider, that individual believes that he or she is transacting only with that provider. The Home Office wants to introduce a panoply of other entities into that communications process, thereby ensuring that no one can ever be certain as to where their personal information resides. Put more simply, if someone communicates with a friend and then deletes that communication the next day, not only will the social-networking service retain this information, but any number of UK service providers may also collect and store it and provide access to a myriad of government agencies far beyond the control of any of the entities involved in the original communications transaction.

Q26. Are there concerns about the consequences of decryption?

42. Even after consultation with leading security experts from around the world, we continue to be perplexed by the Home Office's belief that they can circumvent encryption in a way that is computationally feasible and that wouldn't destroy the nation's confidence in internet security.

August 2012

Marisha Ray

Context of this evidence

During 2005 I chaired a council scrutiny committee which investigated the use of CCTV in England and took evidence not only from organisations which promote civil liberties in our society from which you have heard or will be hearing, but also from three CCTV control centres outside London, in England, and a greater number within London. While the data gathered in those cases may not correspond exactly with the data which is your primary interest, I and that committee did gain an insight into the attitudes of police, council and other staff up and down the country to privacy, civil liberties, requests for data by the police and data protection issues in general. In particular we had close contact with relatively junior staff and were able to quiz them gently, ask about their training and judge their attitudes to their work. I have been urged by some former members of that committee also to write to you today.

From 2006 to 2008 I was a council executive member, also known as council cabinet member in some local authority areas, with responsibilities which included community safety, public protection, procurement and the performance management of all council services in an inner London borough (Islington), with the third most significant level of deprivation of all London boroughs, a diverse community both ethnically and in most other respects and a great variety of socio-economic groups living in integrated, mixed communities not in separation as is seen in some other areas including parts of London. Our borough prided itself on the way that it tackled community safety issues in the area with novel solutions working with all who could potentially have an impact on those solutions, including local residents and members of our local community including those who work in the area, people of a wide variety of faiths and their representatives, local, regional and central government agencies including police and fire services, local businesses, the local press, researchers in criminology from London's universities and voluntary sector organisations and other individuals and groups who wished to contribute. We used a wide spectrum of means including the implementation of a CCTV scheme and a combined scheme to enable help to be summoned, therefore I would claim that we had some experience of the controlled and measured use of surveillance in public space at the local level.

I write also as someone who can be visibly identified as a member of a minority ethnic group, who is female, who has spent most of her life in London and who was the mother of a toddler while a councillor, which gives a different experience of the local community and seems to bring with it a kind of intimacy that crosses all social divides. In addition members of my family in another country have been involved in the legal representation of minority communities and individuals from those communities, often from faiths which feel persecuted in that country and also in our country, and therefore I believe I may be more sensitive to these issues here.

My career outside local and regional politics has been principally in the IT industry both as a consultant and in a corporate IT department working in both cases with teams and systems which covered many countries though mostly based in the UK, but on occasion elsewhere as well; and this is an additional reason why I am responding today. I retain links to the industry and to those who work in the communications and telephony industries. I have also had the benefit of having lived in France on three separate occasions during the past 20 or so years and have lived in rural, provincial urban and Parisian environments for over 2 years in total working in the IT industry there too.

Comments

On social changes which have taken place recently facilitated by information technology
While it has been said that all the world is at six degrees of separation, in other words that from friends and friends of friends and onwards through that chain we are connected with the whole human population of the world within six steps, it was announced recently and plausibly that that number is decreasing because of information and communication technology and that the chain continues to decrease. In addition there is a change in the way people behave in that they may well be more likely to help, advise or recount their experiences to people whom they made contact with or had introductions from by electronic means. I ask the committee here, how meaningful is the data that the committee proposes should be made available through surveillance by

this draft bill? What conclusion if any, in an age of access by one individual to much of the human race, can be drawn from the fact that two individuals have been in communication or contact? Much of the change in interactions which was foretold by the book The Cluetrain Manifesto in its first chapter in how individuals interact with large organisations has indeed taken place, however these changes apply not just to commercial organisations as discussed in the book, but across the board to all organisations and most individuals who have access to modern communications technology. I question for how much longer the data which you propose to collect will continue bring benefit. Please look to the obsolescence of the measures which you propose to put in place and how widely they should therefore be used.

In addition I urge you to consider the fact that several million warrants have been issued under RIPA, well over half a million in a single recent year and given the scenario I have described above it is easily possible for any measures you put in place to be used excessively too and like RIPA far beyond the scope for which they were originally, publicly promulgated. I appreciate that you are, in this draft bill putting measures in place to prevent that, and yet what bodies are you putting in place to challenge those who overstep the mark and what confidence do you have that they will prove effective regulators. There are some powers which you should withold on the basis that on existing form those who apply for warrants have shown that they will do so excessively and not keep to the spirit of the law, but aim for the letter of a poorly regulated area, which may well prove impossible to regulate effectively within the resources which you have at your disposal.

In addition in Malcolm Gladwell's book the Tipping Point we see that there are certain individuals who have contact with a far larger number of individuals than others, he calls them the connectors. While you may or may not accept other conclusions of his book, it is true that such individuals exist, that they are influential, and that many successful politicians are or were amongst their number. Therefore any large scale attempt at surveillance of their data will necessarily include an overly large proportion of data concerning such people, amongst them politicians. It is therefore necessary to bear this in mind when extending powers of surveillance, particularly as the objective of the powers is to uphold democracy and not to snoop into the processes which allow the democratic process to be meaningful. It should also be borne in mind that people become more hesitant or more cautious to communicate frankly and freely, speaking their minds, with people whose communications they believe might well be monitored.

On effects on local communities and individuals and on crime prevention and reduction
In the field of crime reduction and crime prevention, particularly when struggling to tackle issues such as domestic violence or other forms of abuse, which affect all communities, it is key that people believe their communications are truly confidential; not only the content of their communication but also the fact that they have made any contact at all. An increase in the level of monitoring may have a positive effect on fighting some sorts of crime, but also have a negative effect on other sorts. The other sorts are sorts which need even greater focus and have an important impact on families, children and often women in particular, groups whose interests are under-represented in our imperfect democracy and whose wellbeing may not be as well served in a political establishment where other groups are more dominantly represented. Merely increasing the culture of surveillance of private communication in our country will be a step backwards in working to reduce crimes of this sort which take place in secret hidden from view. The types of crime of which I write lead to the death of approximately 100 women each year in our country and are typically preceded by several years of events which if reported in confidence might well lead to measures being put in place which would save those lives. However while I quote that statistic that is not the only type of crime which is more likely to be reported in an environment where privacy is assured and the individual can make a decision about the pace at which they proceed; it is an illustration of a more general point.

During 2005, while taking evidence with other members of the committee investigating the use of CCTV surveillance in England, I took the opporutnity to ask may questions both on the use of CCTV and the regulation of surveillance not as it stood in law, but as it was practically implemented by the people carrying out that surveillance. I was struck at the time by how poorly regulated surveillance with cameras is, and have no reason to believe that I should have any greater confidence in the regulation of any other form of surveillance in this country. Relatively junior members of staff from whom in many cases we took evidence felt no real

authority to say no to the police or other agencies or to question the need for data. I see that in this draft bill you propose that more senior staff should have greater control over the processes, however given the volume of warrants which are issued I question whether any single member of staff will without fail give the matter of whether a warrant is justified or not the attention which it deserves. The attitudes of senior members of staff in all organisations to civil liberties and privacy varies, often as a function of their own political views and persuasions; and it is questionable that without training in this area and moderation and standardisation of their actions across the country, merely appointing a senior member of staff alone would serve your purpose. In addition, without spot checks- in depth investigations in randomly chosen cases and widespread knowledge that such checks will take place as a matter of routine in a substantial number of cases- I question whether any mechanism would provide an effective check or balance to the tendency to just wave through all warrant applications without question in the way that I was led to believe was already taking place. There was no possibility that the person whose privacy was intruded upon would find out about or have the capacity or right to take action for the issue of an inappropriate warrant, thus there was a negligible chance that those acting upon the warrant or those applying for it would face consequences and indeed the issue of the consequences of failing to question the grounds for issue of a warrant was never raised with me even though the taking of images at a known time and place on public and potentially private property is undoubtedly intrusive.

Writing as a member of a visible minority ethnic group, who has spent most of her life in London and who was a local councillor from 2002 to 2010 in one of the most deprived and in almost every way diverse boroughs in London, I believe that the excessive and widespread use of surveillance as enabled by RIPA 2000 has a corrosive effect, creating groups or communities well aware that they are monitored or likely to be monitored and groups or communities less aware of this and dividing us into those who are wary to communicate because of the potential for communications to be taken as evidence of some unforeseen and unintended intent who feel vulnerable, and those who are confident of the ability to defend ourselves in that event perhaps because we are more articulate or have the resources to command others who are.

I also believe on the basis of what I have seen since 2005 that attitudes to privacy, surveillance and intrusion both physical and electronic differ and that those differences do correlate with, though they may not precisely follow: the sex of the individual, the cultural background of the individual, the family or domestic circumstances and relationships of the individual and their religious background. The equality impact of surveillance is too little researched and too little known and of crucial importance to the cohesion of our society, which is key to the stated aims of this draft bill in its foreword. It is in my opinion important that you satisfy yourselves that the measures you propose would not have too great a differential impact, particularly on those groups most likely to be vulnerable, least likely to have access to your committee and most likely to feel marginalised by our society. Our legal system is complex and for some who are new to this country or who lack the capacity to understand it, its systems, regulations and institutions, there is the feeling that in depth surveillance will inevitably lead to the revelation of areas where they have unwittingly omitted to obey regulations or to discharge duties fully. Thus people who are not entrenched in our society, in the way that most people of all backgrounds in politics do tend to be, feel doubly vulnerable to any increase in surveillance even if they have no particular reason to do so.

On IT issues

I have worked in software development and consultancy, in the procurement of IT contracting services, as a member of the boards or governing bodies of a number of organisations in different sectors and as an adviser to the board of an NHS Trust where IT issues have been regularly raised including issues about privacy and confidentiality. Software is often developed in an organic fashion, meaning that systems are improved and changed while in use. To be entirely confident about the data generated one would have to have perfect tracking of the version and system which generated that data. To be entirely reliable the software would need to be tested to a degree and specification which it is unlikely would be strictly necessary for a mobile phone company, because there is no safety or other requirement to do so. Data on time and position from mobile phone signals is not always of a quality to be entirely reliable, and while it may be useful in attempting to locate a person in need, it is not necessarily consistently of the quality needed to be used as evidence in court. When taking evidence I suggest that you enquire about the quality of the data which is being generated. If the data is not of sufficient quality to be useful for the purpose intended there is little point in forcing its retention in large

quantities for a year, over a period of many years at some considerable cost. It is also unlikely that a commercial or other organisation will volunteer the fact publicly that its data and processes of software development are not entirely reliable because of the potential reputational damage to the organisation, therefore without incisive questioning this issue will not emerge. Data quality is a persistent issue in all large organisations using IT systems, and I imagine that if the data is for use by the services named its accuracy is far more of an issue.

IT development projects in large organisations often use large numbers of contractors and employees from several organisations based in many different countries. Telephony is no exception to this. As in other sectors, the tendency is to arrange for as many as possible who are involved, to sign non-disclosure agreements (NDA's), however detailed inspection of such NDA's does call their effectiveness into question. These agreements sometimes put conditions on those who sign them which could not possibly be upheld if they are to carry out their jobs, and in addition the sheer number of people signing them means it would be near impossible to work out fromwhere any leakage of privileged information had come. I would question whether it is really in the UK's interests to put together databases holding such information which people in potentially any country with any background whatsoever might gain access to. What sanction could be placed upon the people developing the system, accessing live data and potentially giving unauthorised access to others; is it in fact wise to have it in the keeping of a commercial organisation with employees of third party organisations who are may not be aware of any individual sanction which they would face in the event of misconduct?

As someone who has worked with IT contractors, my feeling is that the nature of the agreements to ensure that the data was secure would be complex, costly and the cost not accurately predictable because it would be too much a function of the level of security which was required. Inevitably it would not be politicians, but others who would specify the level of security required, and that level might well be far lower than that which politicians and the public would call for. I do request that on our behalves you insist that you as our representatives are kept fully informed of any compromises which have been reached, any corners which have had to be cut and that you put in place some arrangements to call a halt to projects which do not fit the standards which you yourselves consider acceptable. This is common if not the norm in the private sector, and needs to be the case in the public sector too, particularly when considering sensitive data. I am not aware of a mechanism in parliamentary procedure which allows for such an objective to be achieved and would suggest that it is important for the better management of public IT projects. Accurate forecasting both of cost and of security arrangements in such systems which are hosted externally is far more difficult than arranging security of systems hosted by our own public services. There is much room for misinterpretation and arrangements for public scrutiny would be complex and the workforce involved is often unstable with some personnel being rotated between customers and teams giving far too many people access to systems and data. While I have made generalisations which might not be true in every case, they are certainly true in some cases of which I am aware.

I would advise that the security requirements on real time data providing information on the position of specific individuals be considered carefully. The data would undoubtedly be useful to criminal adversaries of for example any criminal whose whereabouts happened to be being tracked and therefore would necessarily lead to the potential for future corruption, even if there is no likelihood of such corruption at present. This draft presents the perverse incentive for real time data to be inappropriately sought, too carelessly allowed and then corruptly sold. Such data is clearly a significant intrusion into a person's privacy, may put their personal safety at risk if insecure or accessible to large numbers of people. I know from my work on CCTV which records both identity and location, that this is a significant concern to many and I suggest that you engage in a wide and public debate on this issue at a time of year which is more conducive to such matters, as opposed to this call for evidence which has come in July and August. I would suggest that every single occasion of use of real time data should be independently scrutinised and that adequate arrangements be put in place for review of this system of scrutiny.

When you consider the question of data security, please also consider the question of the effectiveness of high level scrutiny in detecting the presence of wrongdoing sufficiently rapidly to prevent harm, particularly when the team of people working on these systems may involve staff based globally with a highly networked structure of teams. My initial reaction is that it is not possible for such scrutiny to be effectively organised, and though it may be that others will express views to the contrary, it is equally possible that they stand to gain directly or

indirectly from holding a contrary view. It is now also a regular occurrence for private information to be accidentally emitted by large organisations. I have not as yet seen any account of a failsafe method for preventing the types of human error which lead to this, therefore for each piece of data which you consider retaining here you might well imagine that one day that data will be made public and it is on that basis that it is being stored.

Thank you for your patience in reading this submission. I will be happy to supply further details or explanations of any of the remarks made here if necessary.

August 2012

J Richardson

Answer to Question 1 :- No. I am convinced the great majority of people are unaware of what the Bill would mean if it becomes an act. Not enough independent publicity and time has been given in order to enlighten the mass of the public about the intrusion this act will have on their privacy and freedom.

Answer to question 2:- No. Speak to the ordinary man in the street and you will soon realize they know very little about what is going on with regard to their privacy and freedom if the bill becomes law.

Answer to question 4:- Already the medium sized town where I live has in excess of 550 CCTV cameras capable of monitoring the activities of anyone 24/7, proven criminal or not. The victim's visits to Hospitals, shops, Hairdressers, their local pub, Post Office on Public Transport,a walk in the park,the cinema and theatre, and other places can all be watched.
The list seems without end. Even his or her activities around their own home are reported back to the local Neighbourhood Watch contact, encouraged to do so by the Police or Local Authority Technocrats. So we have a snoopy, hush-hush situation where neighbour spies on neighbour, rather than the intended strangers and intruders for what they were first intended to do.Causing problems amongst the local community.

Try to get a little privacy by taking by taking a run out in your car to the country for a picnic, you will not get away with it the police and DVLA will have your details, car and all, on their Data Bases.

I am 84 and remember well the information that came out of Nazi Germany about the covert, oppressive and cruel regime that existed there before and during WW2. The set up was very similar to that which exists in this country today.

Comments on question 12:-Access to information gathered by covert means should be treated as highly confidential.

There have been too many instances up and down the country of Police and Local Authority Technocrats abusing the system by using the information gathered , for their own personal use. The number of abusers is in the hundreds , and that is only from a few forces u. Goodness knows what the total from all forces would be.

The law as it stands is more than adequate to deal with the amount of terrorism that occurs in this country. Anti Terrorism Laws introduced as a safeguard are counter productive, and will when used reduce the freedom and privacy of all.

August 2012

Duncan Roy

The proposed Communications Data Bill raises significant issues – issues connected with human rights, privacy, security & with the nature of our society. These issues are raised not by the detail of the bill but by its whole being. Addressing them would, in my opinion, require such a significant re-drafting of the bill that the better approach would be to withdraw the bill in its entirety and rethink the way that security and surveillance on the Internet is addressed.

As noted, there are many issues brought up by the draft bill: this submission does not intend to deal with all of them. It focuses primarily on three key issues:

1) The nature of internet surveillance. In particular, that internet surveillance means much more than 'communications', partly because of the nature of the technology involved and partly because of the many different ways in which the internet is used. Internet surveillance means snooping not just on correspondence but social life, personal life, finances, health and much more. Gathering 'basic' data can make the most intimate, personal and private information available and vulnerable.

2) The vulnerability of both data and systems. No data or system can ever be made truly 'secure'. The evidence of the past few years suggests precisely the opposite: those who should be most able and trusted with the security of data have proved vulnerable. The Communications Data Bill fails to take proper account of that vulnerability and sets up new and more significant vulnerabilities, effectively creating targets for hackers and others who might wish to take advantage of or misuse data.

3) The risks of 'function creep'. The kind of systems and approach envisaged by the draft Bill makes function creep a real and significant risk. Data, once gathered, is a 'resource' that is almost inevitably tempting to use for purposes other than those for which its gathering was envisaged.
I am making this submission in my capacity as a non-practising barrister and legal blogger with a strong interest in techie matters. To describe the government's competence with technical matters is to roll on the floor laughing. Virtually no government in the world seems capable of understanding the key issues or procuring the correct solutions. You are no different. With every step you create new problems for yourself and for us.

1 The Nature of internet Surveillance
As set out in Part 1 of the draft bill, the approach adopted is that all communications data should be captured and made available to the police and other relevant public authorities. The regulatory regime set out in Part 2 concerns accessing the data, not gathering it: gathering is intended to be automatic and universal.
Communications data is defined in Part 3 Clause 28 very broadly, via the categories of 'traffic data', 'use data' and 'subscriber data', each of which is defined in such a way as to attempt to ensure that all internet and other communications activity is covered, with the sole exception of the 'content' of a communication.
The all-encompassing nature of these definitions is necessary if the broad aims of the bill are to be supported: if the definitions do not cover any particular form of internet activity (whether existent or under development), then the assumption would be that those who the bill would intend to 'catch' would use that form. That the 'content' of communications is not captured (though it is important in relation to more conventional forms of communication such as telephone calls, letters and even emails) is of far less significance in relation to internet activity, as shall be set out below

1.1 'Communications Data' and the separation of 'content'
As noted above, the definition of 'communications data' is deliberately broad in the bill. On the surface, it might appear that 'communications data' relates primarily to 'correspondence' – bringing in the ECHR Article 8 right to respect for privacy of correspondence – and indeed communications like telephone calls, emails, text messages, tweets and so forth do fit into this category – but internet browsing data has a much broader impact. A person's browsing can reveal far more intimate, important and personal information about them than might be immediately obvious. It would tell which websites are visited, which links are followed, which files are downloaded – and also when, and how long sites are perused and so forth. This kind of data can reveal habits, preferences and tastes and can uncover, to a reasonable probability religious persuasion, sexual preferences,

political leanings etc, even without what might reasonably be called the 'content' of any communications being examined – though what constitutes 'content' is contentious.
Considering a Google search, for example, if RIPA's requirements are to be followed, the search term would be considered 'content' – but would links followed as a result of a search count as content or communications data? Who is the 'recipient' of a clicked link? If the data is to be of any use, it would need to reveal something of the nature of the site visited – and that would make it possible to 'reverse engineer' back to something close enough to the search term used to be able to get back to the 'content'. The content of a visited site may be determined just by following a link – without any further 'invasion' of privacy. When slightly more complex forms of communication on the internet are considered – e.g. messaging or chatting on social networking sites – the separation between content and communications data becomes even less clear. In practice, as systems have developed, the separation is for many intents and purposes a false one. The issue of whether or not 'content' data is gathered is of far less significance: focussing on it is an old fashioned argument, based on a world of pen and paper that is to a great extent one of the past.

What is more, analytical methods through which more personal and private data can be derived from browsing habits have already been developed, and are continuing to be refined and extended, most directly by those involved in the behavioural advertising industry. Significant amounts of money and effort are being spent in this direction by those in the internet industry: it is a key part of the business models of Google, Facebook and others. It is already advanced but we can expect the profiling and predictive capabilities to develop further.

What this means is that by gathering, automatically and for all people, 'communications data', we would be gathering the most personal and intimate information about everyone. When considering this Bill, that must be clearly understood. This is not about gathering a small amount of technical data that might help in combating terrorism or other crime – it is about universal snooping and profiling.

1.2 The broad impact of internet surveillance
The kind of profiling discussed above has a very broad effect, one with a huge impact on much more than just an individual's correspondence. It is possible to determine (to a reasonable probability) individuals' religions and philosophies, their languages used and even their ethnic origins, and then use that information to monitor them both online and offline. When communications (and in particular the internet) are used to organise meetings, to communicate as groups, to assemble both offline and online, this can become significant. Meetings can be monitored or even prevented from occurring, groups can be targeted and so forth. Oppressive regimes throughout the world have recognised and indeed used this ability – recently, for example, the former regime in Tunisia hacked into both Facebook and Twitter to attempt to monitor the activities of potential rebels.
It is of course this kind of profiling that can make internet monitoring potentially useful in counterterrorism – but making it universal rather than targeted will impact directly on the rights of the innocent, rights that, according to the principles of human rights, deserve protection. In the terms set out in the European Convention on Human Rights, there is a potential impact on Article 8 (right to private and family life, home and correspondence), Article 9 (Freedom of thought, conscience and religion), Article 10 (Freedom of expression) and Article 11 (Freedom of assembly and association). Internet surveillance can enable discrimination (contrary to ECHR Article 14 (prohibition of discrimination) and even potentially automate it – a website could automatically reject visitors whose profile doesn't match key factors, or change services available or prices based on those profiles.

2 The vulnerability of data
The essential approach taken by the bill is to gather all data, then to put 'controls' over access to that data. That approach is fundamentally flawed – and appears to be based upon false assumptions. Most importantly, it is a fallacy to assume that data can ever be truly securely held. There are many ways in which data can be vulnerable, both from a theoretical perspective and in practice. Technological weaknesses – vulnerability to 'hackers' etc – may be the most 'newsworthy' in a time when hacker groups like 'anonymous' have been gathering publicity, but they are far from the most significant. Human error, human malice, collusion and corruption, and commercial pressures (both to reduce costs and to 'monetise' data) may be more significant – and the ways that all these vulnerabilities can combine makes the risk even more significant.

In practice, those groups, companies and individuals that might be most expected to be able to look after personal data have been subject to significant data losses. The HMRC loss of child benefit data discs, the MOD losses of armed forces personnel and pension data and the numerous and seemingly regular data losses in the NHS highlight problems within those parts of the public sector which hold the most sensitive personal data. Swiss banks losses of account data to hacks and data theft demonstrate that even those with the highest reputation and need for secrecy – as well as the greatest financial resources – are vulnerable to human intervention. The high profile hacks of Sony's online gaming systems show that even those that have access to the highest level of technological expertise can have their security breached. These are just a few examples, and whilst in each case different issues lay behind the breach the underlying issue is the same: where data exists, it is vulnerable.

Designing and building systems to implement legislation like the Bill exacerbates the problem. The bill is not prescriptive as to the methods that would be used to gather and store the data, but whatever method is used would present a 'target' for potential hackers and others: where there are data stores, they can be hacked, where there are 'black boxes' to feed real-time data to the authorities, those black boxes can be compromised and the feeds intercepted. Concentrating data in this way increases vulnerability – and creating what are colloquially known as 'back doors' for trusted public authorities to use can also allow those who are not trusted – of whatever kind – to find a route of access.

Once others have access to data – or to data monitoring – the rights of those being monitored are even further compromised, particularly given the nature of the internet. Information, once released, can and does spread without control.

3 Function Creep

Perhaps even more important than the vulnerabilities discussed above is the risk of 'function creep' – that when a system is built for one purpose, that purpose will shift and grow, beyond the original intention of the designers and commissioners of the system. It is a familiar pattern, particularly in relation to legislation and technology intended to deal with serious crime, terrorism and so forth. CCTV cameras that are built to prevent crime are then used to deal with dog fouling or to check whether children live in the catchment area for a particular school. Legislation designed to counter terrorism has been used to deal with people such as anti-arms trade protestors – and even to stop train-spotters photographing trains.

In relation to the Communications Data Bill this is a very significant risk – if a universal surveillance infrastructure is put into place, the ways that it could be inappropriately used are vast and multi-faceted. What is built to deal with terrorism, child pornography and organised crime might creep towards less serious crimes, then anti-social behaviour, then the organisation of protests and so forth. Further to that, there are many commercial lobbies that might push for access to this surveillance data – those attempting to combat breaches of copyright, for example, would like to monitor for suspected examples of 'piracy'. In each individual case, the use might seem reasonable – but the function of the original surveillance, the justification for its initial imposition, and the balance between benefits and risks, can be lost. An invasion of privacy deemed proportionate for the prevention of terrorism might well be wholly disproportionate for the prevention of copyright infringement, for example.

The risks associated with function creep in relation to the surveillance systems envisaged in the Bill have a number of different dimensions. There can be creep in terms of the types of data gathered: as noted above, the split between 'communications data' and 'content' is already one that is contentious, and as time and usage develops is likely to become more so, making the restrictions as to what is 'content' likely to shrink. There can be creep in terms of the uses to which the data can be put: from the prevention of terrorism downwards. There can be creep in terms of the authorities able to access and use the data: from those engaged in the prevention of the most serious crime to local authorities and others. All these different dimensions represent important risks: all have happened in the recent past to legislation (e.g. RIPA) and systems (e.g. the London Congestion charge CCTV system).

Prevention of function creep through legislation is inherently difficult. Though it is important to be appropriately prescriptive and definitive in terms of the functions of the legislation (and any systems put in place to bring the legislation into action), function creep can and does occur through the development of different interpretations of legislation, amendments to legislation and so forth. The only real way to guard against function creep is not to build the systems in the first place: a key reason to reject this proposed legislation in its entirety rather than to look for ways to refine or restrict it.

4 Conclusions

The premise of the Communications Data Bill is fundamentally flawed. By its very design, innocent people's data will be gathered (and hence become vulnerable) and their activities will be monitored. Universal data gathering or monitoring is almost certain to be disproportionate at best, highly counterproductive at worst.

This Bill is not just a modernisation of existing powers, nor a way for the police to 'catch up'. It is something on a wholly different scale. We as citizens are being asked to put a huge trust in the authorities not to misuse the kind of powers made possible by this Bill. Trust is of course important – but what characterises a liberal democracy is not trust of authorities but their accountability, the existence of checks and balances, and the limitation of their powers to interfere with individuals' lives. This bill, as currently envisaged, does not provide that accountability and does not sufficiently limit those powers: precisely the reverse.

Even without considering the issues discussed above, there is a potentially even bigger flaw with the bill: it appears very unlikely to be effective. The people that it might wish to catch are the least likely to be caught – those expert with the technology will be able to find ways around the surveillance, or ways to 'piggy back' on other people's connections and draw more innocent people into the net. As David Davis MP put it, only the incompetent and the innocent will get caught.

The entire project needs a thorough rethink. Warrants (or similar processes) should be put in place before the gathering of the data or the monitoring of the activity, not before the accessing of data that has already been gathered, or the 'viewing' of a feed that is already in place. A more intelligent, targeted rather than universal approach should be developed. No evidence has been made public to support the suggestion that a universal approach like this would be effective – it should not be sufficient to just suggest that it is 'needed' without that evidence, nor to provide 'private' evidence that cannot at least qualitatively be revealed to the public.

That brings a bigger question into the spotlight, one that the Committee might think is the most important of all: what kind of a society do we want to build – one where everyone's most intimate activities are monitored at all times just in case they might be doing something wrong? That, ultimately, is what the draft Communications Data Bill would build. The proposals run counter to some of the basic principles of a liberal, democratic society – a society where there should be a presumption of innocence rather than of suspicion, and where privacy is the norm rather than the exception. Is that what the Committee would really like to support?

Even if you enact this bill, it won't work - the people you most want to catch won't be caught by it because the means to evade it are already well known. Take the hint, drop it.

August 2012

Dr Peter Saul

I would like to make just a few comments on this Bill, I'm sorry but my paragraph numbering does not link with the committee's.

1) I have serious concerns with respect to privacy. This Bill will involve routine intrusion into law abiding citizen's privacy. Authorities will be able to track who a person is contacting and when and often from where. The ability to look at which websites are visited is like being able to track which books and magazines a person reads, again an important invasion of privacy.

2) A knowledgeable person could circumvent proposed measures by using proxy servers and overseas mail providers. Really bad people would likely know this and only less sophisticated low level criminals might have data captured

3) If one accepted the need to review this data by the authorities I feel that higher levels of scrutiny and permission should be sought. I would expect at least an application to a magistrate and for the applicant to show reasonable cause to seek it.

4) I'm not sure where the Home Office gets its figure for proposed savings. I suspect that the government has decided that it will have this Bill and submissions like this have minimal effect. But if it does go ahead and the savings don't come please ensure they ditch it.

August 2012

Dr Ashley Savage

Introduction

1. I make this submission in my capacity as lecturer in Law at Northumbria Law School, Northumbria University where I teach public law and information rights in employment. My doctoral thesis, completed at the University of Durham, considers the position of Crown servants who leak official information or make whistleblowing disclosures and accountability of the executive and central government departments. Considerable focus is given to the protection of official information and the whistleblowing mechanisms available to employees in central government departments and the intelligence agencies.

2. It can be readily identified that the proposals contained within the Draft Communications Date Bill are likely to interfere with an individual's right to respect for private and family life, enshrined in article 8 ECHR. Whilst it may be argued that the interference can be justified in the interests of national security, or the prevention or disorder or crime (or indeed any of the exceptions contained in art.8 (2) ECHR) public authorities have clear obligations from the initial interference in obtaining the data to the way in which it is used and stored. Public authorities are likely to be in breach of their obligations, rendering any interference disproportionate, where they fail to provide: "practical and effective protection to exclude any possibility of unauthorised access occurring in the first place."[461] With this in mind, my response will firstly outline concerns for data security. It will then proceed to outline the need for robust accountability and reporting mechanisms. Finally, I note general concerns relating to the impact that the bill will have on freedom of expression and journalistic source protection.

Concerns regarding data security

3. One would hope that procedures and systems will be put in place to safeguard the data from computer hacking. However, we should also consider the risk caused to such information by human error, loss or theft. In January 2008, the MOD lost details of 600,000 persons interested in joining the UK Armed Forces by the MOD. In July 2008 news reports emerged that the MOD had admitted that 658 laptops had been stolen, 89 lost and 32 recovered since 2004 and 121 memory sticks were unaccounted for.[462] Thirty five laptops were reported to have been lost at GCHQ resulting in concerns raised by the Intelligence and Security Committee in their 2007-2008 annual report.[463] In the same year, a mobile telephone sold on eBay was found by the new owner to contain photographs and information relating to terrorism investigations which had not been deleted by the previous owner, an operative in MI6.[464]

4. Detailed questions need to be asked as to how the information will be stored once obtained so that the risk of unauthorised third party access could be minimised. It is appreciated that, following the aforementioned data losses, the Intelligence and Security Committee was provided with assurances by the government that new controls had been implemented. Could these processes be improved and should these assurances be checked before the bill proceeds further?

---

[461] According to the European Court of Human Rights in *I v Finland* (Application no.20511/03), para 47.

[462] *'MOD admits loss of secret files,'* BBC News Website, http://news.bbc.co.uk/1/hi/uk/7514281.stm (accessed 15/11/09).

[463] Cm 7542.

[464] *'MI6 Photos Sold on Auction Site*,' BBC News Website, http://news.bbc.co.uk/1/hi/uk/7643374.stm (accessed 15/11//09).

5. Where such important private information is at stake, we must ask whether, in appropriate circumstances, data losses should be dealt with by way of a criminal penalty. Section 55 Data Protection Act 1998 provides an offence to knowingly or recklessly obtaining or disclosing data. Furthermore, the information that the Communications Data Bill proposes to cover is likely to be protected by the Official Secrets Act, in particular s.4 which concerns crime and special investigation powers. Section 8 of the Act makes it an offence where a Crown servant fails to take such care to prevent an unauthorised disclosure that a person in his position ought to reasonably take. Despite the number of data breaches of information which would be covered by the categories of information listed in the Act, to date, the offence has only been used once to prosecute a senior Civil Servant who left top secret documents on a train.[465]

Concerns regarding accountability

6. The process of authorisation contained in clause 9 of the Bill is most concerning. The designated senior officer may grant authorisation for the purposes of a specific investigation or for testing the system. One must question whether clause 9 contains sufficient safeguards from abuse. Whilst any authorisation made must be 'necessary' and 'proportionate' this places a significant burden on the senior officer to make the correct proportionality assessment where the individual may have a vested interest in obtaining the information sought. Where disproportionate interferences do occur, the victim of the intrusion is unlikely to be aware unless he or she is contacted during the course of an investigation. It is acknowledged that bill provides for scrutiny by the Interception of Communications Commissioner, however, given the potential number of requests and the number of public authorities involved it will be difficult to maintain effective monitoring. If access to the provisions is expanded to include local authorities the scheme will become very difficult, if not impossible, to monitor effectively.

7. It is suggested that consideration must be given to the whistleblowing/ reporting mechanisms within the organisations concerned to determine whether they are sufficiently robust for employees to raise concerns about abuse of the provisions. Regular independent monitoring and review of the mechanisms is needed by oversight bodies such as the Civil Service Commission (for HMRC) Her Majesty's Inspectorate of Constabulary (for the police) and the Intelligence and Security Committee (for the Intelligence agencies).

8. Little information is provided as to the whistleblowing procedures available to employees of the security and intelligence agencies. Media reports and brief reference in hansard suggest that there is an independent staff counsellor. The Intelligence and Security Committee provided no official acknowledgment of the independent staff counsellor in its annual reports until its 2007-2008 annual report when it discussed a new ethical counsellor available to employees of the Security Service. It may be that the respective counsellors are very effective and are trusted by the employees, yet, effective oversight of these roles is needed by the Intelligence and Security Committee. Procedures should be in place to allow employees from all public authorities who would have access to the provisions contained in the bill to directly contact the Interception of Communications Commissioner. At present it is not known whether there are procedures or protocols in place for the Commissioner to receive concerns from employees.

---

[465][465]*R v Jackson*. (unreported) *Civil Servant Fined for leaving documents on Train, Independent,* 28th October 2008.

9. Consideration must also be given to the employment protection employees may receive if they choose to raise concerns. Police officers, employees in SOCA and HMRC would receive protection for raising concerns under the Public Interest Disclosure Act 1998 provided that they do not break the law in doing so. The Information Commissioner is currently included as a 'prescribed person' designated to receive whistleblowing concerns. At present, the Interception of Communications Commissioner is not designated for this purpose, meaning that it would be more difficult for individuals to receive protection for raising concerns to the Interception of Communications Commissioner because the evidential requirements are harder to satisfy. Employees of the Security and Intelligence services currently do not have access to PIDA, thus reducing the incentive to raise concerns.

10. Employees of the four main bodies will likely face prosecution if they raise concerns about wrongdoing to the general public where the information disclosed breaches the Official Secrets Act 1989. In a report outlining best practice for intelligence services the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism identified suggested that protections from reprisal should extend to disclosures made to the media or the public if they are made 'as a last resort' and 'pertain to matters of significant public concern.[466] Currently, the United Kingdom falls short of this ideal, however while the option of public disclosure remains unavailable for these employees it is vital that the effective accountability and oversight mechanisms are in place which offer direct access to raise concerns.

General concerns regarding article 10 ECHR

11. Retention and use of traffic data is likely to have an impact on the right to freedom of expression, safeguarded by article 10 ECHR. The nature of the proposed retention and monitoring can be likened to Bentham's Panopticon. Individuals who would otherwise be critical of authority may feel inhibited from political expression for fear that they are being watched. At present the bill does not contain adequate safeguards to ensure that freedom of expression will be protected.

12. It would appear that no safeguards are in place to ensure the protection of journalistic sources. The Strasbourg court has consistently applied a high standard of protection identifying that potential sources will be deterred from assisting the press to inform the public on matters of concern.[467] There is no question that the proposals will act as a "chilling effect" on journalistic sources. The emphasis on communications data rather than the content of the messages will offer little hope – public authorities will still be able to determine which individuals have contacted journalists and when. This will present a more attractive alternative than obtaining a search warrant under the Police and Criminal Evidence Act which provides safeguards for journalistic material. This deficiency could be rectified by adding additional requirement as part of the authorisation process currently contained within clause nine. It would require a degree of knowledge that the individual in question is a journalist or is involved in journalistic activity. A fundamental flaw in the proposals is that it would be near impossible to protect all individuals engaging in journalistic activity, particularly those involved in blogging or other forms of web-based media.

---

[466] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight (2010), Practice 18. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

[467] See for example *Goodwin v UK* (1996) 22 E.H.R.R. 123, para 39.

Further Information

13. I would be happy to provide further advice or assistance to the Committee where required.

August 2012

Robbie Simpson

My submission primarily addresses technical factors and potential limitations of the proposals. This is in keeping with my background as a student and researcher in Computing Science (I should declare that while I have studied many aspects of security that networking is not one of my main areas of interest).

Section A provides an overview and discusses the difficulty of separating communication and non-communication traffic. It addresses questions 22, 23 and 24 of the call for evidence.

Section B discusses the problem of separating communications data and communications content. It addresses questions 22 and 23 of the call for evidence.

Section C addresses the problem of intercepting encrypted traffic. As such it may address questions 25 and 26 of the call for evidence.

Section D address the feasibility of storing communications data. It addresses question 22 of the call for evidence.

A. Technical feasibility of interception

Current laws provide a strong framework for the government to access communications data held by organisations that are effectively bound by UK law; entities located in the UK or entities with assets within the UK, entities performing business in the UK etc. Current law does not provide an effective method to ensure compliance by entities located outside of UK jurisdiction, and attempting to directly obtain legal control over such entities is effectively impossible.

This draft bill instead intends to oblige communications providers operating in the UK to store communications data between UK entities and overseas providers. In practice this would include telephone providers maintaining records of calls made, and internet service providers holding records of traffic between their customers in the UK and computer systems overseas.

It is my belief that such a scheme is theoretically possible but would encounter a number of tradeoffs that would make it either technically infeasible or of incredibly limited use. Key issues include the difficulty of identifying communications of interest from background traffic, difficulties in storing this information and in separating metadata (so called `communications data') from content ('communications content'). The issue of dealing with encrypted content must also be addressed.

The first issue I will address is the difficulty of identifying communications of interest from communications traffic in an efficient manner. Allow us to suppose that an order to obtain communications data has made in regard to a specific individual under the provisions of this Act. Let us then consider the practical implications from the point of view of an internet service provider.

According to OFCOM the average internet user in the UK downloads 17 gigabytes of content per month. This is not a fair reflection of the total data transferred, as it omits uploads – however upload figures are normally considerably lower than the corresponding download usage. Combined, a total transfer of about 20GB per month seems a reasonable approximation.

Very little of this will be communications data in the sense of this Act. Some of it will be entirely automated communications that form part of the infrastructure – the headers of HTTP packets, Domain Name Server lookups and many more similar systems. The majority of the data will probably be made up of large media objects – streaming video or radio, or the downloading of applications. Much will be impersonal written content – blogs, newspapers, how-to-guides. This leaves very little that is likely to be communications in the intent of

this Act – personal communications between entities, be it in the form of emails, instant messaging, voice conversations etc.

Performing highly sensitive analysis of all this data is clearly infeasible due to the large amounts of data that would be needed to process. It is not difficult in practice to separate out the different forms of traffic described above, and hence isolate the communications worthy of further investigation. However, this process cannot be perfect. It is entirely feasible to hide important communications within non-communications data. The technique of stenography is well known – hiding information within images. More technical approaches are entirely possible, and we will elaborate one.

Domain Name Servers are used to map web addresses (e.g. www.google.com) to IP addresses (e.g. 130.209.240.151) so that traffic can be routed. This process occurs every time a computer attempts to reach a previously unknown web address. This can easily be used to transmit messages. Individual A can set his computer to use a server in the control of Organisation B as a DNS server. If A then attempts to access the URL bombplantedatX.com his computer will transmit this URL to B's server. This will appear as perfectly legitimate infrastructure traffic, but B can locate this message in the logs of their server.

This would be almost impossible to distinguish from normal DNS traffic without using the most elaborate of classifiers, and such classifiers could not practically be applied to the full range of network data produced due to the sheer size. Similar logic does of course apply to hiding messages within images, video or indeed any object transferred over the network.

This allows to me to propose the first tradeoff – ensuring that all potential communications are discovered without requiring incredibly expensive systems. It appears to me that any such system would either cost considerably more than the £1.8 billion proposed, or would provide too many forms of evasion to be practical.

B. Feasibility of content and data separation

A key plank of the proposed bill is the separation of communications content from communications data (which I shall refer to as 'metadata', as is standard in the literature). The bill is right to highlight this difference, and not just because of the legal position of metadata being less privileged than content. Attempting to store and analyse all communications content would be practically impossible - Cisco reports monthly internet traffic in the UK of 844 petabytes as of 2011. 844 petabytes of storage would cost about £200 million using current storage technology. These proposals therefore are infeasible unless an effective and efficient mechanism for separating content and data can be developed.

In section A I have already outlined how communications content could be hidden in several forms of normal traffic, and put forward my opinion that it is not possible to detect this to 100% accuracy. However, I acknowledge that the government may be satisfied with a high but <100% coverage, so I will discuss a more conventional (if somewhat stereotypical example).

Person A is a member of a jidhadist cell based in the UK, while person B is a jidhadist leader operating out of Saudi Arabia. They communicate by exchanging emails on a Pakistan-based webmail system. For simplicity we assume that connections to this webmail system are not encrypted.

Authorisation under this act has been granted to intercept the communications of A, and his ISP is recording the traffic between his computer and the webmail system. This communication is in the form of HTTP transfers for pages stored in the webmail server. The response is a web page – containing the layout of the page, style information, links to access other pages on the system and the content of emails themselves. However, the separation of these elements is not neat – and will vary depending on the software running the webmail system and its configuration. There is in theory an infinite amount of possible combinations of content.

The difference between email content and other content on a webpage is quite an easy task for humans to perform – we do it every day. It is not trivial for a computer to perform, especially when we desire both speed

and accuracy. For our purpose it must be 100% accurate – as the authorisation granted by this bill only allows interception of metadata, not content. Is it possible to develop a computerised classification system that can separate communications and content on an unknown webpage with 100% accuracy? The answer is clearly no.

The same goes for many other types of communication, including those outlined in section A. The old certainty of phone communications, where call metadata and call content was separate do not apply here. From an internet service providers point of view all communications are just data packets to be routed from one computer to another – and the protocols within these packets need not be either open or documented. This leaves us in a tricky situation if we aim to intercept a packet between two computers – how can we possibly separate metadata and content if we do not know the specification of the data within? We cannot.

A metaphor may assist – this is akin to opening every letter sent in the mail, only to discover that each letter contains thousands of words written in one of a thousand different languages. To uncover the difference between data and content (or even the final destination of the letter) we need to learn to understand all these languages without reading the content of the letters.

C. Feasibility of decryption

So far we have not considered the case where communications are encrypted (rather than hidden). Encryption cannot hide the intermediate destination of any internet traffic, as that must stored in cleartext so the packet can be forwarded. The final destination of the traffic can easily be hidden though, with the next step being decoded once the packet arrives at the next hop. This is how the internet works – a packet may leave London bound for Amsterdam, and on arrival in Amsterdam be forwarded to New York, and then onwards to Mexico City. This whole process takes only a few seconds, and it is not always clear what the final destination is.

However, let us focus on one common form of encryption – the use of so-called "VPN tunnels". These have become popular for those involved in the illegal transfer of copyrighted material, as well as other illegal activities. In this system a server located outside the UK (usually in a country considered to have strong protections from government interception, such as Sweden) is remotely connected to from within the UK over an encrypted connection. When the user within the UK accesses the internet the outside world sees their connection as originating at the Swedish server – while their UK ISP sees traffic going to the Swedish server, but has no idea where it travels from there onwards.

Unless this encryption is broken this Bill can have no effect – it is not possible to identify who is being communicated with. But breaking encryption is non-trivial – the open nature of research in this field means that the average user has access to the same encryption algorithms used by security services and multinationals. An entirely standard and straightforward encryption algorithm : RSA encryption with a 1024-bit key has never been broken. Many techniques exist that exploit weaknesses in implementation, but well implemented encryption is unbreakable. Knowing this there are provisions under RIPA to force the disclosure of encryption keys with several penalties for not – but in some cases it may be easier to take the penalty for failing to disclose keys than to reveal evidence of terrorism or paedophilia.

D. Technical feasibility of storage

This draft proposes that all communications data would be stored for a period of 12 months. I have already outlined the difficulties of separating data and content, which makes quantifying the amount of data to be stored difficult. Therefore we need to think in terms of options and tradeoffs.

If we decide that storing the maximum possible amount of potential communications data is key we would need to store all the Internet traffic passing through the UK within that 12 months. As outlined in part B, this amounts to around 10000 petabytes or 10 exabytes. A system capable of storing this amount of information was recently announced by the American company Cleversafe, and reporters estimated the purchase cost of such as

system at over $1 billion. Actual costs in the UK would likely be much higher, as data would be stored by individual service providers and not pooled, reducing economies of scale.

Alternatively, let us assume that a system exists that can extract useful communications data with a high level of accuracy, and therefore we need only store 1% of internet traffic – a mere 100 petabytes. A scientific project in Australia aims to store this amount of data for around £40million, although once again this is a centralised system and not separate storage.

It appears that storage is perfectly feasible as long as only a small percentage of overall internet traffic must be stored. However, it is impractically expensive to store communications if content and data cannot be accurately separated.

One final note – while the cost of storage will undoubtedly decrease, history shows us that internet traffic will increase at at least the same rate. We should not be fooled into believing that time will make infeasible proposals more feasible.

August 2012

Richard Smith

I would like to submit evidence in line with one of the questions posed by the Joint Select Committee on the draft communications bill.

My credentials are the following:

Individual:
BSc 1st in Computer Science Edinburgh University

Corporate:
Director of a Small Wholesale Business (+20 staff) whos main country of supply is China and who uses many of the technologies described below to provide secure and unmonitored communications with suppliers and contacts in this country.

I have chosen to provide information related to point 25 as I believe it is one of the most important questions as if a technology designed to catch the few but monitor the many can be circumvented with ease by the few then what benefits does it have to the many?

27. *How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?*

It will be incredibility easy to circumvent the measures in this bill in the following ways:

- A user may create an encrypted connection to a 3rd party (outside the monitoring proposed in this bill) who in turn makes the requests for them and passes the information back to them. In this case the system proposed by this bill will only see that the user created some kind of encrypted connection between to the 3rd party and nothing more. Examples of this in use today are any kind of VPN (most business in the world who have employees outside their main office use this technology), any secure tunnel for web data e.g. a ssh tunnel.

The cost of such a service runs to the turn of a few pounds a month and one service can be shared with a large number of users (I personally have web hosting for my personal website with a company outside the uk who offer unlimited ssh accounts which any user could encrypt their traffic though. So theoretically I could offer the entire of the uk anonymity from this bill for the one of cost of less than a yearly tv licence.)

The real world examples I offer of this are that most of my non tek savy business contacts and friends who live in China use this technology everyday to access banned sites such as facebook and youtube and many use it to access useful services such as google apps.

- Any user who uses a website over ssl (this is the padlock or green bar you get when you connect to your bank or anyone reputable online shop or email service) will be protected from the vast majority of monitoring of this kind without even knowing it or having to change their web habits whatsoever.

Any website which displays this padlock or ssl technology is also creating an encrypted tunnel between the user and the site in question so as in point 1 the monitor will only be able to see they visited this website and nothing as to what the user was doing on this website. For example they could see you visited https://www.hotmail.com but nothing else. If this site is offering webmail such as hotmail, yahoo or gmail and the user is sending emails though their servers (which if located outside the UK) this bill will have no effect.

Furthermore I believe this point incentives users to use and pass data though services in other countries who could potentially be monitoring these communications themselves therefore providing them with information rather than the UK government. Also it will incentivise companies to move their data sites out of the UK to

countries with less restrictive and intrusive laws which in turn reduces security for the UK not to mention jobs and investment.

- The use of software such as Tor (www.torproject.org) will allow any user to browse the web anonymously out of the reach of this bill. This is standalone software that can be installed and run on any computer at a few clicks of a button.

Any would be criminal can employ any of the above technologies and many more to get around this bill. Any organised criminal activity will surly adopt these techniques very quickly if such a bill is passed. These technologies also have very legitimate uses so can not be also made criminal with any level of ease.

As such as this bill stands I consider it woefully inadequate to deal with this kind of crime. At the same time I consider it to be monitoring on a scale unprecedented in UK history and offers serious risks if the data recorded falls into the wrong hands.

I would gladly comment on many more of the points raised and will do so if the submission date is relaxed. If the committee would like I am willing to provide more evidence with references and examples of use to any of the points mentioned above as well as any other points on technical and business impacts of implementing such a law. I believe that having had an education covering almost all aspects of the implementation of this technology as well as having business experience in operating in a country that employees laws very similar and in many cases more rigorous than those proposed in this bill gives me a good incite into how effectively this law would function if put in place.

August 2012

Robert Smith

General:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?
    a. No, the excuse fighting terrorists is rubbish. There's something that tends to identify terrorists, they are Muslims. The entire population of the UK is not Muslim (yet), ergo the correct decision would be to only monitor those belonging to that religious group. Of course, this government is as spineless and directionless as the last lot and can't be seen to be picking on any minority, preferring to obliterate any idea privacy for all of its citizens.
2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?
    a. Absolutely not! It's blatantly clear that the procedure of approaching a Judge with sufficient evidence to issue a warrant will do exactly what is required. Of course it implies that our security agencies and government aren't incompetent buffoons and actually have some evidence.
3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?
    a. How about the straw that broke the camel's back? You're bringing about a totalitarian state seemingly with gay abandon. It's good that you acknowledge that Communications Data Bill is not the only way the government intrudes into its citizen's privacy though. How about making a big list and publishing it, just so everyone knows what you're up to?
4. What lessons can be learnt from the approach of other countries to the collection of communications data?
    a. I'm sure a study of Nazi Germany, Basathist Iraq and Stalinist Russia would be very useful to you.
5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?
    a. The fact this question exists implies that the bill is going to get pushed though regardless. I propose you don't! I do have a point to make about the cost however: Ultimately it does not matter which technique is used, it's your citizens that will be made to foot the bill, whether it's though their tax contributions being redirected to this shamble or forcing the ISPs to pay for it. The ISPs will pass the cost on to the customer.
6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?
    a. I'd go one overreaching piece of legislation. That way it will be easier for the political party that gets voted in after you lot to overturn it.
7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?
    a. Nothing, absolutely nothing is essential in this bill, all of it should be scrapped.
8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?
    a. Of course it will, who will want to have to conform to storing petabytes (possibly exabytes) of data? Given the choice I would not set up an ISP business if I had to outlay extra millions for disk storage and presumably a compatible DMS in order for the data to be queried. The whole thing will stifle any hope of economic recovery you lot are failing to engineer.

Costs:

9. Is the estimated cost of £1.8bn over 10 years realistic?
    a. I'll answer this question with a question. Since when has a major IT development instigate by this or any other government come in on time and under budget? Now compare that with the failures, such as the NHS system. I think you'll have your answer. However, never being one to underestimate any political party's ability to lack any form of comprehension when comes to anything involving computers: Of course it won't be enough! I'll lay odds now that you'll hit £1.8 billion in six months!
10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?
    a. No of course it's not; you'll go massively over budget, negating any perceived benefits. You will have forgotten to factor in elements such as the funding for the policing body that monitors for and punishes misuse of the data by political parties or the civil servants with access to it. You know, like the one that checks that local councils aren't misusing RIPA powers. For stuff like barking dogs, noisy children, illegal fishing or offences under the Weights and Measures Act. All very important against the War on Terror.

Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?
    a. Probably not, these things rarely are. However I'm hoping some idiotic loop hole has been left in so that's all I'm going to say on the matter.
12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?
    a. None of them, it should not be available in the first place!
13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?
    a. Once again, I get the feeling this bill is going through regardless. All this effort explaining to you just how stupid you are will be wasted.

Use of Communications Data:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?
    a. There are no circumstances this type of data should be accessed without a warrant issued in a court of law.
15. Is the proposed 12 month period for the retention of data too long or too short?
    a. Too long, should be 0 seconds.

Safeguards:

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?
    a. The "designated senior officer" should be defiled as a Judge in a court of law, who provides a warrant once sufficient evidence has been presented.
    b. Article 8 ECHR: Yes, there should be concern, your basically defecating on it from a great height. The wording has been deliberately misinterpreted; it's ridiculous to argue that the original intention of this wording would allow the blanket surveillance of the entire countries'

citizens. Of course there's a world of difference between concern and actually doing anything about it isn't there?

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?
    a. Hell yes, a warrant issued by a judge for ANYONE wanting access. The implication would be that you lot have to present some evidence first, which would imply that someone would be doing their job for once.
18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?
    a. Why propose them if they are not sensible? Really why? It's a legitimate question.

Parliamentary Oversight:

19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?
    a. Of course they are not. And they never will be.

Enforcement:

20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?
    a. They are no doubt totally over the top, I recommend a sternly worded letter.
21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?
    a. No, the penalty should be incarceration for life for the individual and all of their superiors. With no chance of appeal or release. And yes I am being serious.

Technical:

22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?
    a. No, it's possible to encrypt and hide data in so many ways that the ISPs will never be able to do it; they will have to capture everything and leave it to you Muppets to try and work out what's communications and what's not. In other words you're going to end up with a huge (and I mean huge) pile of data who's format will probably differ from ISP to ISP that you'll never be able to fully normalise. Think of all the data on Facebook, multiply it by a hundred, stick it in a blender and presto! That will be the reality of what you're dealing with. Any genuine terrorist knows this and knows how to hide their data, the only people you will ever catch will be the ones that are as think as pig poo and have already left a trail a mile wide for people to follow.
23. How safely can communications data be stored?
    a. It can't be, even if the impossible happens and access to this data is not misused from within, it will still be hackable no matter how secure you think it is. If humans can access it, then they can be tricked. By its very nature it will need access to the internet. And remember that the hardware itself could be vulnerable, Sergei Skorobogatov still maintains that a back door has been found in Chinese chips used by the US military. I wonder how much of the UK's internet infrastructure is built using Chinese hardware?
24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?
    a. NO! See answer to question 22.
25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?
    a. No comment.

26. Are there concerns about the consequences of decryption?
    a. I predict a sharp rise in the use of encryption should this abortion of a bill come to pass. The consequence is that more hardware will be required to decrypt it, driving up costs massively (it's computationally expensive to decrypt something). I imagine it will make a mockery of any carbon footprint targets too.

If you've got to the end, well done, I fully expected for this to have been binned before now.

I'll leave you with this final thought, you put through this bill and the least you can expect is the loss of my vote. I intend to be as vocal and as active as possible (while staying within the law) in getting this bill overturned and removing the conservatives from power for a long as possible.

If you care about this country, ask yourself this.
Assuming you had parents or grandparents that fought in WWII, what type of world where they fighting to avoid? How much, now does this country resemble the regime that was destroyed during that bloody war? If you can't see the parallels then you a traitor to this county and a traitor to your own family, don't destroy any more of our hard won liberties please.

August 2012

SOCA

GENERAL:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

Yes.

The Serious Organised Crime Agency (SOCA) is tackling serious and organised transnational crime at a time when there has been an explosion of communication means and services, many of them facilitated by the internet. A short analysis of the issues that SOCA and other law enforcement bodies face during investigations that seek information from communications data (CD) is explored further in the paper on the use of and changes in communications technology at Annex A.

SOCA's understanding of the scope of the draft Bill is that it will ensure law enforcement can maintain access to subscriber data, traffic data and service data in very much the same manner as it currently does, but that the data retained by Communication Service Providers (CSPs) will reflect the changes in technology and thus include information relating to communications sent using the internet.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

Yes.

It is important to distinguish between obligations to retain data and rights to access it. The draft bill creates a power that the Secretary of State may use to mandate the retention of CD that is not currently subject to the Data Retention Regulations. This is a new power. However, it will ensure that the quality and coverage of CD available to public authorities is maintained at the current level with mobile networks. There are no new powers to obtain CD by public authorities; the powers in Ch II of the draft Bill are almost identical to those currently in RIPA, with a minor administrative change to place the focus on assessing the privacy implications of requests, rather than the legal form used to secure the data.

SOCA believes that the draft Bill will enable the agency to maintain its capability to obtain CD in the dynamically changing technology environment. A growing and particular challenge is obtaining data which may not be held by a CSP because there is no current business need for it to be retained, or that data is held by CSPs based overseas and there are obstacles, especially in terms of timely acquisition, in acquiring relevant information.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

SOCA understands that the degree of intrusion into individuals' privacy maintains that of the current CD acquisition legislation and in the consideration of each application, the full assessment of the benefits of obtaining data against the intrusions of privacy are made in accordance with Article 8 ECHR.

SOCA, along with other law enforcement agencies, conducts investigations using a broad range of overt and covert techniques. In order that SOCA can minimise the impact on an individuals' privacy, the operational strategy devised by the investigating officer must consider the proportionality of every technique that is deployed, and also assess the aggregated proportionality of all techniques deployed through the life of the investigation. The acquisition of CD is the least intrusive of covert investigative techniques: it is focused and can reduce the reliance on traditional resource intensive, more intrusive and expensive techniques such as mobile surveillance and deployment of covert human intelligence sources.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

The communications landscape in the United Kingdom is significantly different from most of Europe and the rest of the world. The commercial provision of infrastructure and services by a wide variety of organisations has seen the cost of access reduce and the take up by private citizens rise exponentially. UK law enforcement therefore faces a more complex task in obtaining CD and has no obvious overseas partner against which it can

either compare or benchmark the manner in which it currently operates. This factor is compounded by the very different legal systems from that experienced in the UK (eg civil code, or non-ECHR common law).

During collaborative investigations with overseas partners, SOCA has observed that several European law enforcement organisations have a relatively low authorisation level for access to CD. In one country, access to subscriber data can be self authorised with desk top access to the CSP database.

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

SOCA and other law enforcement partners have worked closely with CCDp to consider a number of alternatives, which have all been assessed to be too sensitive, too costly or technically impractical and we consider this change to legislation as the most appropriate response to the technology challenge.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

SOCA does not consider this to be an additional power for law enforcement. The effective investigation of crime is itself part of safeguarding civil liberties. The new bill represents a return to the previous levels of coverage experienced when communications were primarily via voice and text-message telephony. All the same checks and balances for obtaining CD remain.

COSTS:

SOCA is not directly engaged with costs related to implementation of the Bill.

However, the benefits that SOCA gain from the deployment of highly focused CD acquisition should not be underestimated. Gathering of evidence to prove/disprove criminal conspiracy through use of CD will be a cheaper financial cost than more staff intensive investigative methods, and will carry significantly less operational risk than more intrusive covert techniques. Further, the timely use of CD during crimes in action such as kidnap or threats to life will lead to swifter resolution of an operation. The average cost of a murder investigation is £1.8M; swift intervention therefore saves not only lives, but considerable sums for the public purse. In 2011, SOCA was involved in 240 operations of this nature with no loss of life; the cost of full murder investigations for all these cases would approximate to £432M.

SCOPE:

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

SOCA believes the draft Bill should maintain the current provisions under RIPA acquisition of CD. The requirement for new legislation is driven by the external technology changes and should not affect who has access to CD. The issue of SoS amendment by Orders already exists within RIPA and should be maintained within the new legislation.

USE OF COMMUNICATIONS DATA:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

By definition, SOCA uses CD for the purpose of preventing or detecting crime. [SOCA's functions are set out in the Serious Organised Crime and Police Act 2005 (SOCAP) and (in relation to civil recovery functions) in the Serious Crime Act 2007. They are to prevent and detect serious organised crime and to contribute to its reduction in other ways and the mitigation of its consequences, and to gather, store, analyse and disseminate

information on organised crime. SOCA works in close collaboration with UK intelligence and law enforcement partners, notably UK police forces, HM Revenue and Customs (HMRC) and the UK Border Agency (UKBA); the private and third sectors; and equivalent bodies internationally.]

The difficulty in setting the bar for 'serious' crime is that the issue will be considered subjectively by an investigator. There will also be cases that may initially seem relatively minor but which can swiftly escalate as the nature of the criminality or conspiracy is better understood and the investigation progresses. In general terms, if a criminal offence has been committed for which there is a criminal penalty, law enforcement should be able to investigate using proportionate and necessary investigative techniques. These may include obtaining CD if the tests are met, in order that a judicial outcome may be achieved.

15. Is the proposed 12 month period for the retention of data too long or too short?

There are occasions when SOCA is unable to obtain communications data because it is no longer available having exceeded the 12 month retention period. However, as the majority of the communications data that is required by SOCA to undertake our investigations falls within the 12 month period, SOCA would not seek to increase the current retention period.

SAFEGUARDS:

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

The safeguards articulated in the Act and in the Code of Practice are implemented over and above a security framework that involves the following protective security features:

1. Personnel Security: Due diligence followed by national security vetting is conducted to ensure that staff who operate in the communications data unit maintain a level of integrity, honesty and trustworthiness that is commensurate with the information to which they are granted access.

2. Physical Security: Both physical and procedural security measures are deployed, such as robust building design, locks, alarms and auditable access control systems to protect the communications data from unauthorised access.

3. Information Security: Confidentiality, Integrity and Availability of data is assessed and proportionate protection, auditable access control, and secure data storage are implemented to prevent unauthorised access.

4. Training: All staff that are involved in the processing of applications for CD undergo relevant training for the role; the Single Points of Contact (staff with responsibility for acquiring the data from the CSP) undergo formal and continual assessment before they can be issued with a "Personal Identification Number" that grants them access to CSP's data.

Every application requires designated senior officers to judge the necessity of obtaining the data, including other possible means of obtaining the information, and how proportionate obtaining it is when judged against the outcome the applicant is trying to achieve. Weighing up both criteria for each application ensures that the privacy rights protected by Article 8 ECHR are given full effect by the CD application process.

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

No.

The current framework provides proper scrutiny of a process that seeks to balance investigative necessity and proportionality with the obligations of Article 8 ECHR. SOCA follows the process as set out in the Code of Practice which has a number of steps, each separated by either function or grade, or both:

1. The applicant, usually of a lower grade and linked to the investigation, will submit their case for CD within the framework of the investigating officer's overall strategy having assessed necessity, proportionality and collateral intrusion. Training is provided to Applicants to ensure they recognise human rights implications of their activities, material benefits and requirement to be accountable.

2. The application is submitted to a Single Point of Contact (SPOC) who: has undergone formal training; is independent from the investigation; will advise the applicant; and will submit applications that meet the requirements of necessity, etc for authorisation.

3. Authorisation is undertaken by the Designated Person (DP), a senior officer at a rank stipulated by Parliament, also independent from the investigation and trained in considering the impact of necessity, proportionality and collateral intrusion on an individual's privacy.

4. If authorised by the DP, the application is returned to the SPOC who will obtain the CD and pass it to the applicant.

5. The process is overseen by the Senior Responsible Officer (SRO) who is accountable for the integrity of the process.

SOCA is inspected by the Interception of Communications Commissioner's Office (IoCCO) annually who scrutinise the process. The primary objective of the inspection is to ensure that the system in place for acquiring CD is sufficient for the purposes of the Act and that all relevant records have been kept; ensure that all acquisition of communications data has been carried out lawfully and in accordance with the Human Rights Act (HRA), Part I Chapter II of RIPA and its associated Code of Practice (CoP); and, provide independent oversight to the process and check that the data which has been acquired is necessary and proportionate to the conduct being authorised. Obtained CD is also subject of intense examination in the judicial system. Law enforcement activity occurs within the criminal justice process, in what is probably the most rigorous disclosure regime in the world. Criminal trials often expose applicants and DPs to cross-examination, and their decisions to judicial scrutiny.

SOCA believe the current oversight and scrutiny process is robustly sufficient and therefore do not support a 3rd Party authorisation process. There would be considerable resource implications to initiate any new process as they would require training in the process and in the investigative methodology applied by law enforcement, security clearance of staff and security infrastructure to be put in place, and to be available to meet not only routine but urgent and out of hours requests. Whilst none of these issues are insurmountable, there would be no reduction in the degree of internal scrutiny by law enforcement prior to CD requests being submitted for authorisation by whatever body was elected to conduct such activity. The ongoing maintenance to sustain the sheer number of applications per year would require additional configuration in the workflow processes, potentially including secure ICT infrastructure, and would cost time in both extraction by law enforcement to attend magistrates' courts/independent body, and delay in authorisation which may impact on urgent or dynamic operational activity. It is unclear how such 3rd Party authorisation would add value to the current process, whether it would offer any additional assurance or how any additional oversight of this new safeguard proposal would be introduced as not to be subject of any further criticism.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

Yes.

SOCA sees the role of the Interception of Communications Commissioner, dealing with issues of data access, and the Information Commissioner, dealing with data retention, as being essential to ensuring there is independent oversight and scrutiny of the processes used by SOCA in this environment. They provide reassurance that SOCA activity remains lawful and, because of their reach across different organisations, can provide a perspective on best practice in terms of both the process by which activity is conducted and why certain aspects are necessary or work well in different circumstances.

ENFORCEMENT:

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

SOCA has not been subject of any issues of inappropriately requesting CD. SOCA staff may face prosecution for misconduct in a public office, or potentially under the Computer Misuse or Data Protection Acts, if found to be obtaining data unlawfully. In addition, staff would be subject to disciplinary proceedings if they were found to be in breach of the SOCA Code of Conduct. Whilst the Code of Practice is recognised as being the lawful process by which CD is obtained, it is very much a set of guidelines about how to implement the Act and it is unclear how sanctions for contravening the Code would add value.

TECHNICAL:

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?

The draft Bill maintains the current access regime and SOCA does not therefore envisage there being any change to its current business processes nor to the security and safeguards that are already in place as a result of the implementation of the draft Bill.

It is assessed that organised crime groups already take counter measures to try to evade detection by law enforcement. The draft Bill should enable law enforcement to build up a richer view (when necessary and proportionate to do so) of a wider range of suspects' online communications. That makes it less likely that criminals' counter measures will succeed.

Annex

Introduction and Background
The following scenario and statistics are provided to give an example of how the communications environment in the UK has changed in the past 20 years, since the first dial-up internet access was offered in 1992. Figures are taken from Ofcom or the International Telecommunication Union (part of the UN). It is intended to illustrate the reasons why traditional CD, held by CSPs pursuant to the Data Retention Directive 2006 is no longer sufficient to give a detailed picture of a target's communications.

Scenario - A day in the life -
Dougie is a medical student living in Milton Keynes with his parents and studying in London while holding down a part time job in Costa Coffee to help fund his studies. He is a keen Aston Villa fan and has a passion for gadgets as well as being a regular on-line gamer.

a. A typical day starts with Dougie being woken by the alarm clock on his iPhone4 at 7am. Using WIFI connectivity, connects to the Virgin Media Superhub installed at his parent's home. He checks his Yahoo email account, Twitter account and Facebook profile. He also logs into the SkyGo application using his parents Sky ID

to watch Sky Sports News to see if Aston Villa have signed any new players overnight. He also logs into the team's Aston Villa fan forum to see what rumours and speculation other fans have submitted;

b. While eating his breakfast, he checks the Virgin Trains and TFL applications downloaded onto his iPhone to check for train and underground delays, before leaving the house to travel to his place of study at Gower Street in London;

c. Dougie rides his bike to Milton Keynes Central Station and boards a Virgin Westcoast train to Euston. On the train he connects to the WIFI service, provided to the trains by T-Mobile and tops up his Oyster card online;

d. He arrives at Euston Station and heads towards the Victoria line to catch a Southbound train to Warren Street. While waiting on the platform he uses the Underground WIFI service provided by Virgin Media to check his emails again. He reads an email from his girlfriend stating that she has booked the hotel in Rome; he now needs to sort the flights;

e. He arrives at Warren Street and makes his way to his lectures. During his breaks he logs into the internet (GSM) on his iPhone provided by Vodafone and checks his Facebook location services to check if any of his friends are in classes today and checks in himself so that they are aware he is in London. He arranges to meet two of them for coffee, sending them Instant Messages (IM) on the service provided by Facebook chat;

f. He finishes his lectures for the day and heads to Oxford Street to start his shift at Costa Coffee and meet his friends. During his shift, he logs onto the free WIFI service provided in Costa Coffee, provided by O2, and logs into his Easyjet account using the application downloaded to his phone. He books flights for himself and his girlfriend to travel to Rome, entering names, addresses, dates of birth, financial information and passport details. He also makes use of the free WIFI connection to call his girlfriend on his Viber application to give her the details of the flights;

g. Dougie completes his shift and travels back to Milton Keynes, continuing to utilise the WIFI services on the Underground and Virgin Trains. While on the train, he sends a free text (SMS) message using his WhatsApp application to his brother in Italy telling him to be in at 9pm when he will ring him from home. He then logs into his Ebay account and buys himself a new suitcase for the trip and books his car in for a service at the local Kwikfit centre, entering his car details and time/date for the service;

h. Back at his parent's house, he uses his iPad to log in to his favourite VOIP account, Webcalldirect and sets up a call back service from his parent's landline number supplied by Virgin Media to his brother's telephone number in Rome, supplied by Telecom Italia. This service provides a free call between two landline numbers, but originating/connected from the Internet call. After providing the flight and hotel details of his visit, Dougie arranges to meet his brother on-line in 5 minutes to play World of Warcraft, where they continue their conversation using the in-game chat facility.

The above scenario, although fictitious, is by no means complicated or futuristic in its content and the applications, websites or connections are used by many millions worldwide everyday.

The below is a table compiled by Ofcom to show how friends and family in the UK regularly communicate (each means being used at least once per day)

Overview of changes in UK communications market

Fixed line (broadband) infrastructure:
In 1992, the first dial-up internet access was introduced to the UK. This "narrowband" service has now almost been entirely replaced by superfast broadband exchanges and mobile (internet) phone networks.

In 2000 the ITU reported that 26.2% of the UK population were using the internet; this had increased to 52% by 2004, and 82.5% by 2010. Ofcom statistics show that at the end of 2011, 18.8 million fixed residential broadband

connections were installed in the UK; over 75% of homes. Superfast broadband services became widely available in 2010; 1.4 million connections were in place by 2012. This represents almost 7% of all broadband connections. Superfast broadband is capable of sustaining more services at faster speeds, with the potential to increase the number of services an individual uses considerably

Mobiles and Mobile Internet:
The first publicly available "mobile" phone was released in 1983. By the end of 1999, 13 million people in Britain had a mobile phone. Tentative (and possibly naïve) predictions suggested this would rise to 20 million within 5 years. But by October 2000 British owned mobile phones had reached 34 million (over 50% of the population): ownership appears to have coincided with the 'texting' phenomenon.

2005 saw the introduction of the 'Smartphone' which offered mobile internet access (Global System for Mobile Communications (GSM)) among many other things. In the following 7 years to March 2012, 33 million units were sold in the UK alone and Smartphone usage accounted for 50% of the mobile phone market. Ofcom have reported that in the 3 years from 2008-2011, the UK saw the number of Smartphone data users (internet usage) almost quadruple from 8.4 million to 32.6 million.

In 2002, the first multimedia messaging services (MMS) were introduced and by 2005 GSM networks accounted for over 75% of the worldwide cellular network market serving in the region of 1.5 billion subscribers. Today, GSM Association estimates that GSM standard serve 80% of the global mobile market – over 5 billion people across 212 countries and territories.

Current infrastructure and associated risks
With the introduction of more complex and improved networks, faster connection speeds, cheaper (or free) services, fragmentation, thousands of applications and an abundance of devices available, more and more data is potentially available.

Fragmentation:
The internet was developed as a 'best efforts' technology; rather than establishing a single physical connection between two points (as in 'circuit-switched' telephony), information is broken down into many pieces and sent across the network to be re-assembled at the destination terminal. This increases the speed with which large amounts of data may be sent, but results in the data being fragmented across the network. The internet was also designed as an 'end-to-end' technology, with no centralised control; this means that the only points in the connection where all the packets are guaranteed to appear are at the end users' terminals. Packets lost in transmission are re-requested and re-sent, but this can only be done by the recipient end user's device. Further, CSPs providing connectivity have no interest in the communications sent using the service. Whilst the type of data packet – for example, video, text – will have implications for capacity, the use made of internet access is of no interest to CSPs and as such is not captured. Data about how users communicate online is therefore held by several application providers and not by CSPs themselves.

Growth forecasts – looking forward
There have been significant rises in the uptake of broadband services, superfast broadband services, mobile phones, internet enabled mobile devices, Smartphones and applications, but what can we expect to see over the next few years? CISCO forecasts huge and rapid growth in the take-up, use of and evolution of IP enabled devices and their associated traffic:

a. IP Traffic forecast: IP Traffic will grow 4-fold from 2011 to 2016, a compound annual growth rate of 29%;

b. Internet Traffic forecast: Internet traffic (overall internet use) will grow 3.8 fold from 2011 to 2016, compound annual growth of 31%;

c. Mobile Data forecast: Mobile Internet access predicted to grow 18 fold from 2011-2016, a compound annual growth of 78%. Mobile data traffic in 2016 will be 5x that of the entire Global internet use in 2005;

d. Device Growth forecast: There will be 19 billion networked devices in 2016, up from 10 billion in 2011.

Communications devices will continue to evolve rapidly and their use is going to increase at the same rate. Changes in technology will allow a quicker, easier and more convenient way to communicate.

August 2012

Society of Editors

The Society of Editors has more than 400 members in national, regional and local newspapers, magazines, broadcasting, digital media, media law and journalism education.
It is the single largest organisation for editors and senior editorial executives. Its members are as different as the publications, programmes and websites and other platforms for the delivery of news that they create and the communities they serve. But they share the values that matter:

- The universal right to freedom of expression.
- The importance of the vitality of the news media in a democratic society.
- The promotion of press and broadcasting freedom and the public's right to know.
- The commitment to high editorial standards.

Following consideration of the Committee's Draft Communications Bill, the Society lends its support to a detailed submission by the Newspaper Society. We support the concerns outlines in their entirety.

We remain alarmed, as previously echoed by Lord Black during a debate on the Queen's speech, at the breadth of the legislation and the potential threat [and lack of specific safeguards] to protect confidential journalistic sources which can be revealed by communications data.

Although naturally the Bill is being described as a protective measure to enhance the safety of the population against online criminals we remain concerned that plans to beef up data retention include a "request filter", which could allow police officers, tax inspectors, the security services etc to trawl for information across privately-owned databases in order to build up a picture of suspects' internet browsing habits, contacts and movements, and that this may potentially be granted on a very wide range of grounds each capable of very broad interpretation.

In light of this it is entirely feasible to assume that this could have a detrimental effect on journalistic sources, deter whistleblowers and increase the risk of personal details being hacked.

As is often the case in terms of predicted expenditure and savings we remain unconvinced of the feasibility of an estimated cost of £1.8bn over 10 years. Furthermore 'benefits' of between £5 billion and £6.2 billion over the same period appear unrealistic when placed alongside Whitehall's history of preventing initial figures from spiraling out of control.

The fact that the UK is thought to be the only country in the world attempting to gather communications data in this way is worrying. Aspects of the bill seem capable of being judged merely as a 'snooping charter.' We are yet to be convinced that there is adequate justification for widening the scope of access to communications data when figures released by Sir Paul Kennedy in his annual report outline a significant number of "communications data errors" in recent months. In light of this we question not just the inadequacy of safeguards but the inadequate justification for the widened scope as a whole.

August 2012

Professor Peter Sommer

Summary

This submission concentrates on the technical feasibility and efficacy and value for money of the policies behind the draft Bill. The Bill's aim is to realise the ambitions of the Home Office's Communication Capability Development Programme (CCDP).

The role of retained communications data in investigations needs to be understood within the broader context of all the available potential strands of evidence available for consideration. The ever wider use of computers and telecommunications by individuals, businesses and governments has had a transformative effect on many types of criminal and intelligence investigation. Retained communications data is but one element and while over time some forms are becoming less available, this loss is more than balanced by the increased availability of other types of digital evidence.

The precise problems associated with communications data are best addressed by looking at the various types of Communications Service Provider and the classes of data they might retain. The globalised percentages approach of the Home Office misleads. Many forms of communications data will continue to be available for the foreseeable future without new legislation, while others are held by businesses outside the easy jurisdiction of the UK courts, raising the question of how UK laws, orders, and court decisions can in practice be enforced.

A key requirement of any law is that it is easy to interpret. It is now increasingly difficult to align and interpret the legal definitions of "communications data" and "content" with the complex ways in which data is transmitted over the Internet. Resort must be made to expensive hardware to apply a very large number of technical filters which are supposed to reflect the statutory definitions. These filters must be constantly updated and added to, to reflect the incredible dynamism of the Internet. Even then one can anticipate some of these will require testing in the courts. The complexity and difficulties also have an impact on the extent to which Parliament can be expected to scrutinise the Orders contemplated in Part 1 of the Bill, and to which the regime can be effectively overseen by the Interception of Communications Commissioner.

The penalties for incorrect separation of communications data from content fall chiefly on the police. The regimes for access are very different – interception of content requires a warrant from the Secretary of State, communications data an authorisation from a senior designated officer. Communications Service Providers are de facto protected from mistakes, but police who have acquired material ultra vires will find themselves in difficulties, not the least at disclosure and the possibilities of arguments about abuse of process. The problem is significantly compounded by the UK's almost unique position in treating intercepted content as inadmissible and not referable to in legal proceedings.

The Request Filter proposals in cl 14-16 appear to be an attempt to overcome the twin problems of interpretation and the two entirely separate regimes for communications data and the interception of content. But making this a function, direct or delegated, of the same Secretary of State who also issues interception warrants and Orders under the Draft Bill is surely a mistake; if there is to be a credible and viable independent filtering agency much more needs to be said about its resources and governance.

The costs of the Home Office's proposals are impossible to calculate as there are too many unknowns but it is possible to identify criteria for likely value for money. Neither the Explanatory Notes nor the Impact Assessments discuss the source of funding but it seems reasonable to assume that in the current economic climate funding will have to come from existing resources. It is thus useful to seek to evaluate the role of the features of retained communications data that would be enhanced were the Home Office's proposals to be accepted against the loss of some funding to other existing forms of investigative activity and evidence.
Those who seek to avoid having their Internet activities being monitored will have a number of easy routes, even after significant public expenditure on the CCDP. There is a danger that CCDP will have ever-expanding technical ambitions as the Internet changes which, coupled with the need for secrecy, will lead to runaway costs.
I suggest that ways forward include:

- bringing interception evidence back into admissibility so as to simplify many of the technical interpretative problems the draft Bill creates

- continuing the current position that the requirements of domestic CSPs to retain communications data is limited to records they create as part of their regular business activities

- a substantially revised system for the issuing of warrants and authorisations coupled with more robust and credible forms of oversight, so as, among other things, to persuade critical non-UK-based Communications Service Providers to accede to the requests of the UK authorities.

This submission concentrates on the following questions in the Joint Committee's Call for Evidence: 1, 2, 5, 6, 11, 13, 17, 18, 19, 22, 24, 25, 26.
References to comments made in earlier oral evidence sessions are to the uncorrected versions published on the Joint Committee's website.

Digital Evidence Landscape

The requirement for and cost-justification for an enhanced regime for retained communications data needs to be tested in the context of the vastly increased range and extent of many types of digital evidence available to the UK authorities since the passing of the Regulation of Investigatory Powers Act 2000 (RIPA).

Over 75% of the UK population have access to the Internet from their home and each UK household on average owns three Internet-enabled devices[468]. Nearly 80% have at least one home computer[469]. Costs of hard disk storage fall by 50% every 18 months – a 1000GB (1 TB) hard disk now costs about £60 - so that in a typical police search warrant execution on domestic premises they can expect to find several PCs of various vintages, plus external data storage devices such as disks and USB memory sticks. There are 130 mobile phone contracts per 100 of the population, 39% of them smartphones, in effect powerful ultra-portable computers[470]. Nearly all of these devices contain substantive files, copies of emails sent and received and histories of such Internet activity as websites visited, pre-occupations of and research carried out by the owner. PCs may also contain artefacts relating to other types of Internet services used, complete with user names and passwords. They may also provide strong evidence of persons with whom the computer owner has been in contact. All mobile phones will contain some records of calls made and received and copies of SMSs made and received – Ofcom says 200 SMSs are sent per person per month[471] . Smartphones will contain much more recoverable data.

All of these are key sources of digital evidence and none fall within the regime of the Regulation of Investigatory Powers Act 2000 (RIPA) or the Draft Bill, which are solely concerned with data in the course of transmission. Significant types of evidence that can be obtained under RIPA powers can also be found on seized PCs and mobile phones; and the recovered data will have a considerable historic element because of the capacity of the associated storage devices. Computers and mobile phones are normally seized under powers within Part II of the Police and Criminal Evidence Act, 1984 (PACE) but there are also many additional powers in other

---

[468] Ofcom, Q2012, http://media.ofcom.org.uk/facts/

[469] ONS, Selected Consumer Durables, http://www.ons.gov.uk/ons/rel/family-spending/family-spending/family-spending-2011-edition/sum-consumer-durables-nugget.html

[470] Ofcom *Communications Market Report 2012* http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/UK_0.pdf

[471] http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/UK_0.pdf

legislation[472]. Whereas the RIPA route will exclude "content" for admissibility purposes[473], the same material if found on a hard disk is fully admissible.

Over the last 12 years, since RIPA came into force, the amount of information collected by commercial bodies about individuals has increased greatly, chiefly through "get to know your customer's interests better" Customer Relationship Management (CRM) software and the development of commercial credit and marketing databases.[474] Commercial marketing-type data can be bought by law enforcement agencies on commercial terms, privately-held data can be acquired via Production Orders under PACE, subject to the provision of a certificate under s 28 or 29 of the Data Protection Act 1998. [475] The same route can be used to obtain information about banking and credit card transactions – credit and debit card data may also contain information of the location at which a transaction took place.

At the same time the availability of Closed Circuit Television (cctv), both officially and privately owned, has expanded greatly, both in the quantity of cameras[476] and their locations and in the quality of images. [477] . The UK's National Policing Improvement Agency operates a national DNA database, which is one of the world's largest, with profiles on an estimated 5,570,284 individuals as of 31 March 2012. It also operates a national automated number plate recognition system, which by March 2011 was receiving 15 million sightings daily, with over 11 billion vehicle sightings stored. A national fingerprint database contained 8.3m individual's prints in April 2010. [478]Another new-ish method for tracking the movements, at least of people in London, is via the Oyster card[479].

Types of Communications Service Provider

There are several distinct types of organisation and business subsumed under the phrase "Communications Service Provider". By identifying them we can more easily see what potential evidence they might produce, what role that evidence could have in investigations and what obstacles the authorities may encounter. Several important forms of communications data are not under threat of diminution in value as a result of technological developments.

Individual businesses may offer combinations of these roles and there may also be a limited amount of blurring of functionality.

Telcos These are the conventional telephone companies, offering either fixed or mobile services. In terms of communications data, they use and all telcos can provide: the identity of subscriber [480]and for each call: counter-party number, time and duration of call. Mobile phone companies can also provide location data (which is based on the technical requirement for the mobile phone system to know where each of its subscribers'

---

[472] Eg s 14 Computer Misuse Act 1990 and s 114 Finance Act, 2008

[473] S 17 RIPA 2000

[474] Eg DataHQ, Experian, Equifax. http://www.graydon.co.uk/, http://www.world-check.com/

[475] See also *Government Access to Private-Sector Data,* Brown, International Data Privacy Law, 2012 (in press)

[476] Cheshire Constabulary estimated in 2011 that there are 1.85m CCTV cameras in the UK, 1.7m of which are privately owned

[477] See BBC research in 2009 on the density of local authority-owned cctv cameras: http://news.bbc.co.uk/1/hi/uk/8159141.stm and a Channel 4 News assessment that in 2008 there was a cctv camera for every 14 citizens. http://www.channel4.com/news/articles/society/factcheck+how+many+cctv+cameras/2291167.html

[478] www.npia.police.uk

[479] http://news.bbc.co.uk/1/hi/england/london/4800490.stm

[480] But not for PAYG customers; additional forms pf ,matching are needed to identify them

phones is located so that they can be actuated to receive an incoming call). Mobile phone call data records also include the hardware identity of the handset (IMSI) and the SIM in use (IMEI).

All telco-related communications data is useful in building up patterns of calls between parties, perhaps to show some form of conspiracy; mobile phone location data additionally shows the movements of a cellphone owner by time over a landscape. Police routinely use special link analysis software to show the patterns of usage[481] and a number of companies also offer Cell Site Analysis to show patterns of movement. Although some fixed line calls may over time migrate to Internet-based telephony (VOIP, Skype), the use of mobile phones is unlikely to diminish and however these phones are used, so long as they are switched on, they will continue to deliver location data.

Network Access Providers This is what most people regard as Internet Service Providers. The core service is to give the subscriber some form of box (hub) through which the Internet may be accessed. The actual service may be superimposed on a conventional telephone line or entertainment tv cable, or may involve a dedicated line, perhaps fibre. A Network Access Provider (NAP) usually thinks of itself as a conduit. In addition to the basic facility there will usually be others, to handle conventional email, to improve the experience of using the world wide web (for example by caching), and the same business may also offer its subscribers hosting facilities, for example to provide a base for a web-server from which the subscriber can publish their own information.
NAPs can provide: details about their subscribers[482] and also which of their subscribers held which IP addresses at particular points in time.[483] The latter is especially important as the originating IP address of a communication is routinely gathered in many types of Internet transaction such e-commerce, e-banking, use of file-sharing services, and it then becomes possible to associate the IP address with a subscriber or an individual. The NAP also provides a very convenient collection point at which to monitor the activities of their subscribers, subject to legal constraints. Nearly all large NAPs will have already have installed Lawful Intercept facilities (as required under s 12, RIPA, 2000) and they are also the logical place where any filtering to retain communications data might take place.

Under the Bill NAPs will bear the burden of carrying out the filtering functions; in effect their role will change from merely retaining data routinely generated as part of their business functions – for billing and quality of service purposes – into collecting data about their customers for which they have no business use but which may be required by the Secretary of State.

Private Business Networks As the name implies, these are networks run by businesses and organisations for their own benefit or to serve the requirements of a discrete industrial, professional, academic or other community. They are typically run on equipment owned or rented by the organisation. These days they nearly all use the same technical protocols as the Internet (TCP/IP). General admission to the public is not allowed; many private networks have gateways, some limited, to the public Internet. Private Business Networks still fall within the remit of the Draft Bill - (ss 1(3) and 2(1) RIPA, 2000) and more particularly if the private network is facilitating a communication onto a public telecommunications network.

Because they have control over the network, owners and managers have complete technical access to all traversing traffic, though lawful surveillance may be limited.[484] There may also be extensive logging to record accesses by users, visits to websites and the activities of anti-virus software. If a RIPA approach does not prove

---

[481] eg I2; http://www.i2group.com/uk

[482] The NAP/ISP can only provide information about their subscriber, the person with whom they have the contract, that may only indirectly point to who was actually using the equipment at the time

[483] An explanation of IP address appears from para 0 below. The availability of data is unlikely to be changed as a result of the migration from IPV4 to IPV6.

[484] Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

effective, the same information could be obtained by Production Order or, in extremis, by a PACE or similar warrant to seize records and hardware,
The authorities might incur difficulties in getting access under RIPA or other means if the private network is managed from overseas and is uncooperative. RIPA covers all situations where the traffic crosses the UK, but enforcement would then require resort to a Mutual Legal Assistance Treaty, the outcome of which could be unsatisfactory.

Social Network Service Providers This rather awkward phrase (SNSP) encompasses businesses who offer communications and information services via a web-interface or phone/tablet app. The services are sometimes described as nomadic, as they are available whereever there is an Internet connection. Examples include the web-based email facilities of Microsoft (Hotmail, Live, Outlook.com), Gmail, Yahoo and many others. It also includes businesses that offer social networking such as Facebook and LinkedIn and Internet indexing facilities such as Google and Bing. Many Voice-over-Internet-Protocol (VOIP) services, including Skype, fall into the same category.

Cloud-services are a variant: they offer remote storage and remote processing; examples are Google Apps/Drive, Microsoft SkyDrive, DropBox, Amazon Elastic Computing, Windows Azure and Apple iCloud. The same provider may offer more than one facility: Microsoft and Google both offer Internet-indexing, web-based email and "chat" (real-time conversation via keyboard); Google provides social networking as well Internet indexing and email, Facebook provides a messaging service, Skype, primarily a VOIP service also offers text messaging and so on.

A yet further variant are sites offering participation in online games; in some of them whole virtual worlds are created, participants can create avatars of themselves and chat to other participants; a leading example until recently was Second Life; a number are now delivered via games consoles such as Xbox. . Concern is sometimes expressed that these services can be used for covert messaging between criminals and others, though I have been unable to identify any verified instance.

The headquarters of the legal entities behind the vast majority of SNSPs are based outside the United Kingdom, which means that non-cooperative enforcement of UK law is difficult. Most are based in the United States. The UK would have to rely on the operation of Mutual Legal Assistance Treaties (MLATs) and these can be slow in process because of the need to follow a variety of local protocols; they also rely on the enthusiasm of law enforcement agencies in the countries in which the SNSP is located. Many larger SNSPs have technical facilities – computer server farms – located in many jurisdictions all over the world, so that identifying where any particular communication or transaction is physically taking place may be almost if not entirely impossible.

SNSPs will have limited subscriber data as for many the enrolment process relies on the voluntary supply of information, which is often not verified; most do not impose a charge for their basic services, so that there is no linkage via the banking/credit card system. However IP address data may be collected so that an individual may traced that way (see above). However SNSPs often collect large quantities of content; for some the business model consists of giving desirable information or facilities to customers in order to collect information about them which in turn can be translated into opportunities for targeted advertising. In investigatory terms the content may be directly invaluable and may also help identify individuals even where those individuals have sought to obscure who they are. Cloud suppliers also store large quantities of their customers' data files; these presumably could be available to investigators, subject to the appropriate legal processes.

Many of these services use https, the secure encrypted form of the web, and which is also the foundation of web-based electronic commerce and banking. Encryption is used, not to thwart law enforcement but to protect customers from criminal eavesdropping. But the use of https also makes the type of NAP monitoring to obtain enhanced data retention contemplated in the draft Bill much more difficult to achieve.

In the US attempts are being made to bring SNSPs into the lawful intercept framework of CALEA (Communications Assistance for Law Enforcement Act, 1994, as amended) which would imply, in the US at

least, an interception capability – although this could be provided using software on SNSP servers, rather than the interception of communications "on the wire".

The Joint Committee will undoubtedly be making its own enquiries of SNSPs but informal indications are that some US-based SNSPs are willing to respond informally in a positive and timely fashion to UK RIPA-type requests. However in so doing they have to consider, among other things, their obligations under US law, the impact that knowledge of their co-operation has on their customers and hence their business, and concern that authorities in other jurisdictions would want similar facilities. What is likely to be persuasive is the fairness and transparency of the ways in which requests (which would otherwise be warrants and authorisations) are made and by whom, how any material supplied is subsequently handled, and the quality and extent of oversight and audit.

Small-scale informal private network service facilities This equally awkward phrase covers the situation where communications and information facilities are set up on the Internet by individuals and small groups to service the need of small communities. Although the services are available on the Internet, access is restricted and may be only available by payment or specific invitation. Examples include bulletin board systems (which also have private messaging), private chat systems, file sharing systems, and secure email (which operates outside or in parallel with public email).

These services require only modest levels of technical skill to set up. Software to create the basic infrastructure is readily available, much of it at low or no cost. It is easy to run such services with cryptographic protection (https and its e-mail equivalent). Many ISPs offer hosting facilities, that is, the use of computers already connected to the Internet and to which the customer can upload his own software. It is also possible covertly to set up such services on large computer systems which are insecurely managed

Many of these services are non-sinister; for example bulletin board systems may serve people with particular professional or leisure interests. But the same technical infrastructure can facilitate illegal enterprises.

The opportunities for the authorities to detect such sinister services by routine as opposed to targeted Internet surveillance are very limited. The normal methods of detection are via traces left on the computer of one of the participants, confession or infiltration of the membership.

Other forms of covert Internet communications At this point we also ought to consider other forms of covert communications across the Internet, typically using existing Internet facilities and protocols in ways so that messages and data can be sent without easy detection. It can be a mistake to believe that covert Internet communication is only possible through the deployment of a sophisticated technology. Messages can be published via email, web sites, social networking sites where the words though innocent in appearance, have particular meaning to individuals; it is trivially easy to publish web-pages and files which are not directly indexed on an otherwise innocent site and which could therefore only be found by those with specific instructions. More sophisticated methods of concealment are also available, but they require greater levels of skill in participants.
Almost none of these covert communications will be detected by routine Internet monitoring.

Communications Data and Content

Laws, in order to work, need to be capable of easy interpretation. One of the great weaknesses of the draft Bill is that the definitions of communications data do not align with the reality of the circumstances the Bill is supposed to be regulating and managing. At the heart of the Home Office's proposals is a belief that it is possible easily to separate content from communications data.

The penalties for incorrect separation of communications data from content fall chiefly on the police and other agencies. The legal regimes for access are very different – interception of content requires a warrant from the Secretary of State, communications data an authorisation from a designated senior officer. Communications

Service Providers are de facto protected from mistakes[485], but police who have acquired material ultra vires will find themselves in difficulties, not the least at disclosure and the possibilities of arguments about abuse of process. [486] The problem is significantly compounded by the UK's almost unique position in treating intercepted content as inadmissible and not referable to in legal proceedings.[487]

Packet communications

In conventional analogue telephony, the distinction is easy to make.[488] "Communications data" consists of an enhanced telephone bill (traffic data, who called who, when, and for how long) and information about the subscriber. The content is the voice component, what would be captured if a tape recorder or similar were placed across the line. In mobile telephony, location data is also provided but is clearly separable from the voice element.

Data packets While in conventional telephony a permanent unique communications link exists between the parties for the duration of the call (a series of switches creating the link for as long as it is needed) , Internet traffic of all kind is transmitted as a series of packets. The system makes much more efficient use of available physical links; each link may convey large numbers of "conversations" or "transmissions". Data to be transmitted is broken down into a series of small chunks ("packets") each of which contains: the address ("IP address"[489]) of the originator, the IP address of the intended recipient, some supervisory information in case packets arrive at their destination out-of-order and need to be re-assembled correctly, and "payload".

Packet payload may include what RIPA regards as communications data and also what when captured becomes a RIPA interception. But there will also be a series of structures – commands, labels or values – which are the building blocks of the many protocols that make up the Internet – email, web-services, secure web-services, file transfer, file-sharing, Voice-over-Internet. These commands are not normally seen by the regular user; some of these commands and labels may themselves be either RIPA "communications data" or RIPA "content", or may help identify the subsequent sequences of text, etc. as either "communications data" or "content"."

Contents of web pages The complexity does not end here. A single web page may contain, at least in the terms hoped for in the draft Bill, both "communications data" and "content". A typical example would the "inbox" of a webmail service. The identity of the sender and the time of transmission is "communications data", but the subject matter is "content". On an individual basis visual inspection may easily spot the difference, but what is required is that the separation be carried out automatically at very high speed by software; each individual different design of a webmail web-page would need separate attention and whenever a specific webmail service has a changed design, the technical instructions for scraping the communications data from the content may need to be altered as well.

---

[485] They protected *de jure* under s 3(3), RIPA in that they are allowed to view intercept material for the purposes of separating it from content. In the event of inadvertent release they would argue absence of *mens rea* and also invite the CPS to apply a public interest test.

[486] See, for example the Codes of Practice on the *Disclosure and Acquisition of Communications Data* and *Interception of Communications* issued under s 71 RIPA and in particular Chapter 7 of the second Code. See also the *CPS Disclosure Manual* and in particular Chapter 27.

[487] See, among others, *Telephone Tap Evidence and Administrative Detention in the UK,* John R Spencer *in A War on Terror, ed Wade & Maljevic, Springer verlag 2010* and *Intercept Evidence: Lifting the ban,* Justice, 2010, Privy Council Review Chilcot, .Cm 7324,

[488] I am conscious how useful illustrations and demonstrations might be at this point but am also mindful of the restrictions in normal Parliamentary publishing. I would be happy to provide Committee members with a series of demonstrations if they feel it would aid their understanding

[489] IP addresses are relatively unique to an individual computer; under the present system, IPV4, the ISP/NAP assigns IP addresses to their individual customers and maintains a record of such assignment, usually via the RADIUS log. Large organisations have permanent IP addresses which can be looked up via the Internet "whois" facility.

As if this is not enough, modern techniques for creating web-pages rely on taking material from multiple sources and using programming facilities loaded into the web-browser, the page is only finally assembled on the individual user's computer. (This technique relies on variants of JavaScript and HTML). In order to reconstruct from monitored packets the web page that the user sees – and hence be in a position to apply the legal definitions of "communications data" and "content" - several different packet streams may have to be assembled and reviewed. Some of the packets will contain fragments of the Javascript, etc. miniature programs.

DPI The basic tool for examining packets is called Deep Packet Inspection (DPI); it can operate in software in situations where traffic levels are low, but for high traffic levels (as when monitoring all communications by very many users), specialised hardware must be deployed. All DPI software and hardware arrives with an inbuilt-knowledge of the main Internet protocols of the time and can perform basic analyses on a per-packet basis. But any additional features require the writing of specific filters. Where the analysis requires several packets to be considered for their effect together, as in the complex web-page and JavaScript etc. facilities described above, the capabilities of DPI equipment to handle large amounts of data automatically and rapidly are unknown.

DPI equipment can usually only work where the web page instructions and components are sent unencrypted. But services from the likes of Google, Facebook, web-based email, are now delivered in encrypted form – using https – not deliberately to thwart the police and Agencies, but to protect their users for eavesdropping by criminals. For practical purposes in these circumstances, the only entities that can separate communications data and content are the Googles, Facebooks, and owners of webmail services, which I have referred to as Social Network Service Providers.

Request Filters As noted above at paragraph 0, an apparent individual communication may involve several different CSPs, a typical example being webmail or social networking. A subscriber's Network Access Provider would only be able to capture the identity of the machine to which the subscriber was connecting – cl 28 (2) and (3). The Social Network Service Provider might recognise that a customer/member was in communication with another customer/member but might lack detailed and authentic knowledge of who that customer/member is. The NAP does know, however, because the subscriber is identified when they pay – by direct debit or standing order – for the network access service.

The Bill, cl 14-16 and ENs 73-93, envisages an entity separate from both the CSP(s) and the requesting law enforcement agency which analyses a specific problem, requests material from the respective CSPs which will probably include "content" along with "communications data" and then combines them so that there is a resulting clearer identification of who is communicating. The process, so it is hoped, will prevent the requesting investigating agency from seeing anything other than communications data. In terms of webmail it will enable the requesting agency to see that their person of interest, who is now clearly identified from data supplied by the NAP accessed the webmail service and via it exchanged emails (or other messages) with a number of individuals at particular times. But the requesting investigating agency would at no stage see the subject matter of the messages. This is also the explanation offered by Peter Hill at Q94.

Cl 14-16 have a number of safeguards in that necessity and proportionality tests must be applied throughout, there must be rigorous security, after the delivery of the filtered material any remaining material obtained by the Request Filtering Entity in the course of their work must be destroyed, and audit records kept for scrutiny by the Interception of Communications Commissioner. However if these safeguards are not rigorously applied and fully examined by the Interception of Communications Commissioner there is a risk that that what is described as "request filtering" becomes large-scale data mining; the necessity and proportionality tests need to be applied not to just the individual data streams as supplied by CSPs but to the likely effect when they are assembled together.
The main purpose of this complex arrangement seems to be to protect CSPs and law enforcement agencies from the situation where the requesting investigating agency inadvertently receives "content" with the consequences indicated at paragraph 0 above.

Doubt must also be expressed about the credibility and viability of the entity that performs the Request Filter. Could it really be the same Secretary of State who also issues interception warrants under RIPA Chapter 1 and who also issues the Orders under cl 1 of the Draft Bill? If it is to be a separate "designated public authority" as suggested in cl 20(1) it will need resources, among them highly skilled staff who are familiar with the law, the applicable technologies and police investigative procedure – and who can also act independently. They will almost certainly need high levels of security clearance. In the private sector such people are likely to earn fairly high income; moreover they will want some form of career structure and stability. But there may not be a sufficiently consistent flow of work to make this possible.

Practicalities and Interpretations

The process of separating communications data from content is thus theoretically as follows:

- In the first place the communication must be viewed as the participants would normally see it and the legal definitions in clause 28 (2-5) applied.

- This must then be converted into instructions which the DPI interception equipment can implement; this in turn implies a full understanding of the various protocols in use for the main Internet services as well as the construction of certain web pages which contain both communications data and content.

Some aspects may be easier than others, for example cl 28(2)(b)(iii): "comprises signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of the communication". This sub-clause more-or-less reflects something that can be recognised at a technical level. But others do not.

The Bill has a number of clauses in this area that look as though they are capable of several interpretations. For example cl 28(3):

Data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication is not "traffic data" except to the extent that the file or program is identified by reference to the apparatus in which it is stored.

This is borrowed from s 21(6) RIPA, 2000. One particular problem is the status of web pages within a website – the identity of the website is communications data, the web pages within it are content, but what happens if the filename of the web page gives an indication of its content? An example: http://www.independent.co.uk/news/uk/crime/rebekah-brooks-and-andy-coulson-conspired-to-hack-milly-dowler-and-600-others-7966265.html

Or cl 28(4):

"Use data" means information—(a) which is about the use made by a person—(i) of a telecommunications service, or (ii) in connection with the provision to or use by any person of a telecommunications service, of any part of a telecommunication system, but (b) which does not (apart from any information falling within paragraph (a) which is traffic data) include any of the contents of a communication."

What would be the position of a website which builds up a profile of its customers' activities in order to make them future offers based on previous sales – like Amazon? Or a social networking site that similarly collects information about its user so that inter alia it can make recommendations? Both Facebook and LinkedIn frequently suggest "People You May Know" as suitable to add as "friends" – based on previous activity.

Simple interpretation of web pages generated by social networking sites such as Facebook may also be surprisingly difficult; here there can be significant problems in identifying which elements on a web page are communications data as opposed to content even before we attempt to turn these into technical instructions. Do we take it that the identities of posters are "communications data" and what they say (or pictures they put up) is "content"? What is the effect if some postings are only available to selected viewers – "Friends" - as opposed to being published to the world at large? What is the position of one-to-many communications but which still fall short of general public publication?

Implications for clause 1 Orders
The structure of the Bill is that it is provides a framework, with the detail to be covered by Orders to be issued by the Secretary of State. EN22 sets out the intentions:

In practice, it is likely that an order under clause 1 may, amongst other things, impose requirements on operators to: generate all necessary communications data for the services or systems they provide; collect necessary communications data, where such data is available but not retained; retain the data safely and securely; process the retained data to facilitate the efficient and effective obtaining of the data by public authorities; undertake testing of their internal systems; and co-operate with the Secretary of State or other specified persons to ensure the availability of communications data.

Clause 2 sets out the requirements that Ofcom, the Technical Advisory Board (TAB) set up under s 13 RIPA (and which I understand has until now hardly ever met), and relevant stakeholders must be consulted. But the main democratic safeguard is supposed to be that Orders are subject to affirmative resolution by Parliament - cl 29 (2).
Given the pressures on Parliamentary time and material that will be technically complex and outside the normal experience of most Parliamentarians, it seems highly doubtful that detailed consideration will take place. Any such discussion would require information about the precise nature of the threats and, based on what ACC Gary Beautridge said to the Committee in oral evidence (Q 152), the police will want to discourage public debate as they fear that might inform criminals and others of gaps in law enforcement capability. In effect, Parliamentary affirmative resolution will not be a safeguard.

Costs, Value for Money
The Impact Assessment accompanying the draft Bill estimates costs to be £1.8bn for the 10 years from 2011/12 without allowing for inflation, VAT and depreciation. The main assumptions are: the total volume of internet traffic increases tenfold over 10 years, CSPs retain data for 12 months, data storage costs decrease by 25% per annum. Of the £1.8bn, £859m is the estimated cost to the private sector – CSPs of all kinds – and which will be paid for by the Home Office. The balance is made up of costs likely to be incurred in management and facilities by law enforcement and the agencies and in oversight by the Interception of Communications and Information Commissioners[490].

One of the unfortunate features of the Impact Assessment is that the only bodies listed as formally consulted were the users of communications data, as opposed to the CSPs who are expected to provide it[491]. It is puzzling how costs could be calculated without their input.

Forecasting anything to do with the Internet is fraught with uncertainty. Looking back over the last 10 years one must point out that the earliest manifestation of Facebook, one of the key concerns behind this Bill, dates from 2004 and was only opened to the public-at-large in 2006. MySpace, its predecessor in popularity, was founded in 2003 and in June 2006 was more-visited, at least in the US, than Google[492] but it was overtaken by Facebook by April 2008 and by August 2012 had declined to being the 166th "most visited" Internet site[493]. Twitter dates from March 2006, Google Apps, its consumer orientated cloud service of email, online calendar and remotely-stored and editable documents was fully launched in July 2009[494]. Skype, often cited as a particular problem for investigators, was founded in 2003 and has been through a number of versions.

---

[490] See also Charles Farr's reply at Q73.

[491] Paragraph A3 of the Impact Assessment.

[492] http://news.cnet.com/Googles-antisocial-downside/2100-1038_3-6093532.html

[493] http://www.alexa.com/siteinfo/myspace.com

[494] http://googleblog.blogspot.co.uk/2009/07/google-apps-is-out-of-beta-yes-really.html

Cost and Benefit Estimates

The Home Office Impact Assessment seems solely based on increases in the total volume of Internet traffic, not on its increasing complexity and level of change, which is what any form of separating of communications data from content will have to be concerned with. Even forecasts of traffic volumes over 10 years are problematic; looking simply over the next three years much will depend on the rate of roll-out of high-speed fibre-based links (which by themselves would encourage greater usage) and also to take-up of video-on-demand services, in which customers see films not over the air (terrestrial, satellite, conventional cable) or by renting DVDs, but by receiving video over the Internet. [495]

Similar doubts must exist of the estimate of benefits, which are suggested as being between £5 and £6.2bn. The Impact Assessment says:

These benefits are assessed by operational stakeholders and, using a model validated by HM Treasury, translated into economic values. The assessment takes into account an analysis of criminal behaviours by the Serious and Organised Crime Agency and an analysis of the future communications market based on OFCOM and other market sources. The largest categories of benefits are direct financial benefits arising mainly from preventing revenue loss through tax fraud and facilitating the seizure of criminal assets. Values for benefits for example from lives saved and children safeguarded are derived from standard estimates by Home Office economists.

But if we turn to the main Home Office Research document cited[496] many caveats are made:
Whilst information on the total and average costs of crime is extremely useful, average cost of crime estimates in this study need to be treated with some caution, for a number of reasons.

> _ *Different crimes within the same offence category are likely to have vastly different costs.*
>
> _ *Particular crime reduction initiatives may impact on different types of crime within the same offence category.*
>
> _ *Average cost estimates given…. are best estimates of costs given the information available. However, due to lack of good information in a number of areas, the estimates are inevitably imprecise.*
>
> _ *The costs of an identical crime may fall differentially on different social, economic or geographic groups –*
>
> _ *Some crimes are inevitably costed less accurately than others, and unquantified costs exist which may differ between crimes.* A *comparison* of average costs between different crimes could therefore be misleading. A higher average cost for one crime than for another could reflect the size of quantified, rather than unquantified costs, rather than a real difference in the costs of the crimes to society, although to some extent this is unavoidable in an exercise of this nature.

The Impact Assessment's "benefits" have a further problem: they are claims about what would result from the increase in access to communications data over what is currently already available.

Whatever the size of the costs and benefits, the Impact Assessment makes a further assertion: "The proposed 10 year investment in communications data capabilities of £1.8bn compares with an annual cost for policing alone of £14 billion." But this is for every aspect of policing; it may be more realistic to look at the front-line organisations dealing with serious crime. SOCA's resource expenditure in 2011/12 was £427.9m, with a further £34m in capital expenditure[497]. A further basis for comparison is the UK's Cyber Security Strategy from

[495] See the House of Lords Communications Committee Report: http://www.publications.parliament.uk/pa/ld201213/ldselect/ldcomuni/41/4102.htm

[496] http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/pdfs/hors217.pdf

[497] http://www.soca.gov.uk/about-soca/library/doc_download/392-soca-annual-report-and-accounts-201112.pdf

November 2011.[498] The National Cyber Security Programme has a budget of real new money of £650m for the four years 2011-2015, of which only 10%, £65m, will go to the Home Office for "tackling cyber crime". Out of this comes a specific budget for the police: the new National Crime Agency will include the existing Police Central E-Crime Unit, the existing SOCA e-crime and CEOP, the child online protection group. On this basis the estimated costs for the proposed Communication Capability Development Programme begin to look rather large.

Source of Funding for CCDP

Even if costs are difficult to calculate it is possible to identify criteria for value for money. One of the great weaknesses of the Bill and the policies behind it is that nowhere has there been any explanation of the source of the required funding. The government is currently seeking reductions across the whole of public spending costs of 20%, including the police. It seems a reasonable assumption that similar cuts will be expected from the Security and Intelligence Agencies. Only unambiguous evidence of new and growing threats would overcome this. But overall crime is down[499] and the last deaths in the UK from terrorism were in 7 July 2005, although of course this cannot be the sole indicator of level of threat.

If we assume that the CCDP will have to be funded from existing resources, the question then arises: which current areas of expenditure will have to be further curtailed beyond the 20% across-the-board savings already demanded? There seem to be two broad choices, either from every form of government expenditure – education, health, defence, transport, social services, etc. – or more specifically from the police and Agencies. One suspects that the police in particular will have reduced enthusiasm for CCDP if they have to partially fund its infrastructure costs.

Essential Criteria for Success

If CCDP is to be successful, or value for money, it must have a number of features, not all of which are explicitly referred to either in the Explanatory Notes or the Impact Assessment:

DPI equipment must not slow down the Internet experience At present CSPs are simply required to retain business records which fall into the definitions of "communications data". The Bill requires them to process it (see paragraphs 0 ff) and as we have seen these processes can be quite complex; without very high-speed equipment – which implies expense – the user's experience of Internet browsing will be slowed. This outcome would directly conflict with other aspects of Government policy, including that for superfast broadband.[500] DPI equipment installed now would need to be upgraded as fibre-based delivery services are rolled out

Monitoring must be near-complete The avowed aim of data retention is that once an individual, hitherto thought innocent, comes under suspicion, investigators are able to discover their past online activities. Although 100% availability of retained communications data seems infeasible, each 1% per cent drop surely significantly weakens the benefits as one must expect that those who wish to conceal their activities will take evasive action. A 90% coverage would incur significant costs but might only capture the activities of the wholly innocent. Thus, every UK ISP, no matter how small, would need to be covered, unless that ISP was only able to function by being a client of a larger, UK-based ISP.

The Home Office's position here appears confusing. At Q9 Charles Farr speaks of hoping to get, by deploying CCDP, up to 85% of "coverage" which presumably refers to 85% of communications data being transmitted in and through the UK. Richard Alcock at Q77, says the same but at Q82 says:

---

[498] http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

[499] http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/period-ending-march-2012/stb-crime-stats-end-march-2012.html

[500] http://www.culture.gov.uk/publications/7829.aspx

In terms of the general number of CSPs, just in the United Kingdom, I think it is in the order of 250 to 300 communications service providers. We certainly do not envisage working with that many within the piece. Clearly, it depends how communications services change over time and whether groups gravitate to a certain service or not. But we certainly do not envisage working with everyone, and I estimate it will be a relatively small proportion of those. (emphasis added)

This lack of clarity about intended scope of coverage looks odd against the suspiciously precise projected cost of payments to CSPs of £859m.

Evasive measures In addition, the proponents of CCDP will need to explain how they would address the obvious easy routes to evading attention:

- Bought-for-cash pay-as-you-go-SIM, giving anonymity
- Use of Internet cafes and other public access services (unless it is assumed that the owners of these services will keep elaborate verified records of the identities of all their customers)
- Hi-jacking of unencrypted domestic Internet access points (with the result that the Internet activity is attributed to the registered subscriber)
- Use of encrypted webmail and other services from providers outside the UK and with whose law enforcement agencies the UK does not have close working relationship
- Use of small NAP/ISPs, thought unlikely to be asked install the DPI monitoring equipment

There are other methods of evasion but the above require no skill on the part of the user, other than to know that the route exists

How will encrypted services be handled? As we have seen, an increasing number of large important services are now encrypted, using https – see paragraphs 0 and following above. There does not appear to be a routine means of decrypting and hence getting access to anything that might be communications data. HTTPS is fundamental to Internet-based e-commerce and e-banking. In the course of a targeted investigation it may well be possible to obtain the co-operation of the encrypted service as there will then be evidence upon which judgements of necessity and proportionality can be made[501]. But CCDP is about the routine retention/collection of data from the whole population and in the absence of specific suspicions.

A possible solution would be for the CSP to retain all data that appeared to be encrypted and to make no attempt at separating communications data and content until there was a specific request. However, given the quantities of encrypted transmissions, CSP storage costs would soar. But Richard Alcock, Q47, seems to say that RIPA would not allow this, presumably as content, even if encrypted, cannot be retained.[502] And most versions of https can only be intercepted at the time encrypted messages are sent, using a "man-in-the-middle" attack.

How will overseas CSPs be dealt with? The UK appears to have two routes to dealing with CSPs outside the jurisdiction. The first is to seek their co-operation, a view reflected in Charles Farr's response at Q52: "The central plank of this programme is a collaborative relationship with service providers in this country and overseas. DPI, black boxes, or whatever other metaphor or language we choose, only come into play in certain circumstances when an overseas provider or the state from which an overseas provider comes, or both together, tell us that they are not prepared to provide data regarding a service which is being offered in this country and which we knew and know is being used by criminal elements of whatever kind." This incurs relatively low

[501] There are also other technical routes which are available in a targeted investigation in the event of non-cooperation from the service provider

[502] It is possible that the uncorrected transcription on which I am relying is not wholly accurate at this point.

financial costs but may involve persuading the CSPs that the legal and regulatory framework for issuing requests is fair and rigorous. See my remarks at paragraph 0 above and 0 below.

The second route appears in the same answer: "The legislation therefore creates the option, in those circumstances, of putting a black box, using your language, on a UK network across which the data from the overseas provider must move, with the purpose of sucking off that data, under our guidance—"control" is too strong a word—and storing it through that network provider." In other words a form of filtering based on that service. At Q54: he says: "The network provider would take off the network the data particular to the service of concern to us and store all that data. We would then apply to the network provider for specific bits of the data that has been so stored, in accordance with usual practice." This would incur expense and the Joint Committee should make further enquiries as to its likely level.

Many of the big overseas services with which we assume there is the greatest concern, like Google, Live/Hotmail, Twitter, Facebook, etc. use encrypted links, in which case this second route would have very limited effect.
Benefit Elements

The Home Office express the benefits in terms of globalised percentages, saying that they hope to move from a 75% availability to 85% (Q9). At Q22, Charles Farr produces a percentage breakdown of applications for communications data, presumably based on existing law.

27% of data for which applications are made and obtained is for drugs-related offences, 15% is for property offences, arson, armed robbery, theft, 12% is for financial offences, 10% is for sexual offences, 6% is for homicide, 5% is for missing persons, 5% is for harassment, 4% is for offences against the persons, and 4% to 5% is for explosives.

But what is really required, if there is to be a proper value for money assessment, is the ability to identify particular types of communications data originating from particular classes of communications service provider. Many existing highly useful forms of communications will continue to be available for the reasonably foreseeable future – including mobile phone location (which is not Internet dependent) and, from Network Access Providers, the ability to link IP addresses obtained by a variety of means to the identities of their subscribers. What is needed is a way of identifying the specific forms of further communications data that CCDP will deliver – so that it can be related to the costs of acquiring it.

One purpose of setting out the various types of CSP and the classes of data they might produce in paragraphs 0 to 0 above was to assist the Joint Committee in gaining a better ability to assess these separate elements. I note the remarks of ACC Gary Beautridge to the Committee in oral evidence (Q 152) and have some sympathy with his concern not to expose current law enforcement weaknesses. But I hope the Joint Committee will pursue with vigour and carefully test any confidential information supplied to it by ACPO and others.

Cost Elements
DPI Boxes The first cost element, to be paid for by the Home Office, is the installation of the DPI boxes at NAP/ISPs. Because one must anticipate attempts at evasion by those of greatest interest to the authorities, this investment will have to be front-loaded. That is to say, near 100% coverage of UK NAP/ISPs will be required not too long after the intended start-up. Although the Home Office speak of wishing to run pilot studies, usually an important means of testing a policy, the pilots could not show how well CCDP was meeting the threats of evasion. This significantly increases the risk to the taxpayer.

As noted above, given the growth speed, and difficult-to-predict nature of the Internet DPI boxes would need constantly to be upgraded

Filtering Software As explained at paragraphs 0 to 0 above, the provision of filters to be run on the DPI hardware is likely to be an extensive and on-going project. It is not clear who will do the necessary research and

produce final products – GCHQ might be a candidate. This will still be a cost which has to be met from some budget or other ultimately funded by the tax payer.

CSP additional costs In addition to the costs identified in the ENs and Impact Assessment, the Joint Committee should ask CSPs about the costs of producing material from their archives of retained data at speed to meet likely emergency requirements from law enforcement. It is not enough that required communications data is simply kept, it must also be available; and that implies some near online capability. Mobile phone companies, on whom there are frequent demands but where the normal requests are very standardised – calling number, receiving number, date/time, call duration, IMEI, IMSI, location – have automated or semi-automated systems. Will something similar be required of other types of CSP, and what will be the cost implications?
Open-ended nature of CCDP

The following elements are highly difficult to forecast: the growth in Internet traffic volumes, the levels of complexity of future Internet services, the numbers of CSPs, and the extent of attempts at evasion. If allowed to proceed in in anything like its current form CCDP will have all the pre-conditions for an uncontrolled government computing project or MoD defence contract. Its details will be shrouded in secrecy in order not to give criminals and others an advantage, any associated contracts will be hidden from scrutiny as "commercially confidential" and the precise specification will be subject to constant change. This is the classic formula for runaway costs and hence a significant risk to the taxpayer.

Possible Alternative Legislative and Policy Routes

I hope it will help if I sketch out some alternatives to the proposals in the draft Bill.
Intrusive Data Monitoring Warrant A more radical form of legislation would almost certainly have to abandon the attempt to separate communications data from content, so that an intrusive data monitoring warrant would cover both. This would mean that the peculiar UK position of making intercept evidence inadmissible[503] would also have to be abandoned. RIPA already features directed and intrusive surveillance regimes – s28 and s 32 respectively. The test for granting would depend on the levels of intrusion rather than a technical assessment of whether data was "communications data" rather than "content".

Any new power along these lines would almost certainly have to be subject to judicial scrutiny as opposed to the current position where warrants are issued, for historic reasons, by a Secretary of State acting on behalf the Crown. I am aware the arguments for and against of warrants issued by a Secretary of State and of the similar arguments about self-authorisation by designated senior officer in relation to communications data.

Data Retention of Business Records This would be very similar to the current position where CSPs retain records that they create in the normal course of their business and which would include "communications data" as currently defined in RIPA or EUDRD but would not require them to do any further processing.

I would favour passing power this over to judicial scrutiny as well, not the least for the reasons now explored below.

Position of Overseas CSPs, including SNSPs As we have seen, much of the material which the authorities hope CCDP would make more available is held by CSPs based outside the UK. It seems much more sensible to seek their co-operation rather than relying either on Mutual Legal Assistance Treaties, which can be cumbersome and too slow to be effective, or to hope that the data can be monitored while in transit in the UK. But to do this may require convincing SNSPs that UK legal procedures are fair and transparent. As noted above, SNSPs will need to consider their position under the laws of their home jurisdiction, usually the United States, and also the perceptions of their world-wide customer base.

---

[503] S 17 RIPA

Judicial supervision is far more common and understood worldwide than then UK practices of a politician to grant warrants for the most intrusive activities and self-authorisation by senior law enforcement officer for the rest. For that reason alone, judicial supervision is likely to be more credible and persuasive.

There is a further element: companies like Google, Facebook hold large amounts of personal data about their customers and do so with their consent. Cloud providers hold files created by their customers. In these circumstances the assessment of proportionality becomes especially important. Should a warrant automatically give access to all the material the cloud provider holds? To my knowledge this issue has not be examined in any detail anywhere in the world.

Enhanced role of Commissioners Also as part of a policy of convincing SNSPs and others of the rigour and fairness of UK procedures, there surely needs to be a more visibly robust regime of Interception of Communications and Information Commissioners. Information Commissioners have always had a public profile, appearing on television, engaging in debate and making public demands for law changes and increased resources. Interception Commissioners have until recently been almost invisible. The most recent report[504], for 2011 provides more detail and candour than hitherto, but the Commissioner held just one meeting outside a wholly official environment, with the specialist Data Protection Forum.

Although his Report describes how he audits the activities of the police, Agencies and other bodies, it is unclear how far he questions the reasoning and evidence of the "necessity and proportionality" tests that are the starting point for each warrant/authorisation. If he doesn't he should do so – and identify situations where matters went awry. Obviously any review of such tests would have to be on the basis of information available at the time. The Commissioner could also usefully describe in more detail the resources and skills of his inspectors. Consideration should be given to moving this role into the Information Commissioner's Office, where it might be less easily perceived as "captured" by the law enforcement and intelligence agencies it is supposed to be overseeing.

The Investigatory Powers Tribunal is even less visible, and hence less credible, than the Interception of Communications Commissioner. It would have much greater perceived independence and credibility if reconstituted directly under the control of the Supreme Court (as is the US Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Appeal), with more transparency.

A new type of retention warrant? One can also envisage a new type of warrant, also issued by a judge, on the basis that although an individual who is not currently presenting sufficient of a threat to justify full scale monitoring there was the possibility by virtue of people whom they knew or views they were thought to hold, it might be useful if the ISP were to retain their communications and content for a period of year against the future possibility that the police or other investigators produced a full warrant to view the material. This would address a problem identified by investigators that on occasion they identify a substantial conspiracy in an advanced stage and wish to know something of the previous actions and thoughts and associates of those thought to be involved. However this last proposal has many difficulties associated with it – what would be the actual criteria for the issuing of such a warrant and how would it be supervised? But it would have the further advantage of being targeted – effort and expenditure would be directed against those who might in the future be of interest, as opposed to the 99.5% of the population who never will be.

I would be happy to answer any questions the Joint Committee may have.

August 2012

---

[504] http://www.intelligencecommissioners.com/docs/0496.pdf

Dr Eric Stoddart

Summary

i. A sophisticated test of proportionality comprises four dimensions. A simple one-question test is inadequate for this Bill.
ii. An holistic model of communications data is required in order to appreciate the *assemblage* of surveillance data. It is a mistake to consider information retained as merely many instances of discrete data points.
iii. A relational, performative understanding of the self challenges attempts to bifurcate communications data from message content; both are integral to forming the self and thus demanding of privileged protection.
iv. An adequately resourced warrant system for instituting searches of retained data is recommended.
v. The capacity to retain everyone's communications/content data is acknowledged but it is proposed that this be actioned only by warrant towards targeted persons.
vi. The wholesale retention of everyone's communications data is rejected.

The author is Associate Director of the Centre for the Study of Religion and Politics, and a lecturer at the University of St Andrews, Scotland. He is the author of *Theological Perspectives on a Surveillance Society: Watching and Being Watched* (Aldershot: Ashgate, 2011) and writes here in a personal capacity.

A sophisticated proportionality test.

1. The government repeatedly claims that the proposals in the draft Bill are 'proportionate'. Quite what this means and whether it can be applied as a single test across the Bill in its entirety are questions largely left aside. I contend that there are at least two separate tests of proportionality required here: (a) considering the indiscriminate retention of communications data beyond that currently held by CSPs for business purposes, and (b) the proposal that databases be searched, albeit mediated by a filtering system, without a warrant. Furthermore, a proportionality test does not comprise only one question. Although there is no precise legal formulation for such a test, its use in the review of cases under the UK Human Rights Act has generated typically four sub-questions. These address the legitimate objective, rational connection, minimal impairment and overall balance.[505]

2. The first sub-question asks **if the objective is sufficiently important**. This is immediately problematic in this Bill because there are multiple objectives scooped-up within the initial overall aim of 'protecting the public' (stated in the initial Home Office press release prior to the Bill later being published). This aim becomes, 'to protect the public and bring offenders to justice,' in the Home Secretary's foreword to the Bill. When Assistant Commissioner Cressida Dick gives her oral evidence she refers to the value of communications data in cases of abduction, locating suicidal persons, and tackling gun crime, robberies and rapes (wherein mobile phones are often stolen).[506] The scrutiny committee has already been exercised over the objective of tackling a 'serious' crime - for which no legal definition exists - and recognizes that 'serious' is a subjective and contextual designation.

3. It means very little to settle questions of proportionality at the general level in which this Bill is worded. Proposers and supporters of the Bill are mistaken if they believe that proportionality tested at a very general level can be treated as if it were a trickle-down effect. Whilst an instance of alleged gun crime might be of considerable seriousness to a particular community such contextual specificity should not be deemed to be proportionate in relation to the mass and indiscriminate retention of the population's communications data. Neither ought the devastating human cost and tragedy of incidents of this kind be deemed, as it were, to generate a 'trickle-up' effect to the proportionality test.

---

[505] Alan D.P. Brady, *Proportionality and Deference under the UK Human Rights Act: An Institutionally Sensitive Approach* (Cambridge: Cambridge University Press, 2012).

[506] HC 479-iii, q.150. (Neither witnesses nor Members have had the opportunity to correct the record. The transcript is not yet an approved formal record of these proceedings.)

4. The whole question of legitimate objective within a proportionality test is further complicated for, in operational practice, unacceptable discretion is handed to a designated senior officer to determine proportionality. The actual point at which proportionality is tested is not in Parliament but at the desk of an officer within what, as witnesses to the Committee have already alluded, might be a 'canteen culture' of minimal scrutiny or within a paradigm that gives the benefit of the doubt too-readily to institutional objectives over individual rights and/or the public interest.

5. The second proportionality sub-question asks **if the measure is appropriately connected to the objective.** At both the general level of the Bill and in operational contexts this question could be easily answered in the affirmative. Communications data is so clearly relevant to monitoring the behaviour and actions of networks of people and individuals suspected of or involved in any level of criminal activity. This dimension of the proportionality test ought not be invested with too much importance because so to do would give a false impression that over-simplifies questions of proportionality. In other words, the sub-questions do not contribute equally to the overall test. The test of rational connection is both easier to answer and of lesser importance; an invidious combination of features when some incidents, such as the London riots of 2011 or child abductions stir the public imagination.

6. A third sub-question **expects minimal impairment**. We, the public, want assurance that the measure goes no further than is necessary to achieve the objective. This is particularly contentious and difficult to answer convincingly given the paucity of longitudinal studies into the effects of being under mass surveillance. If the systems were able to retain the data of *anyone* then a strong case could be made that targeting a specific person or communications device is legitimate (in just the same way as warranted covert surveillance under existing legislation). The problem for proportionality is that the system retains the data of *everyone* to enable retrospective analysis and rapid (if not real-time) tracking of a device and a network of communicants.

7. What is happening is that notions of prevention, precaution and pre-emption are assuming ever-increasing importance. The new paradigm of precaution adds further dimensions to responsibility (for ourselves and others) and solidarity (where the cost of damage is shared across society and business by compensation and insurance systems). Concerns over irreparable and catastrophic damage lead us to expect precautions to be taken and sanctions to be in place for those people who not only fail to heed available knowledge but risks that ought to have been suspected as demanding pro-active attention.[507] We endeavour to *prevent* a terrorist crime by guarding vulnerable sites and scrutinising travellers and their luggage. *Prevention* focuses surveillance but *precaution* diffuses it because we know that there exist threats of which we are, as yet, unaware. *Pre-emptive* action is therefore expected of those charged with preserving our security and safety.

8. An otherwise proper precautionary approach can leech into culture in such a way that it contaminates our attitudes and mutates into an illegitimate defence of pre-emptive 'responses'. We see this in crime control where a public health conception 'requires the pre-emptive identification and management of "risky individuals"'.[508] In the context of mental heath services charged with similar pre-emptive analysis, Nikolas Rose observes that an agenda of protecting society may obscure the need for protecting *from* society when prejudice is stoked by fear of those who are different and vulnerable.[509] Without judicious handling, intervention policies to pre-empt people's action become deterministic. In other words, the future harm is presented as inevitable in the light of which pre-emptive strikes (as in military action) or intervention (as in gathering data on whole populations from which a 'threat' *will* emerge) are legitimated.[510]

---

[507] François Ewald, 'The Return of Descarte's Malicious Demon: An Outline of a Philosophy of Precaution', in Tom Baker and Jonathan Simon (eds.), *Embracing Risk: The Changing Culture of Insurance and Responsibility* (Chicago & Longon: University of Chicago Press, 2002), 273-301.

[508] Nikolas Rose, *Powers of Freedom : Reframing Political Thought* (Cambridge: Cambridge University Press, 1999), 7.

[509] Nikolas Rose, 'At Risk of Madness', in Tom Baker and Jonathan Simon (eds.), *Embracing Risk: The Changing Culture of Insurance and Responsibility* (Chicago & Longon: University of Chicago Press, 2002), 209-37.

[510] 'Through the pre-emptive lens the future becomes an inevitable series of events, elevating "fate" to an agent of historical evolution,' Greg Elmer and Andy Opel, 'Pre-Empting Panoptic Surveillance: Surviving the

9. The myth of pre-emption is the state's response to having its cover blown when terrorists, other criminals or deranged individuals commit acts that demonstrate how little real order and control a state can exercise over its territory.[511] The irony is that a public who feels the need for pre-emptive action such as data-gathering is itself then designated as the site from which such risky-individuals emerge and thus blanket surveillance of *everyone*, not just *anyone* is expected.

10. We simply do not know what effect on general and local populations accrues from a vague awareness that they are under mass surveillance. Whether or not it matters that monitoring and analysis of the data is performed by software rather than directly by human analysts is also under-investigated. Much, in this sub-question, depends on the time-scale over which impairment is to be tested. It is quite possible that the Bill as envisaged has little adverse effect on the public's behaviour if measured on a day-to-day basis. Broader and long-term effects of a culture of surveillance could prove to be much more damaging. Scholarly discussions of a 'risk society' and the designation of 'risky individuals' suggest that narratives of precaution, pre-emption, and prevention could turn out to be more detrimental than previously thought.

11. The fourth proportionality question asks **if, overall, a fair balance was struck between the rights of the individual and public interests**. 'Balance', as Lucia Zedner points out, is another notion that can easily obfuscate assumptions that need to be made transparent. Before we can conclude that a *fair* balance has been struck we need to ask what has tipped the balance, in whose interests the balance has been secured and what lies in the scales?[512]

12. In this case the disequilibrium to be addressed is one over the shift to digital and mobile communications devices that generate data that escape the purview of police and security services. However, the estimates of the 'data gap' need to be read against a backdrop of both a culture of fear and of precaution. It is too easy to set up a 'them' and 'us' (whose interests have been forfeited through criminal action, intent or suspicion). I agree with Zedner that we offer ourselves a false sense of security that we will never be amongst those who fall foul of surveillance activities by the state. Drawing on the example of the limitations on the right of silence (arising in the specific context of terrorism in Northern Ireland), Zedner warns that emergency measures have 'an uncanny way of being perpetuated beyond that emergency and extended to offences of lesser gravity'.[513] Plans to further standardise communications data across Europe to more easily facilitate lawful interception are significant in this regard too.

13. When it comes to asking what lies in the scales, known interests (such as privacy) are weighed against future uncertainties; what can be understood as 'temporal dissonance'.[514] The uncertainties of security are themselves of two conditions: objective (being protected from some harm) and subjective (psychological state of being fearful). It is vital that 'balancing' is itself viewed critically for it assumes that, 'even those aspects of our life most closely associated with our status as free and equal, is, in principle, up for grabs'.[515] The stakes are high here for all of us. By treating human rights as *quantities* of freedom it is easy to forget that those rights serve a more fundamental purpose in protecting our status as moral agents.[516]

Inevitable War on Terror', in David Lyon (ed.), *Theorizing Surveillance: The Panopticon and Beyond* (Cullompton, Devon: Willan Publishing, 2006), 139-60 at 144.

[511] David Garland, 'The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society', *British Journal of Criminology,* 36 (1996), 445-70, Gabe Mythen and Sandra Walklate, 'Criminology and Terrorism: Which Thesis? Risk Society or Governmentality?', *British Journal of Criminology,* 46/3 (May 1, 2006 2006), 379-98.

[512] Lucia Zedner, 'Neither Safe nor Sound? The Perils and Possibilities of Risk', *Canadian Journal of Criminology and Criminal Justice,* 48/3 (2006), 423-34.

[513] Zedner, 'Neither Safe', at 515.

[514] Zedner, 'Neither Safe', at 516.

[515] Stavros Tsakyrakis, 'Proportionality: An Assault on Human Rights?', *International Journal of Constitutional Law,* 7/3 (2009), 468-93 at 489.

[516] Tsakyrakis, 'Proportionality', at 490.

14. 'Fair balance' within the proportionality test could be defended where objective harm is being prevented. Quite whether this is a fair balance *overall* is another matter altogether. Communications data retention of *everyone* rather than merely *anyone* is at the heart of not only this Bill but an approach to governance that saturates a British response.

An holistic model of communications data.

15. The Bill is predicated on a distinction between communications data (subscriber, usage and traffic) and message-content. In this way, the Bill's proponents and defenders believe that concerns over individual privacy are unwarranted; rigorous data protection regimes being suitable safeguards. The assumption that information can be bifurcated into communications data and content is, I suggest, ill-advised and misleading. Such an approach fails to appreciate the nature of contemporary surveillance systems and, more importantly, neglects a properly relational understanding of the self. An holistic model of communications data that addresses these issues presents a serious challenge to the way in which the Bill is conceived.

The surveillance *assemblage*.

16. I do not dispute that knowing *that* I speak to X on a *given occasion* is generally less intrusive than what I say to X. However, to discuss 'communications data' *as if* this refers to single instances is misleading. Knowing that I speak to X nine times in one week, when I am in locations D & E, but not when I am at location F is beginning to compose a variety of possible impressions about me. Information that I speak to X always shortly after speaking to Y, perhaps with no other intervening communications enriches the picture. Add to this, information that I always visit pages P and Q of website T immediately after speaking to X, and a quite detailed profile emerges.

17. It is the *assemblage*[517] of different pieces of communication data that is, I would argue, akin to message-content data. Knowing about whom, when, where, to what sites, and with which devices a person communicates as *discrete* points of information are generally rather innocuous details. However, when assembled, and especially concerning not just one person but a number of people who connect with one another, the ground has shifted.

18. Whilst an authority might legitimately argue that privacy was not breached on any single occasion in the gathering of any discrete element of the data, I suggest that it is the *assemblage* that needs to be legitimated. Unfortunately, privacy and regulatory frameworks fall short because these generally conceive of occasions or discrete pieces of data rather than *assemblages* of information. Even more significantly, in the case of privacy laws, these were formulated when most details about us were ephemeral. As Helen Nissenbaum observes, 'information that was once scattered and transient may now be ordered, systematized, and made permanent'.[518] Data about our movements or connections with people was once possibly known to a few and observable by some more (but not too many) if they had the time and inclination; that situation has changed. With the ubiquity of mobile and other digital devices once obscure information about us is now made accessible.[519]

19. Am I saying that communications data and message-content are therefore the *same*? No, but what the theory of surveillance *assemblage* suggests is that we must discuss communications data (subscriber, usage and traffic) as *another kind* of message-content around which the Bill already concedes there must considerable safeguards against intrusion of privacy.

20. That 'content' is a much wider concept than is currently accepted is a view given even more weight once we start asking questions of the model of the self that is assumed within the Bill.

---

[517] Kevin D. Haggerty and Richard V. Ericson, 'The Surveillant Assemblage', *British Journal of Sociology,* 51/4 (2000), 605-22.

[518] Helen Nissenbaum, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public', *Law and Philosophy,* 17/5/6 (1998), 559-96 at 577. See also Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford Law Books, 2010).

[519] Daniel J. Solove, *Understanding Privacy* (Cambridge, Mass.: Harvard University Press, 2008), 189.

The relational and performative self.

21. A classic liberal model of the self will tend to posit an autonomous agent, abstracted from specific contexts and focus upon the individual as the primary (if not the sole) mode of being human. It is thus possible to see how the division between context and self might be carried over into similar thinking about communications as comprising (abstractable, detachable) communications data and (personal-)content data. To posit instead a relational self is not merely to acknowledge the importance of human cooperation, connection and shared interests. A relational model of the self contends that it is in relationships that the self is constructed. The implication for communications data being that these, just like the content of messages, are bound up with formation and reformation of the self; worthy thereby of similar protections.

22. There is no single conceptual model of the relational self. Although some alternatives to the liberal, autonomous, decontextualised agent ground the self in psychological and social relationships these may not be sufficiently critical of cultural expectations and particularly of the way power is deployed by institutions and social structures that seek to normalize us. For poststructuralists like Judith Butler we have no stable essential self; instead personal identity is an illusion because the self is performative.[520] In other words, by saying something we are doing something - not merely describing or reporting it.

23. The implications for attempts to bifurcate communications data and content of messages come into sharp focus not only when we consider our connectivity (our relationships) as intrinsic to our self-formation but once we appreciate that we are not *being* a self but *doing* a self. A communications-data/content dichotomy is untenable and indeed pernicious for the performative self. The performative speech-acts in which we continually make and re-make ourselves cannot be carved up into content, subscriber, usage and traffic components. All elements together and indivisibly form speech-acts. Attempts to disengage discrete components are political steps, particularly so when this affects those who live at the intersections of systems of economic, racial, gender, and class stratifications.

24. The problem does not, however, vanish if we are unable to concur with Butler's poststructuralism. Seyla Benhabib has argued for a socially-situated self and rational philosophical justification of universal norms.[521] Her narrative conception of the self is one in which we are constantly writing and revising our understanding of who we are as we engage with the self-reflective narratives of other people. We continue to be faced with the crucial point that who, when, for how long, where and with whom else we are communicating is integral, not extrinsic, peripheral or detachable from our mutually-engaging narratives.

Conclusions

25. A relational model of the self in conjunction with an appreciation of the *assemblage* of data leads to the conclusion that the current defence of the proportionality of the Bill's proposals is predicated on a mistaken bifurcation of communications data from message-content.

26. Setting it within a broader context of precaution and pre-emption, the Bill fails a sophisticated test of proportionality. Possibilities of function creep and greater standardizing of communication technology specifications at a European level only exacerbate the dangers in the government's proposals.

27. A system for retaining communications data and content is necessary. However, retention of data (beyond necessary business purposes) ought only be permitted upon the issue of a warrant.

28. Although the data of some innocent parties may be retained and searched during a specific investigation, procedures can be required for this data to be destroyed upon elimination of such an individual from enquiries. This approach would authorise the creation of a means of retaining and searching everyone's data but, crucially, its use would only be permitted in a targeted and warranted investigation.

---

[520] See, for example, Judith Butler, 'Contagious Word: Paranoia and 'Homosexuality' in the Military', in Iain Morland and Annabelle Willox (eds.), *Queer Theory* (Basingstoke: Palgrave Macmillan, 2005), 142-57.

[521] Seyla Benhabib, *Situating the Self : Gender, Community and Postmodernism in Contemporary Ethics* (Cambridge: Polity, 1992).

29. An important corollary follows: that the resources be made available to adequately train the magistracy in order that they might make informed decisions in a rapidly-developing field and, similarly, that information commissioners might provide robust oversight.

30. In sum, surveillance (as a tool and as a disposition) is to be constrained whereby although *anyone* may be monitored, not *everyone* is.

August 2012

Steven Taylor

1. "If you've got nothing to hide, you've got nothing to fear"

It isn't about what we've got to hide but about what we want to protect, i.e. our private thoughts and personal space, our private legitimate business and our personal details. No one would be happy if the government or the police wanted to install a CCTV system in their house just in case they one day suspect you have committed a crime, would they? Crime prevention arguments must not unquestionably override the privacy of law-abiding citizens.

2. "The police service needs access to this information to keep up with criminals and stop terrorists"

The police and intelligence services already have powers to place individuals suspected of committing crime under surveillance.
The draft bill however, would allow information to be systematically collected about everyone, effectively treating all law abiding citizen as suspected criminals.
Furthermore, this is not just about serious crime or terrorism detection by the police or secret services. Access to communications data is granted to local authorities and many other public bodies for a wide range of purposes that have nothing to do with crime fighting.
What's more, there are and will always be methods of communication that do not come within the State's reach. These range from the use of pay-as-you-go mobile phones to complicated encryption techniques not used by ordinary, innocent people but no doubt familiar to and widely used by serious criminals, who will likely avoid detection. Whilst the sensitive, personal and private data of many innocent people will be captured, serious criminals may be unaffected and go unmonitored.

3. "The Communications Data Bill won't change anything. It's already a requirement for some texts, emails and phone calls to be stored"

It is my understanding that his requirement is already problematic and the Government now wants to go much further. For the first time private companies will be instructed to collect information on billions of communications made by their customers for no other reason than the authorities' future demands for access. This amounts to mass, blanket, surveillance of the population outsourced to the private sector.
For these reasons courts in Germany, Romania, Bulgaria, Cyprus and the Czech Republic have found similar arrangements in their respective countries to be unconstitutional.

4. "It's not about the content - reading people's e-mails or listening to their telephone calls. It's about the 'who, when and where' of communications"

Fraudsters can steal a person's identity by simply sifting through a persons rubbish to compile a picture of their target from the fragments of information they retrieve. Your "communications data" trail can build up a very detailed picture of your life: who you have texted, emailed and telephoned on any given day; where you were when the contact was made and for how long; which websites you have visited in the privacy of your own home and more. In particular, web addresses can tell you an awful lot about a person – the state of their health, their hobbies or political interests.
This, together with the concerns expressed in the following paragraph, could expose innocent, law abiding citizens to unnecessary risks of fraud and/or identity theft which would be difficult to rectify due to the fact that access to the data-holding bodies by ordinary citizens would likely be restricted.

5. "Communications companies and the state will keep our personal information safe and never look when they're not supposed to"

If the data loss scandals of recent years have taught us anything, it's that the building of huge and unwieldy databases carries real and proven risks. In recent years the government has lost 25 million child benefit records

(mine amongst them) as well as the personal information of those serving in the armed forces, witnesses in criminal cases and prisoners. Local authorities have also used intrusive surveillance techniques simply to determine whether a family lived in the right school catchment area.
Building such a comprehensive database of the web habits of the whole population leaves us all at risk of bureaucratic error and fraud – something that will not be lost on the criminal computer-hacking community.

6. SUMMARY
I believe there are already sufficient powers in existence which are at the disposal of the police and other law-enforcement agencies to deal with suspected criminals and terrorists.

Effectively placing the whole population under surveillance is akin to using a sledgehammer to shell a peanut. It would be enormously costly and potentially so unwieldy as to be ineffectual.

The risks to the ordinary, law-abiding citizen from data loss, hacking and fraud should not be underestimated or discounted. No system is 100% secure and the more information held upon it the more likely it is to be targeted by hackers and criminals. Sensitive data has been lost previously which was supposed to be held securely.

Finally, I like to think that we still live in a civilised society where one has a right to enjoy privacy in one's private affairs. Previous generations fought wars against despots and tyrants who used similar mass data collection to control the populations in their countries. The introduction of this Bill would, I fear, put in place powers which could potentially have dark consequences for the future freedoms of every citizen in this country.

August 2012

Telefónica UK Ltd

GENERAL:

1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

Telefónica UK Limited (TUK) understands the issues the Bill is attempting to deal with and the communications from the Home Office has been comprehensive.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

TUK takes the privacy and security of its customer's data extremely seriously and has always responded responsibly and in a timely fashion to lawful, authorised disclosure requests regarding its own customers. The widening of the scope to include TUK's own customer's data that may not currently be held for business purposes appears to be a reasonable extension of today's powers. Widening the scope to ANY data that happens to traverse our network does not.

TUK is currently not convinced that all providers of UK communications will be treated equally and fear that UK based providers may find themselves disadvantaged by this Bill.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

TUK believes it offers a fairly balanced impact on the privacy landscape. The additional intrusion of extending access to ALL data is offset by the additional proportionality of the request filter and the additional oversight of requests from local authorities etc.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

TUK believes few lessons can be learnt from the approach of other countries.. The funding model adopted by the Home Office in addition to an adversarial justice system means that the UK law enforcement is one of the most sophisticated users of communications data in the World

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

TUK believes that the most cost-effective route forward is to extend current powers to include all data belonging to the Communications Service Providers (CSPs) customers whether collected for business purposes or not. Collecting transiting data introduces expensive duplication, drastically reduces the usefulness of the data collected and a harsh commercial imbalance in the communications industry.

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

Two pieces of legislation - one that clearly states **what** will be collected and the other that says **how** it will be accessed has worked well to date. The Draft Communications Data Bill (CDB), however, replaces the Regulation of Investigatory Powers Act (RIPA) part1, chapter 2, but also tries to over-ride the UK transposition of the European Data Retention Directive (EUDRD) by including new rules for what will be available to be retained, thus blurring the boundaries.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

Within the draft CDB the scrapping of all the odd pieces of legislation that communications data appeared to be authorised by IS a good quid pro quo.

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base? What might be the effect on business?

This bill is set to drive a commercial wedge between UK" public network" providers and the rest of the communications provision industry. At face value the Bill appears to place the responsibility wholly on the backbone network. The OTT players have already dis-intermediated the networks and the financial model upon which they were built no longer exists. This clearly places even more advantage with the OTT players and determines a business model where it makes economic sense to develop products and services outside the UK.

COSTS:

9. Is the estimated cost of £1.8bn over 10 years realistic?

Without further detail as to how this was calculated (and indeed how much of the draft CDB extreme potential will be utilised), TUK is not in a position to comment.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5 6bn. Is this figure realistic?

Without further detail as to how this was calculated (and how the decryption of proprietary encryption will be achieved), TUK is not in a position to comment.

SCOPE:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

The key to the effective use of the collection technology will be a very detailed definition of what is and what is not communications data in an Internet Protocol (IP) World. There is not sufficient clarity available as yet. The words used to describe communications providers are out of date and need updating to ensure there is no room for misinterpretation.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

The public authorities should continue to be limited to the police and certain government agencies that can prove their need under RIPA.

The Secretary of State should be able to vary the list and be able to remove any LEA who has abused the privilege.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

TUK does not believe the plans are at all robust. The spectrum of "overseas providers" goes from multi-national players who see the UK as a tiny percentage of their market and who will be unwilling to change their trading practices to suit, through to backroom application developers who will be impossible to locate.

USE OF COMMUNICATIONS DATA:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

No comment

15. Is the proposed 12 month period for the retention of data too long or too short?
Neither. Since the UK transposition of the European Data Retention Directive was introduced in the UK in 2007, 12 months has proved to be long enough to ensure that data is available long enough to be available for the majority of cases but not so long that a vast amount of innocent data is being held unnecessarily.

SAFEGUARDS:

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

A designated officer should be someone who is specifically trained to understand what he or she is authorising and the impacts thereof. The draft CDB also hands the determination of the correct type of request to the requesting officer. In theory it appears to be a good system.
Used correctly the draft CDB appears to be neutral with regards to Article 8 EHCR.

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

No - The warrant system is antiquated, laborious and offers no more security or assurance.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

More detail required.

PARLIAMENTARY OVERSIGHT:

19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

More detail required.

ENFORCEMENT:

20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

No clear definition of the penalties or how and when they will be invoked are given. It is, therefore, impossible to comment.

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

More detail required

TECHNICAL:

22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

Yes as long as sufficient detail on the definition of content versus communications data is agreed.

23. How safely can communications data be stored?

Communications data can be stored very safely but the complexity of the necessary security and the impacts of handling encrypted data increase the cost.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

TUK believes that it will be technically possible, if expensive, but a lot more detail is required to comment on appropriateness.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?

More detail required.

26. Are there concerns about the consequences of decryption?

There is likely to be a marked increase in the use of encryption if the Bill goes through as currently written. The decryption of the data to turn it into useful intelligence will be a major hurdle.

August 2012

Ernest F. Thornton

I hope you will forgive my intrusion into your deliberations but it is apparently deemed necessary to proceed further along the Orwellian road of people watching. May I take this opportunity to urge the committee to ensure that:

- safeguards, checks and appeal systems are robust enough to protect individual privacy and the right of defence under criminal law.
- the relevant public authorities are accountable and that future requesting authority cannot be handled by a private company (such as G4S) or some obscure quango.
- the Information Commissioner and Interception of Communications Commissioner and judicial authority have sufficient powers and resources to oversee and investigate in order that we do not have a repeat of the misuse of phone-tapping by some local authorities.
- since there is to be an appropriate contribution towards the cost to the telecommunications operator, which in effect means that the taxpayers will be paying for their email communication data to be recorded, will there be any limitation on the amounts paid?
- there is some policing of the duration of authorisations and filtered communications.

Thank you for providing the information that allowed this communication to be made and I wish you every success in striking a balance between protecting the rights of individuals and the interests of public safety or national security.

August 2012

Timico Ltd

Summary
The decision to pass new laws is very much the demesne of Members of Parliament. The decision of whether to pursue the Communications Data Bill will clearly be theirs.

This decision should be based on whether the potential loss of privacy to UK citizens is warranted by the possible gain in detecting and preventing crimes. Timico sympathises considerably with those working in the area of Law Enforcement but has serious concerns that we are going down a path that might better sit in a George Orwell novel.

Whilst it is probably technically possible to achieve many of the measures that might be envisaged for implementation it is unlikely that we have a good understanding of the total long term costs of the project.

There is also a concern that these measures will be insufficient to intercept communications between criminals intent on the most serious crimes as there will be many ways of avoiding detection.

Introduction

Timico is a successful business Internet Service Provider with its Headquarters in Newark in Nottinghamshire. Timico is what you might call a mid-sized ISP. Across the group of Timico companies there are around 25,000 broadband customers to who we also sell hosting, mobile, VoIP and other communications services.

Because of our size and the business nature of our customer base we have typically been overlooked by the Government/Ofcom when it comes to being subject to ISP specific legislation. For example we are not part of the initial tranche of ISPs covered by the Digital Economy Act although we could well be at a later phase. Although it is too soon to tell it is likely that we would also not initially be required to implement a Communications Data Act should the current Draft Bill ever get to that stage.

Preamble

Timico are members of the ISP Association and normally leave it to their expert hands to reply to Parliamentary requests for consultation. On this occasion however we consider the Draft Communications Data Bill to be one of such enormous consequences that we feel compelled to provide our own input.

It is recognised that the Security Services have a need for information that will help to solve or prevent crimes. A great deal of information is already available to these agencies and is already accessed via RIPA requests.

It is also recognised that the technological world has also progressed in the modes of communications being available to people. The plain old telephone call moved on to the call being made from a mobile phone, supplemented by text messages.

Today there are a huge number of ways that people communicate: social media platforms, email, instant messaging, video, online for a, Voice over IP, blogs and other websites. The amount of detailed information available about an individual could be extensive if we had the facility to collecting it all.

Concern #1 Loss of Privacy

Historically the data provided to Law Enforcement and other Agencies has been very targeted.

> Who owns this mobile phone number?
>
> Where was this mobile phone at a given time and date

Who owns the broadband line associated with this IP address

And so on…

The type of information available has been fairly limited but because of this the potential for damage through the leaking or loss of personal data has also been limited.

If we are now asking for what could effectively be a complete characterisation of an individual's personal life to be stored ready for retrieval then the scope for damage to a person's privacy is far greater if that data is lost or stolen.

Who stores the data is almost irrelevant. Storing the data at the ISP may (or may not) prevent access by individuals or Government who might exploit the availability of that data for unintended uses eg fishing for possible perpetrated crimes based on searches against attributes of known criminals. Where the information is stored is not the point.

The point is that it is physically impossible to totally secure this information. Where did Wikileaks get its information from? Whether it is down to insider involvement, corporate incompetence or failure to spot extremely unlikely scenarios as for example happened with the melt-down of the Fukushima nuclear reactors in Japan – surely an area of technological security that had the most reliable safety features built in.

We need to assume that the highly personal information being stored will indeed be leaked and for example published on a Russian website as recently happened with 6.5million LinkedIn passwords.
The question here is whether this is an acceptable trade-off for the benefits that might be accrued to the security of our country?

It could well be argued that many businesses already have a massive amount of personal information about individuals and all that is being requested in the Draft Communications Data Bill is that information similar to this is made available for the purposes of Law Enforcement. It might perhaps be reasonable to ask whether businesses should themselves be allowed to store such personal data.

Concern #2 Cost and technical feasibility

Because the Draft Bill does not go into the specifics of what is going to be asked for it is difficult to determine whether this will be technically feasible or not. On the basis that most technological problems can be solved if enough time and money are thrown at them we can probably say that whatever is asked of ISPs can *probably* be done.

Whilst it *may* be possible to intercept and store all the data requested, the nature of the internet is such that ways of circumventing these detection measures will be found. New email providers, new IM or social media platforms could be used that will inevitably involve an expensive and continuous process of maintaining the capability.

It is difficult to believe that the costs associated with this activity can reasonably be determined without understanding the scope of the work. Due to the nature of what is being pursued here the country could be looking at an expensive and endless task with a total cost that cannot be forecast.

Concern #3 Efficacy

As far as cost goes one might ask "What price preventing another 9/11?" which would be a very reasonable approach.

There is a more important underlying issue here that concerns whether spending the money would really have any effect. It may well be that some crimes would be solved where previously this would not have been the case.

However it is likely that most criminals or terrorists pursuing their goals knowing that Law Enforcement Agencies would be looking out for them would employ communications methods that would not be detectable. For example using proxy servers to hide their true location and using encrypted emails.
As an example of this, anecdotally the blocking introduced to support the Internet Watch Foundation is not considered to have prevented any paedophiles from accessing the unlawful material the blocks were supposed to prevent.

Also the BBC recently reported that the traffic to the Pirate Bay website had grown since the court order was issued making ISPs block access to the site.

http://www.bbc.co.uk/news/technology-18518777

This tells us that any technological methods employed to detect and control access to specific web entities can easily be bypassed.

Concern #4 Scope Creep

If we sweep aside any concerns regarding privacy, cost and efficacy then scope creep still remains as a worry.

The capability that would be put in place here would be extensive in its ability to collect information on people. Whilst the intention might well be to use this information in limited and controlled circumstances it is not difficult to envisage politicians in years to come seeing uses for the information that were not on the radar at the time the Act was conceived.

It isn't constructive to detail what such an extended use might be whether political or in support of private gain. However if the capability is not there it can't be done.

Conclusions

The decision to pass new laws is very much the demesne of Members of Parliament. The decision of whether to pursue the Communications Data Bill will clearly be theirs.

This decision should be based on whether the potential loss of privacy to UK citizens is warranted by the possible gain in detecting and preventing crimes. Timico sympathises considerably with those working in the area of Law Enforcement but has serious concerns that we are going down a path that might better sit in a George Orwell novel.

Whilst it is probably technically possible to achieve many of the measures that might be envisaged for implementation it is unlikely that we have a good understanding of the total long term costs of the project.

There is also a concern that these measures will be insufficient to intercept communications between criminals intent on the most serious crimes as there will be many ways of avoiding detection.

August 2012

The Tor Project

Background to The Tor Project and the Tor software

1 The Tor Project is a 501(c)(3) non-profit based in the United States, but with employees, contractors, and volunteers worldwide (including the United Kingdom). The Tor Project conducts research, training, and software development to improve Internet privacy and safety, and to promote free speech, free expression and civic engagement.

2 The Tor Project is predominantly funded by Non-Governmental Organisations (NGOs) and governments, as well as individual and corporate donations. Recent funders include the Swedish International Development Agency (Sweden), the Broadcasting Board of Governors (US), the National Science Foundation (US), the NLnet Foundation (Netherlands) and Human Rights Watch (US).

3 The core software product developed by The Tor Project, "Tor" was originally designed and implemented as a research project by the United States Naval Research Laboratory. The Tor software improves its users' safety while using the Internet by redirecting communications via the Tor network – approximately 3,000 computers ("nodes") operated by volunteers worldwide. The nodes chosen for a particular communication are selected randomly by the Tor software running on the user's computer.

4 Communications sent via Tor typically will pass through three nodes before being sent to the ultimate destination. Each of these Tor nodes will know the source immediately before it, and will know the next destination for the communication, but any one node will not know both the original source and ultimate destination for the communication. Communication between nodes, and between the user's computer and the Tor network are encrypted to protect against eavesdropping and tampering.

5 Through this approach, Tor protects users against someone maliciously observing their computer's Internet connection from discovering which websites they are accessing, and whom they are communicating with. This could be of importance, for example, to a journalist collecting information about human rights abuses from sources whose personal safety could be put at risk if the government discovered they were talking to journalists.

6 Tor also protects users against websites discovering the identity of the users who are accessing them. This could be of importance, for example, to a law enforcement agency collecting intelligence from a website suspected to be involved in criminal activity. Equally, normal Internet users may desire privacy and want to protect their identity from websites who they are concerned might profile their behaviour and use it inappropriately or sell it.

7 A rapidly growing use of Tor is to allow users to circumvent national censorship schemes. Such censorship may be long term, such as the "Great Firewall of China", or can be responsive to particular events, such as the blocking of Facebook and YouTube by the Tunisian regime in the run-up to the revolution in late 2010/early 2011.

8 Other uses of Tor include victims of crime talking to fellow survivors anonymously, children protecting their personally identifiable information while using the Internet, military personnel working undercover, operators of anonymous tip-lines reducing the risk of their sources being compromised, whistleblowers reporting on corruption, and financial institutions conducting due-diligence.

9 Further information about The Tor Project can be found on our website: https://www.torproject.org/

Use of the Internet by Human Rights Activists

10 This submission is not only based on how the Draft Communications Data Bill would affect The Tor Project and users of its software, but also how the draft bill would affect more general use of the Internet by human rights activists. Information included in this submission is based on experience by Tor Project members of training human rights activists on how to effectively and safely use computers and the Internet.

11 Internet usage by Human Rights Activists can be broadly split into two categories.

12 Firstly there is the use of general-purpose Internet services, such as Facebook, YouTube, Twitter, Flickr, and webmail providers. These are popular amongst human rights activists because they are familiar, easy to use, and capable of withstanding bursts in demand that might swamp smaller services. They are also widely used

outside of the human-rights circles and so may draw less attention by the regime being defended against, and make it easier to get information out of the country to promote their case abroad.

13 Secondly, there are special-purpose tools designed with human rights activists as a significant (although perhaps not exclusive) target user group. Tools in this category include Tor and Martus (a software package developed by Benetech[522] for securely collecting data of human rights abuses). Such tools are developed because there is a lack of security or functionality in general-purpose Internet services and software packages.

14 Both categories of usage are important, although performing a quantitative comparison is difficult. Use of general-purpose Internet services for human rights is likely to be more predominant, but while uses of special-purpose Internet services may be fewer in number they may be greater in their importance.

Comments on the Draft Communications Data Bill

Security of stored Communications Data

Addressing Q22–23

15 The current state of the art in computer security is not sufficient to adequately protect either stored communications data or restrict access to facilities built to collect communications data. Although there are techniques to protect computer systems from large-scale attacks, there are no effective measures for protecting computer systems from targeted attack by a capable adversary, especially when an adversary with state backing is a possible threat (as is the case with communications data concerning human rights activists).

16 This can be seen from the numerous breaches of security of communications service providers, even those who by far exceed industry standard levels of protection. It is likely that there are other cases of breaches that have not been disclosed due to commercial sensitivity.

17 One such example is the breach of Google's webmail service in December 2009[523]. This attack was specifically targeted against Chinese human rights activists. The breach of Google was part of a co-ordinated and sophisticated attack that also included Adobe and other companies that chose not to be publicly disclosed[524]. The attack made use of custom-made malware that was specifically designed to, and succeeded at, avoiding detection by anti-virus software. It also exploited a vulnerability in Microsoft Internet Explorer which was, at the time of the attack, not known publicly. The identity of the attackers remains unknown and was disguised by bouncing their communications through hijacked computers in the US and Taiwan.

18 Another notable incident is the compromise of the Vodafone telephone exchange in Greece[525], allowing attackers to bug the mobile telephone of over 100 high-ranking dignitaries, including the prime minister. In a highly sophisticated attack, custom-designed software activated the lawful-intercept functionality of the telephone exchange even though Vodafone had not purchased it. The attackers also successfully circumvented the audit logging, to hide the unauthorised access. Eventually the tampering was discovered but only after almost a year of being active (the exact date the attack was perpetrated remains unknown).

19 As a final example, a hacker supportive of the Iranian government but who stated that he was not affiliated to the government, compromised the certification authorities DigitNotar and Comodo (and claims to have compromised others), and managed to obtain digital certificates which were successfully used to impersonate Google's website, potentially collecting sensitive information such as passwords,

---

[522] https://www.martus.org/

[523] http://googleblog.blogspot.co.uk/2010/01/new-approach-to-china.html

[524] http://www.wired.com/threatlevel/2010/01/operation-aurora/

[525] http://spectrum.ieee.org/telecom/security/the-athens-affair/

communications data, and content[526]. The same attacker also targeted The Tor Project website, so it is reasonable to suspect that human rights activists were also among the targets.

Sensitivity of Communications Data

20 The draft bill and submissions of the Home Office make clear that only communications data, not content, may be collected and disclosed. The Home Office argue that communications data is less sensitive than content, and thus does not deserve the same safeguards, restrictions on collection, or level of authorisation to access.

21 However, in many cases communications data can be as sensitive as content, and in some cases may be more sensitive than content.

22 For example, "use data" (following the terminology used in the annex to the draft bill) revealing that someone accessed a website which is collecting evidence on human rights violations could put that person or their family in severe danger.

23 Even disclosing that someone was using the Internet at a particular time can be sensitive when it is correlated with, for example, the posting of videos of human rights abuses on YouTube. While the timing of a single instance of a video is unlikely to uniquely identify a person, repeating this exercise, combined with knowledge of the "usual suspects" for such activity, could single out an individual for repercussions.

24 Experiments have shown that 23.3% of Wikipedia users could be uniquely identified from "use data" alone, had they been using Tor to protect their privacy[527]. This proportion goes to 95.7% when only Wikipedia users who have posted 50 or more items on Wikipedia are considered.

25 As another example, "traffic data" showing that a phone call made by a journalist was from a particular location could put that journalist at risk. It has been reported that the Syrian government were using traffic data analysis to target journalists, and this technique has been implicated in the death of Sunday Times war correspondent Marie Colvin[528].

26 Even "subscriber data", while typically less sensitive than use data or traffic data, can be of critical importance. The disclosure of the identity of a person pseudonymously blogging about sexuality, political or religious beliefs could put someone's employment at risk, even within liberal democracies.

27 The reason that communications data can be more sensitive than content is that it is more amenable to automated analysis, particularly when collected in bulk (as proposed by the draft bill). Content is designed for humans to read, and it is a challenging problem for computers to accurately interpret content. In contrast, communications data is designed for computers to interpret and so is far easier for computers to analyse and allowing a more accurate and detailed profile of individuals to be built than is possible with current technology to interpret content.

28 The examples above show that the discussion of the draft bill should not exclusively centre on a tradeoff between civil liberty and security. While it is undoubtedly not the intention of the Home Office, this draft bill will significantly harm the safety of human rights activists. The discussion of the draft bill thus can be framed as a tradeoff between giving additional powers to law enforcement to help improve public safety in exchange for taking away the ability of human rights activists and human rights organisations of protecting themselves.

29 In making this tradeoff it is also important to note that while a single breach of security is sufficient to compromise the safety of a human rights activist, the inability for law enforcement to obtain communications data relevant to a suspected crime does not mean that the investigation will not succeed. There are frequently alternative sources of information that will result in a successful outcome of the case.

---

[526] http://arstechnica.com/security/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached/

[527] http://www-users.cs.umn.edu/~hopper/surf_and_serve.pdf

[528] http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9098511/Marie-Colvin-Britain-summons-Syria-ambassador-over-killing.html

Safeguards

Addressing Q16–18, 24

30 The draft bill proposes safeguards for access to communications data, including approval by a designated senior officer before the application can be made, and requiring that telecommunications service providers retain data securely.

31 As discussed above, it is unlikely that mechanisms to prevent unauthorised access to data, or interception facilities, will work as needed. Audit mechanisms, to detect authorised access, are for the same reasons likely to be possible to bypass.

32 Furthermore, a feature that will likely be required by law enforcement agencies and intelligence agencies is that the queries being passed to the Request Filter be themselves confidential (as the compromise of this data could interfere with investigations). Therefore it will likely not be possible for the telecommunications service provider to properly audit access, and it will be challenging to safely store logs for any subsequent audit by the Interception of Communications Commissioner and the Information Commissioner.

33 Even ignoring the significant possibility of unauthorised access to stored communications data, and ignoring the significant possibility of unauthorised enabling of interception functionality, the mere possibility that the powers in this draft bill will be exercised introduces harm.

34 This is a consequence of the fact that the cost and risk of adding new functionality to a computer system grows dramatically the later in the development process that the change is introduced. While it may be comparatively cheap to add new functionality while a system is on the drawing board, it will be much more expensive to add the same functionality once the system is deployed in the field.

35 Therefore, the fact that the powers in the draft bill might be exercised will lead to telecommunications service providers and their equipment suppliers to put in place functionality to intercept and store communications data, even before any powers are exercised. Providers may also adopt designs for their systems which facilitate interception, such as through greater centralisation, but which leave the systems more vulnerable to attack.

36 As a consequence, the risk of interception capability being activated without authorisation will be increased. Furthermore, the same equipment will likely be sold to other countries who may use the same interception capability to spy on human rights activists.

37 It is also likely that other countries will use the fact that the UK is proposing such legislation as a justification for their own surveillance proposals. This pattern was recently seen when the Chinese state news agency capitalised on the Prime Minister's statement to the House of Commons contemplating the censorship of social networks during the 2011 riots[529].

Responses from industry

38 The response of Internet services to the risks to human rights activists that the proposed bill presents will depend on how important human rights activists, and others who depend in Internet security for their safety, are to the companie's priorities.

39 For general-purpose Internet services, human rights activists are a relatively small proportion of their usage base, and while some providers have been proactive in protecting human rights activists from attack (such as Google[530]), other commercial considerations will likely take priority, and these are better left stated by the companies themselves.

40 In contrast, Internet services designed for human rights activists will likely take a more proactive response in protecting users from harm and so are more likely to avoid being put in the position of having to compromise user safety by avoiding having a UK presence.

---

[529] http://opennet.net/blog/2011/08/amidst-riots-uk-calls-censor-social-media

[530] http://www.guardian.co.uk/technology/2012/jun/06/google-state-sponsored-hacking

41 In the particular example of Tor, recall that it is the user's computer who chooses the path through the network, so if there is sufficient fear that UK nodes are unsafe, users are free to avoid UK nodes without any intervention of The Tor Project.

42 Projects, such as Tor, may also consider that carrying out software development in the UK is too high a risk, because of the possibility that this proposed bill could be used to compel a programmer to introduce a back-door into a program to collect communications data.

Circumvention

Addressing Q25

43 As can be seen with the attacks on Vodafone in Greece, Google and Adobe in the UK, and DigiNotar in Denmark (all of which the identity of the attackers is unknown), it is well within the capabilities of sophisticated attackers to hide their traces by hijacking computers and using these as stepping stones. Hijacked computers are effectively being used as a telecommunications service provider, but will not fall under the control of this law because the owner of the hijacked computer will not know that it is being used as a telecommunications service provider.

44 There are well-known techniques[531], and software available, for defeating tracing communications based on communications data. Specifically, messages are delayed, and extra "dummy" messages are added, at each point that communications are relayed. Such techniques incur a high overhead but an attacker who has hijacked a computer to act as a stepping stones will not be paying for the network resources and therefore will have no need to be concerned at the cost.

August 2012

[531] http://mixminion.net/

Twitter Inc

Twitter is a global communications service that was created in 2006. Twitter allows users to setup an account for free and provides an open platform for communications. A Twitter user "follows" different Twitter accounts and can send and receive short, 140-character messages called "Tweets" regardless of the device they are using. Twitter has more than 140 million active users, including 10 million in the United Kingdom. Approximately 400 million Tweets per day are posted globally on Twitter.

Twitter Inc., is based in San Francisco. Twitter's offices in Europe are largely focused on sales of advertising products integrated into the service features of Twitter.

Most of what happens on Twitter is public and viewable to anyone. The overwhelming majority of Tweets are public and accessible to anyone who wants to follow an account or access the Tweets directly on the web, mobile device, or other medium. When a user sets up an account, Twitter does not ask that a user provide a home address, gender, age, or financial information. The user provides very limited information (such as a "bio" and an avatar picture) and this information is also publicly displayed to all other users. Accordingly, Twitter is a public-facing service in the sense that most users go to Twitter to view public Tweets and public information and to send their own Tweets publicly.

Twitter and Law Enforcement

Most information on Twitter is publicly available to law enforcement entities without any additional assistance. For the limited information that may not be publicly available, Twitter has published Law Enforcement Guidelines (https://support.twitter.com/articles/41949-guidelines-for-law-enforcement) which outline the procedures by which law enforcement can request information or make a request to preserve information for an investigation.

With regards to UK law enforcement, Twitter has established a dedicated liaison point with UK police. Twitter, as a US-based entity, responds to emergency requests where there is a risk of death or serious injury to a person. Accordingly, we process and respond to emergency disclosure requests from the UK, 24/7. In addition, supplemental mechanisms were put in place in preparation for and during the recent London Olympics to ensure that any potential emergency situation could be rapidly addressed. For non-emergencies, Twitter responds to requests for user information from non-US law enforcement that are issued via U.S. court either by way of a mutual legal assistance treaty or a letter rogatory. Moreover, Twitter will also preserve non-public information upon request from UK law enforcement.

Unless otherwise prohibited, it is Twitter's policy to include notice to the user of the request for her or his data before such disclosure is made in order to provide such user the opportunity to seek legal counsel or move to quash the request in court. If no such motion is made or the motion is denied, Twitter's policy is to respond to court orders by producing records in Twitter's possession that do not contain the contents of communications.

Twitter's policy is to be open and transparent with our users about the means and extent of data collection and data requests made of us by law enforcement. In addition to notifying users of requests made for their information, in July, Twitter released its first transparency report (https://support.twitter.com/articles/20170002-twitter-transparency-report). It documents government requests we received for user account information or content removal, along with copyright takedown notices.

Draft Communications Data Bill

Twitter deeply appreciates the opportunity to comment on the Draft Communications Data Bill, and would like to thank the Home Office for their time dedicated to outreach on this important piece of legislation. We note the stated objective of the Bill is to ensure that law enforcement can access certain information in the investigation of crime and terrorism. In offering views on the provisions of the Bill we are also mindful, as indeed the Home Secretary herself has stated, of the need to find the appropriate balance between protecting the public and safeguarding civil liberties.

Part of the difficulty in assessing the implications of this BIll is that it is essentially enabling legislation. The specific details, implementing regulations, and form and content of subsequent orders are as yet unknown.

Part I of the Draft Bill broadly authorizes the Secretary of State to order a telecommunications operator to collect or generate communications data, even where the operator does not currently collect or generate such data. As noted above, Twitter is a service that collects very little information about our users, and what little information we do collect is mostly public to all, including law enforcement. Most governmental entities, including the US, have exerted great pressure on companies to minimize the collection of user data rather than increase it. We recognize that the policy shift flows from perceived new challenges in the investigation of serious crime. However, in that context it would be desirable to see a better articulation of the standards for data collection and how those standards would meet the competing rights and policy objectives.

Clause 14 of the Bill contemplates the implementation of "filtering arrangements" so as to attempt to address fragmentation of data when identifying the genuine user of a communication service. The technological and administrative mechanisms which would facilitate such "filtering arrangements" are not detailed in the legislation or in the explanatory material. It is therefore difficult for Twitter to offer comprehensive observations on this aspect of the Bill. However, because this section of the bill potentially raises significant issues we welcome any additional detail and clarity that the sponsors can provide in order to more fully assess the implications of such "filtering arrangements."

An additional question is whether consideration was given during the drafting of the legislation to balancing the needs of national security and criminal investigation with public transparency about the extent of online surveillance. While the provisions in the draft bill authorise the Secretary of State to issue orders to compel communications operators to generate and store data, it envisages that this will be done in consultation with communications operators. However, there does not appear to be a process for disclosure to or input from the public on this issue. Nor does there appear to be any provision for user notification when requests for their personal data have been made by law enforcement.

We would be interested to understand what consideration was given to issues of proportionality in the drafting of this provision as well as some cross-jurisdictional challenges which may arise. For example, it is possible and indeed highly likely that this type of monitoring would result in the collection and retention of data on users who are outside of the United Kingdom. This has the potential to place us in legally untenable position with respect to privacy, data retention and data protection laws elsewhere in the world.

Following on from the above, we would welcome some clarity on how the provisions of this Bill work in concert with other requirements placed on global companies with respect to user privacy and data retention. These could include EU Data Retention and Data Protection Directives as incorporated into domestic laws in members states, human rights legislation as well as privacy and data retention legal frameworks in the United States, and elsewhere.

On the wider point of the policy principles underpinning the Bill and the considerable powers it proposes to extend to law enforcement, we are interested in hearing what consideration has been given to the precedent it may set internationally. While it is one thing for a government which has incorporated the European Convention of Human Rights into domestic law to seek to assert authority over overseas companies, it would be of quite a different order for the government of a less democratic country to seek to exercise similar powers. In such a case however, there is a risk that the standing of the UK government and UK companies in resisting such data collection from its own companies could be significantly diluted. Indeed, many dissidents abroad, such as Michael Anti in China, count upon Western democracies to lead by example and to pressure their own governments to uphold essential Internet freedoms.

Finally, if companies like Twitter do not establish ready access to such data or generate data that British authorities believe is necessary, there is authorization in the bill for authorities to compel telecommunications operators to obtain that data. We may not be privy to such orders. We may not know when requests to obtain our user data are being made to other telecommunications operators. What is the mechanism for informing overseas companies that its data is being sought or collected? How do we reflect such lack of knowledge in our

own Terms of Service with respect to our users, where we typically describe and are held accountable by regulators in the U.S. for the privacy and security features of our service?

Thank you for the opportunity to provide written comments on the Draft Communications Data Bill. Twitter is prepared to work with the Members of the Joint Committee with respect to any additional questions the panel may have.

August 2012

UK Border Agency

1. On 12th July 2012, Gillian McGregor, Director of Operational Intelligence in the UK Border Agency, provided oral evidence to the Joint Committee on the Draft Communications Data Bill. This evidence builds upon the evidence already heard by the Joint Committee.

2. The UK Border Agency (UKBA), within the Public Authority of the Home Office, is the UK law enforcement agency with responsibility for investigating immigration and border related customs (non fiscal) offences, both as lead agency and in partnership with SOCA and other law enforcement partners.

3. UKBA also currently supports applications that may be made for communications data by colleagues in Border Force, (also under the Public Authority of the Home Office). Border Force split from UKBA in March 2012, but continue to require access to communications data in relation to its primary functions. Under the current operating mandate for Border Force, all matters identified at the border and pertaining to border crime are referred to UKBA for investigation.

4. UKBA uses all three types of communications data (traffic data, service use data and subscriber data) as defined under sections 21(4)(a), (b) and (c) of the Regulation of Investigatory Powers Act 2000 (RIPA) in support of its remit to investigate immigration and border related customs crimes. Applications are made for the statutory purpose of preventing or detecting crime. Examples of key customs offences include drugs and prohibited item smuggling (offences under the Customs and Excise Management Act 1979), as well as money laundering offences under the Proceeds of Crime Act. Key immigration crime offences include those of facilitation and organised people smuggling (contrary to section 25 of the Immigration Act 1971), trafficking offences (bonded labour, vice, vulnerable persons), forgery, counterfeiting and ID offences.

5. In addition to criminal investigations, applications can also be made to support investigations conducted within the UKBA Detention Estate, (for the prevention and detection of crime and in the interest of public safety), and for investigations by the Security and Anti-Corruption Unit in relation to misconduct in public office. UKBA is also empowered to access subscriber and service use data when investigating asylum benefit fraud.

6. UKBA acquires all three types of communications data under RIPA on a daily basis in support of its core functions. The Agency accessed data in relation to 2,854 individual communications data items in 2010, rising to 4,062 items in 2011 and this total is projected to rise to 6,000 for 2012. The volume of checks has grown year on year as the Agency has continued to develop its criminal investigation capability. These increases follow the organisational changes in 2009 which saw the newly created UK Border Agency take responsibility for HMRC drugs investigations and the consequent tripling in the volume of checks made through the Single Point of Contact (SPOC).

Why do we need access to this data?

7. Communications data is particularly beneficial when targeting those involved in cross border crimes, precisely because this criminality involves a great deal of movement. Experience has shown, in both immigration crime and drug smuggling investigations, that those involved frequently co-ordinate much of their business by mobile phone and, to an increasing extent, the internet. If for example, the subjects of the investigation are moving commodities or human beings into the UK, they frequently

liaise with their criminal associates (either the organisers or those responsible for the next stage of the smuggling operation) by mobile phone or the internet. Communications data therefore becomes a crucial tool in the investigation of these offences.

8. With the communication methods of criminal gangs involved in immigration and border crime developing and changing, it is crucial that UKBA retains access to all types of communications data in order to effectively combat this criminality. UKBA needs to be able to utilise effective tools in order to quickly identify and apprehend those responsible, and establish the full extent of a criminal network involved. A subscriber check, whether relating to a phone or email address, can often establish a starting point for an investigation, whilst data from billings can build the picture further by identifying criminal associates or key contacts that are made around the known criminal event, e.g. a drugs seizure. Cell site data is a particularly effective tool when attempting to locate those individuals who are frequently moving between UK air or sea ports and addresses in the UK, such as safe houses. Some of the following successful outcomes would not have been achieved without access to communications data:
    a. Communications data has secured guilty pleas from the subject(s) arrested or secured their conviction at court. In many of the cases that have resulted in a guilty plea due to the incontrovertible communications data evidence that was presented, significant costs have been saved because a protracted trial process was avoided.
    b. Convictions have been secured at trials due in large part to the detail within the communications data evidence presented.
    c. In numerous investigations, the communications data acquired has enabled investigators to identify the wider organised crime group involved in the criminality under investigation, and ensured, for example in a drugs importation, that not only is the courier arrested and charged, but that other key organisers are identified and the modus operandi of the network is established.
    d. In immigration investigations, communications data has identified beneficiaries and/or victims of the criminal network who have been facilitated or trafficked into the UK.
    e. Communications data has also proved vital in excluding subjects from further investigation, ensuring that any additional intrusion is prevented.

9. Communications data played a part in over 460 separate UKBA criminal investigations in 2011. The Agency also disrupted the activity of 74 organised crime groups and secured 1,600 prosecutions. It would not have been possible to progress or resolve many of these investigations if access to communications data had been restricted or was unavailable.

<u>Why can't you achieve the same outcome using other techniques?</u>

10. Border related criminality is often well organised and utilises the involvement of varying numbers of individuals, all with different roles to play in the criminal activity. Much of the communication between these individuals takes place over the internet or using mobile phones. The starting point of an investigation, for example when drugs are interdicted at the border, may provide one phone number or an email address which the investigating officer can build upon. Further communications data checks may highlight other criminal associations and key contacts around a known criminal event. In these instances, communications data can be both the starting point, but also sometimes the only means of progressing an investigation.

11. Without access to communications data, it is likely that investigations would either not be progressed or alternatively, other more intensive and intrusive techniques would have to be used to obtain the same level of evidence. For example, investigators would instead be forced to use expensive and resource intensive directed surveillance for protracted periods in order to identify and evidence criminal associations, activity, locations and modus operandi. In the same way that guilty pleas save money in trial costs, it is clear that if UKBA didn't have this tool it would cost the Agency more money.

Answers to Select Questions Set by the Joint Committee.

12. *Q - Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?*
    A – UKBA believes that the Government has made a convincing case for the new powers. UKBA investigations are often very reliant upon timely access to communications data, for example as the key piece of intelligence that starts an investigation or as the evidence that links the members of an organised gang both to each other and to criminal events. Technical developments have allowed criminals to diversify how they communicate and it is crucial that we are able to keep pace with these changes. As more and more alternative means of communicating are based on the internet, this means that more SPOC requests for communications data are sent to internet companies based overseas. Without access to this data, UKBA will have lost a vital investigative tool and criminals will potentially be able to carry out border related crimes with impunity.

13. *Q - Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?*
    A – The principle concern for UKBA is that we should retain access to communications data for the purpose of investigating border related criminality. In addition, previous organisational changes within UKBA, for example the recent evolution from Immigration and Nationality Directorate, to Border & Immigration Agency and finally to UKBA, plus the current split with Border Force have all demonstrated that there is still a need for flexibility in this area. Organisational changes have the potential to necessitate a change to the list of Public Authorities.

14. *Q - Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?*
    A – As outlined above, UKBA is responsible for investigating a broad range of border related crimes including: drugs and prohibited item smuggling, facilitation and organised people smuggling, trafficking offences, forgery, counterfeiting and ID offences. Some of these offences, such as trafficking have a significant detrimental impact on individuals concerned, whilst other offences such as drug smuggling can have severe social consequences for the UK. Counterfeiting, ID fraud and forgery offences may appear to cause less immediate harm, but these offences can have economic consequences for the UK if they enable large numbers of people to illegally enter the country. Equally, there could be significant consequences for national security if individuals posing a threat to the UK used forged documents to enter. 99% of UKBA's communications data applications are carried out for the purpose of preventing or detecting crimes similar to those outlined above. We therefore believe that it is appropriate, proportional and in the public's interest that UKBA has continued access to this investigative tool.

15. *Q - Is the proposed 12 month period for the retention of data too long or too short?*

A – We believe that the 12 month data retention period is appropriate. Drug smuggling and facilitation organised crime groups have in the past been identified as running operations that cover significant periods of time and communications data going back up to a year has proved crucial in identifying and evidencing criminal events. For example, communications data going back up to a year has been used by UKBA as evidence against organised crime groups who have facilitated individuals into the UK by arranging sham marriages with EU nationals. Communications data in this scenario provided incontrovertible evidence of other older sham marriage events and the criminal associations of the perpetrators.

16. *Q - Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?*
A - From a UKBA perspective, the sheer volume of requests made by the agency in conducting these investigations would make a requirement to seek judicial / magistrate warrant for our requests a severe burden. UKBA currently runs an electronic process which allows for the swift distribution of communications data application forms from the SPOC to the relevant Designated Person, something that is particularly beneficial in urgent operational circumstances. Any system in which a warrant was required would have to ensure that the minimum efficiency standards already existing in this area are maintained in order to avoid having a negative impact on investigations. If a warrant system was introduced for UKBA, this would have a significant negative impact on the time available for investigations as investigators spend time travelling to and from Courts to present their case. UKBA is not in favour of a warrant system given that we believe the safeguards provided by the external inspection regime and the existing processes ensure that the current system is properly robust.

17. *Q - Is the role of the Interception of Communications Commissioner and the Information Commissioner (IOCCO) sensible?*
A - UKBA has had a very positive experience with the Interception of Communications Commissioner's Office (IOCCO) over the last few years. We are not only inspected to ensure our compliance with RIPA, but IOCCO has also consistently given the Agency clear and helpful advice with regard to improving the efficiency of our processes. The robust and constructive approach of the IOCCO inspectors ensures that senior managers are able to have continuing confidence in the Agency's compliance with the legislation.

18. *Q - Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?*
A - Strict processes within the UKBA SPOC ensure the integrity of the process for accessing communications data. Applications for data can only be authorised by specified operational grades within the Agency - HM Inspectors or Senior Officers for border related criminality, and specified grades for anti corruption, asylum fraud and Detention Services applications. Those individuals must have received specific training as a Designated Person and this training ensures that all UKBA Designated Persons are fully aware of the important Article 8 ECHR considerations that form the basis of each application form. The SPOC ensures that application forms are sent to impartial and objective Designated Persons who are not associated with the operation and given that UKBA is a national Agency, forms are usually considered by Designated Persons from completely different regions.

19. The service providers can only issue communications data to a limited number of accredited SPOC officers within the Agency, and only when given the name of the Designated Person responsible for authorising the application. The entire process is fully auditable and application forms must clearly indicate how a telephone number or email address is associated with the investigation. IOCCO carry out random checks on our files in conjunction with the service providers in order to ensure the integrity of the process.

20. UKBA is confident that the robust safeguards in place effectively ensure that no-one can circumvent the process for obtaining communications data. In support of this fact, there has never been any abuse of the process for accessing communications data in UKBA. If any such abuse was identified, UKBA acknowledges the serious nature of these potential incidents and as with existing types of data, breaches would be treated as disciplinary offences which may result in a range of penalties, up to and including dismissal. We believe that these penalties are appropriate and a bespoke offence is not necessary.

Conclusion

21. The harm caused to the UK through the smuggling of drugs, organised facilitation and trafficking cannot be overestimated. Furthermore, for UKBA to meet its obligations as one of the 4 key partners involved in the Organised Crime Partnership Board (OCPB), alongside SOCA, HMRC and ACPO, parity with these agencies is vital. It is only with continued access to communications data that UKBA will be able to continue fully and effectively tackling immigration and customs crime, protecting our border and disrupting such harmful criminal networks.

August 2012

Virgin Media

Virgin Media Limited ("Virgin Media") is an entertainment and communications business which offers a "quad play" of broadband, fixed line telephony, mobile telephony and TV services to residential and (in relation to some services) commercial and public sector customers in the UK. Virgin Media is one of the UK's leading internet service providers delivering fixed line broadband services to over 4 million customers.

Virgin Media welcomes the opportunity to respond to the joint committee's request for written submissions.

Introductory comments

Virgin Media recognises that law enforcement should have reasonable and timely access to communications data in order to help achieve successful prosecutions. Clearly, for this to be the case it is vital that the introduction of any new communications data regime is workable for industry, while retaining the trust of the public. It is also critical that any measures are proportionate and delivered on the basis of reasonable checks and balances to ensure that the legitimate privacy of users is protected. Virgin Media takes its obligations regarding data security and data privacy very seriously and has detailed privacy and information security policies in place.

Virgin Media understands the rationale of the Government's proposals. It is evident that as the digital age evolves, the communications landscape is changing. Communications services and technologies are changing rapidly, bringing huge benefits to the UK's society and economy. But the evolution of communications technology also means that the internet can also be used to underpin criminal behaviour. As a result, law enforcement authorities have a concern to ensure they have access to communications data in order to help achieve effective prosecutions.

The current regime

The current regime has strengths, particularly the Single Point of Contact System (SPOC), which provides an important framework for the relationship between law enforcement authorities (LEAs) and CSPs. Like ISPA, we recognise that the current system also ensures that the costs that CSPs incur when they comply with requests can be reimbursed so that CSP's continued investment in other areas, such as broadband rollout, is not affected by data retention requirements. This also acts as a safeguard with law enforcement only requesting data knowing the cost has to be justified. It is crucial that these elements continue as part of any future communications data regime.

The Draft Communications Data Bill

Virgin Media has been involved in discussions with the Home Office, over a number of months, about the practical aspects of the Bill should it receive Parliamentary approval. The discussions have been useful and have provided much valued clarity about the implementation of the Bill, should it receive approval. However, given that many of the details of the Bill are to be clarified in secondary legislation it is inevitable that discussions on further aspects of implementation will be required in order for the necessary clarity to be delivered

At this stage, our primary concern with the draft Bill as it stands relates to the retention requirements on providers not previously caught by data retention requirements and the requirement for UK providers to retain data of these providers. Virgin Media currently enjoys good working relationships with a range of third parties, both domestically and internationally. In many cases, Virgin Media makes their applications and services available to its customers through, for example its TiVo service. If Virgin Media is legally obliged to provide data from such third parties, this may well damage its commercial relationship with those parties and other third parties, particularly those based overseas who may be reluctant to make their services available to Virgin Media.

Virgin Media is also concerned to ensure that there is a level playing field for all data holders covered under the legislation. The legislation must be underpinned by a robust Code of Practice which sets out the process that is

required for all third party data requests. Virgin Media and other UK based communications providers' obligations to supply third party data should be seen as a last resort, only exercised once the third party in question has rejected the request. Once the Code of Practice is in operation Virgin Media recommends that it is kept under review and regular Parliamentary scrutiny to ensure the appropriate checks and balances remain effective.

Virgin Media welcomes the proposed controls regarding access to communications data by public authorities, but believes it would also be helpful to clarify the ability of third parties to access additional data retained as a result of the Bill under so called 'Norwich Pharmacal' orders. Private companies and individuals regularly make applications to court for disclosure of a wide range of personal data for a wide range of reasons, including defamation, copyright infringement and security and confidentiality breaches, and these applications are frequently granted. The impact of the Bill on these applications and their scope needs to be considered.

August 2012

Vodafone

Vodafone welcomes the opportunity to provide evidence to the Joint Committee and the scrutiny provided by the draft bill consultative process. This is an important and complex policy area which will benefit from a full public debate.

Vodafone recognises the importance of communications data — metadata about a communication, and not the content of a communication — in the fight against terrorism and crime, and is committed to working in partnership with Government, law enforcement agencies and the rest of the industry to play its part. Vodafone recognise that the technological change and spread of communications over the Internet has created new challenges for law enforcement agencies, and understands that this proposed legislation aims to maintain law enforcement capability in the light of these developments.

It is up to the Government to recommend what new powers law enforcement needs to ensure it has the right information to fight crime, and once this has been decided and been passed by Parliament, Vodafone will do its best to support the law enforcement agencies and deliver an effective and efficient service within this new legal framework.

Vodafone also recognises the importance of privacy. It is vital that the measures are proportionate and necessary to protect the privacy of our 19m customers, the vast majority of whom are law-abiding citizens. This means all participants in this debate have a responsibility to ensure that changes to the current regime are implemented in a way that respects their right to privacy.

Vodafone has a solid record of both supporting law enforcement and protecting the privacy of its customers.

In this consultative stage, Vodafone is keen to ensure that any new proposals are technically workable, provide law enforcement the information they need whilst also providing maximum protection of its customers' privacy.

We would urge the committee to ensure that there is an appropriate debate following the findings of the Joint Committee and that the Joint Committee has an opportunity to respond to the Government's response to its report.

From Vodafone's perspective, there are six major issues which the Committee is requested to explore:

- Responsibilities of UK and overseas providers
- Interaction with privacy regulation
- Retention and deletion requirements
- Definition of valid requesting authority
- Oversight
- Technical boundaries

Responsibilities of UK and overseas providers

The major impact of this legislation is that it could be used to ask telecommunications operators to collect data for which they have no day to day business use, simply for the purpose of making it available to law enforcement agencies.

In the main, the recommendations in the draft Bill take the current model (enshrined in the Data Retention (EC Directive) Regulations 2009, and the Regulation of Investigatory Powers Act 2000) and extend it to cover the new platforms and software used to communicate over the Internet. Clearly, taking a pre-internet model and assuming it works in the internet age isn't necessarily going to deliver a workable long-term solution. Pre-internet, the vast majority of communications were enabled by services provided by UK based telecommunications companies, which also operated the network over which the communications were transmitted.

This is no longer the case. There has been a separation of network and service, such as VoIP-based services, and software enabling VoIP communications, and social media. As such, whilst telecoms operators may provide the networks over which these services are accessed, or by means of which the communications are carried, the telecoms operator may no longer be the provider of the service or software — the former link between network and service is no longer applicable. However, the vast majority of internet communications are conducted on platforms or via software provided by a few leading internet companies.

We believe that the best way to tackle this challenge is to ensure that a principle is established that the company primarily responsible for the application or service that the consumer is using to communicate on the internet is the company with the duty to hold the data relating to that communication. This fits with the principle that companies only hold information generated in their day to day business activities.

Naturally this raises a jurisdictional issue. Many of the tools used for communications are offered by companies based overseas. This should not be a reason for their remaining outside the system. The Government therefore needs to ensure the legislation works with these companies. This is an area where the Government needs to be clear how it intends to ensure that this data will be collected in a proportionate and appropriate manner by those organisations best placed to do so. There seems to be scope in the draft Bill to establish this principle, enabling the Secretary of State to impose an order on "any person," whether based in the UK or not. Clearly, this is a wide framework and it would be useful to understand more about how it could be made to work in practice.

In the extreme, where there were rogue applications operating outside of the framework by organisations which don't have an interest in supporting UK law enforcement or complying with UK law, it is understandable that imposing obligations on UK-based operators is seen as a fallback.

If some service providers, by virtue of being based overseas, are able to escape these obligations being placed on them, UK network providers providing communications services will not be competing on a level playing field.

Interaction with privacy regulation

Beyond the question about which businesses should hold the data, it is important that existing (and future) privacy and data protection legal frameworks work well with any new proposals. We need both to ensure the protection of privacy, and avoid multiple different regulatory and potentially conflicting standards when it comes to protecting our customers' privacy, given the potential for conflicting requirements on communication providers.

It would be preferable to have one overarching piece of legislation rather than the draft Bill sitting alongside the Data Retention regulations. As currently drafted, the proposed draft Bill goes considerably further than mere retention, including, as proposed, obligations to "generate" data.

Retention and deletion requirements

The UK chose a twelve month retention period under its implementation of the Data Retention Directive, so there is a precedent but it is for the Government to decide these time periods. The Directive permitted retention for between six and twenty four months. However, the longer Vodafone is asked to hold data the greater the cost and the greater the storage capacity required. It should also be noted that we will be required to hold some data for longer if flagged by law enforcement agencies as potentially related to illegal activities.

We also have concerns about the requirement for an operator to destroy data "in such a way that it can never be retrieved." "Never" is an unrealistic requirement, because we are not in a position to determine the state of the art in the future. Under the data retention regulations, the requirement is to "delete the data in such a way as to make access to the data impossible," reflecting what is possible today, and Vodafone would suggest that this requirement should be reflected here.

Definition of valid requesting authority

If the proposal in the draft Bill is enacted, clearly the list of public authorities able to access communications data needs to be kept to a minimum. Requests need to be necessary and proportionate, and only for the pursuit of criminal activity. It is probably sensible to vary this list but only if there is a pre-condition towards reducing the numbers where possible not increasing them. Requiring judicial authorisation for local authority access is appropriate.

When communications data is requested, we support as high a level approval process as possible to ensure that requests for data are taken seriously, given both the privacy intrusion and the cost to the tax payer of unnecessary requests. We believe that the continuation of the process currently in place (i.e. a notice authorised by a designated person) is a minimum requirement.

Oversight

Without a clear indication on how this regime will work in practice it is difficult to comment on appropriate penalties. Clearly the more bureaucratic and complex the regime, the more protection telecommunications operators should be afforded. If best efforts have been applied then this should be taken into account. A penalties regime should form a separate consultation once it is clear how this legislation will work in practice.

However, it must be the case that public authorities responsible for handling and requesting personal data must take these powers as a very serious undertaking. This being the case, there should be consequences for mishandling data or making erroneous requests. However, we aren't qualified to comment what the penalties should be. Clearly they can't be less than those faced by the private sector.

Because of potential impact on privacy which we highlight above, there is a need for strong independent oversight. Any new operational powers given to either the ICC or ICO need to be properly resourced and fit as closely as possible to existing privacy and data protection procedures. This legislation seems to be asking ICO to take on a much more proactive, inspectorate type role. This would be a notable change of current practice.

Technical boundaries

It is technically possible to retain communications data and communications service providers can already be served with obligations to do so. However, the capability to do this would depend on the communications service in question — this would need to be assessed on a per-service basis. Where it was not possible for a communications provider to differentiate between content and communications data in respect of any given communication, the communications provider must stop attempting to record communications data for that communication.

As a matter of simple practice, if Vodafone were to be obliged to acquire communications data related to encrypted communications, it would need to be supplied with the capability for converting the communication to a format which enables it to extract and store the communications data. Vodafone would not be able to attest to the accuracy of the output of such a capability.

To the extent the obligations require for Vodafone to supply data to a third party system for analysis, we are not in a position to comment on how such a system would work. It should be noted that this approach is new and so

will require a good deal of close collaboration between telecommunication operators, Government and the organisation providing the filtering service. We feel that there should be a proper consultation process with the key players to ensure that this new system works well. However, we are confident that we have the expertise to store communications data safely. We already do this for our 19m UK customers.

August 2012

David Walker

My name is David Walker. I have worked in Information Technology since 1993, and specialise in system and network security. I currently run a small business specialising in design and implementation of multileve and cross-domain secure desktop and server infrastructures, but most notably for the purpose of this discussion, back in 2001 when I was a Security Subject Matter Expert at Sun Microsystems UK (a post I occupied until 2010), I co-designed a "black box" lawful intercept solution based on original research, and presented it, in conjunction with the Home Office and in the context of RIPA and NTAC, to the CTOs of the UK's major telcos.

I have worked on IT security solution design and implementation in a number of industries over the years, including Financial Services, Telco, Utilities and Public Sector (involving Law Enforcement, Defence and Intelligence), and have been involved in research into admissibility of electronic data as evidence, as part of a technical team assembled by Stephen Mason. I also contribute my views on relevant issues to various Information Assurance organisations.

I submit this work on my own behalf, in the form of responses to the specific questions posed in the Consultation. If the Committee wishes to enter into discussion regarding any of the points I raise below, or have me present evidence orally, I would welcome the opportunity to participate further.

SUMMARY KEY CONCEPTS

* Extent of the Internet; significantly lesser extent and reach of British legislation; mismatch between British and foreign legislation and standards; data sensitivity and vetting

* Triviality of setup and migration of remote and distributed communications services

* Proxying, tunnelling, cryptography and other obscuring technologies; mapping to tradecraft techniques

* Co-wrapping and separation difficulty of "communications data" and "communications content"

* Number and diversity of communications protocols

Below are specific questions about the details of the draft Bill. The Joint Committee would appreciate written submissions on any of these questions on which you have evidence to contribute.
It is not necessary to address every question. The Joint Committee will also welcome other comments related to the draft Bill, even if not directly addressing the questions below.

It will probably be helpful, when answering some questions, for me to include hypothetical examples of some communications between up to three "persons of interest". For purposes of illustration, these three persons will be referred to below as "Fred", "Jim" and "Sheila".

GENERAL:

[1.] Has the Home Office made it clear what it hopes to achieve through the draft Bill?

To a large degree, yes; certainly to the extent that it is clear that the Home Office's intentions are not technically feasible to implement in a manner which results in their intended outcomes, no matter how much money is available for solution implementation and maintenance.

However, some elements of the Bill remain unclear, to someone used to communicating in the accepted industry vernacular. See my response to (eg) Question 11 below.

[2.] Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

As individuals and organisations perform more of their social and business communications online, it initially appears sensible to attempt to address these foms of communication from the perspective of interception.

However, as I hope will become clear in my answers to subsequent questions, the world of electronic communications is sufficiently different from the world of physical communications, location and movement, that attempting to identify and isolate the electronic communications of a person of interest of moderate technical skill would be equivalent, in a traditional tradecraft context, to being able to shadow someone able to change their appearance arbitrarily, teleport and produce illusory independent duplicates of themselves at will. Also, it is not necessary for a person of interest to invent any of the technologies needed to achieve these feats; they already exist and have geographically distributed supporting infrastructures in place.

In short, "the need for new powers and initiatives is evident, but having them will not necessarily help fulfil the aims intended".

[3.] How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

In my view (and disregarding technical issues) they sit reasonably well alongside other elements of RIPA.

[4.] What lessons can be learnt from the approach of other countries to the collection of communications data?

I know little of the actions of other nations regarding the pure collection of communications data; however when it comes to the interception and blocking of communications (which can be considered a superset of collection; data to be intercepted and blocked must by necessity be identified, isolated and collected in realtime, such that the realtime requirement is the principal added imposition), large-scale communications censorship infrastructures such as the so-called "Great Firewall of China" are notoriously porous.

Also - as has been found in China and elsewhere - if a person or organisation located in a country and of interest to that country's Government has access to the funds and the inclination to so use them, they could completely bypass any national telecommunications infrastructure (and interception capabilities placed upon it) by spending a few thousand pounds to rent or purchase a handset connected to the Iridium or Inmarsat satellite communications networks.

(I note that Inmarsat is a British company headquartered in London and listed on the LSE, so they could be considered to fall within the sphere of influence of the British Government and thus be required to install communications gathering equipment according to the proposed Bill. Iridium, being American, fall outside the British Government's sphere of influence.)

Expanding on the "Great Firewall of China" experience, numerous techniques have been developed and deployed to circumvent and bypass the controls in place. The techniques - and tools which implement them - are widely known and freely available, and where necessary, have global distributed infrastructures in place to support them. They include:

* tunnelling one network communications protocol over another (such as IRC over DNS); the design of TCP/IP enables this to be achieved for any pair of protocols which run over a TCP/IP stack, and also allows IP to be tunnelled over IP (see eg http://www.ietf.org/rfc/rfc2003.txt).

* use of proxying services to mask the source and / or destination endpoints of a communication (a long-standing and popular anonymous remailer service was hosted at anon.penet.fi; newer equivalents include hidemyass.com). In our context, such a proxying service can be easily set up illegitimately on any compromised Internet-connected system overseas, or legitimately on any overseas cloud service. I note that, historically, many Internet-based attacks used to appear to come from proxy systems located in Singapore; Singapore was chosen

as a particularly suitable place to break into a computer and install a proxy, as until relatively recently it had no legislation aimed at addressing computer misuse.

* use of cryptography and message wrapping techniques, in conjunction with wrapping-aware proxies, to mask the destination endpoint of a communication by concealing encrypted message destination data with encrypted message content. In traditional tradecraft terms, this is equivalent to double-bagging a postal communication; Fred could send Sheila a letter in the post, for example, inside which is an envelope containing another letter, addressed to Jim and with delivery instructions for Sheila. This scheme naturally extends to triple- and n-bagging.

* use of online file storage facilities such as http://www.dropbox.com/ , with sharing of accounts to create the digital equivalent of tradecraft "dead letter boxes". This started (and continues) with shared accounts at cyber-cafes; Fred writes a file, goes away, and Jim comes along with knowledge of Fred's credentials, logs on as Fred and reads the file. This changes the scope of "communications" tracking - if Jim knows the details of Fred's account, then there is no electronic communications data which indicates data passing from Fred to Jim.

[5.] Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

I would suggest that this question is extended, to consider alternative means by which the ends intended to be achieved by obtaining communications data, could be achieved. A rephrasing to something like "What alternative means of achieving the stated objectives, if any, might be more likely to succeed, given the funds available and developments in communications technology and infrastructures over the past decade, as well as those currently under way?" seems appropriate, and I would hope that this question yields constructive answers from respondents skilled in conventional tradecraft and forensic investigation.

To put this in context, the issues of obtaining communications data are sufficiently asymmetric - from the perspective of creating, provisioning and maintaining lawful data-obtaining capability being very difficult and expensive, and evading communications data-obtaining measures being fairly easy and monetarily either free or nearly so - that diverting funds currently earmarked for communications data gathering to other law enforcement and intelligence initiatives, would probably yield greater benefit.

For example, I recall Prof. Ross Anderson's comment on Radio 4's "Today" Programme on 01/11/11; apparently, it has been found from well-known conventional bank account tracing techniques that the vast majority (some 90%) of funds garnered by Internet spam merchants are funnelled through 3 banks in Azerbaijan. As actions have been successfully taken to sever communications between the SWIFT network and all banks in Iran, as part of economic sanctions against that country, a "follow the money" approach suggests that, if part of the intent of communications tracking is to facilitate attacks against organised crime, attemplting to sever connections between SWIFT and these Azeri banks would likely be of benefit.

[6.] The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

It makes more sense to me to keep the pieces of legislation separate, as while their purposes overlap, data retention also relates to contexts other than communications interception.

I also note that the issue of data destruction needs to be addressed more explicitly; see later.

[7.] If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

Not that I am aware of.

[8.] Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

Yes - and this applies more widely than just to communications service providers.

For communication service providers who will be required to integrate and host communication data gathering equipment, the means of integrating this equipment becomes a primary requirement of any current and future communications infrastructure design. Provision for feeding data to gathering equipment will have to be maintained, for as long as the proposed legislation is in force. This may act as a drag on innovation; data gathering boxes will need to be maintained as separate entities, which will require provision of physical connections of appropriate type and speed, and provision of appropriate data to those physical connections. If at some future point an intercept capability is incorporated into infrastructure as a virtualised service, the assurance of separation will need to be verified, tested and assured by the likes of GCHQ - and this will involve imposing regular inspections and other inconvenience on service providers.

Also, the wording of the proposed Bill regarding reasons for data gathering, seems very broad - specifically, page 25 subsection 6 clause d. "in the interests of the economic well-being of the United Kingdom".

Depending on the interpretation of this clause by their risk managers, companies in the Financial Services industry could interpret this as meaning - especially given many stories in the press over the last couple of years about views between Government and Financial Services - that any Financial Services company could readily be subject to gathering of all their communications data by Government. While this would be unlikely to be pivotal in a decision regarding whether to conduct (or continue to conduct) business in the City of London, it may have adverse effect.

COSTS:

[9.] Is the estimated cost of £1.8bn over 10 years realistic?

I am unable to comment on this, as the working by which the number is derived is not given.

[10.] The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5 6bn. Is this figure realistic?

I am unable to comment on this, as the working by which the number is derived is not given.

SCOPE:

[11.] Are the definitions of communications data and communications service provider appropriate?
Do they sensibly define the scope of the powers in the draft Bill?

Not really. In terms of defining "communications service providers":

* A "telecommunications company" is an entity such as BT, Vodafone, Virgin Media, AT&T etc; a company which owns and runs physical cables, switches, satellites and routers (OSI layers 1-3, at least) over which communications protocols run.

* A "communications company", by contrast, includes companies such as Google, Twitter, Apple etc, who provides communications applications and protocols to run over the infrastructures provided by the telecommunications companies.

* Also, somewhere in between (and it needs to be decided and stated which side of the distinction these companies fall on) are those companies who provide infrastructure accessible via telecommunications

companies, and which can be purposed for anything the customer is capable, including standing up their own communications service instances. Cloud Service Providers such as Amazon, Rackspace and Firehost are included in this set.

* Further, I note that some communcations companies own and host their own infrastructure; others use Cloud environments.

* Still further, there are pseudo-telecommunications companies such as TalkTalk and Tesco.net, which re-brand and resell bandwidth on communications infrastructure ultimately owned and provided by BT.

Which class(es) of company, from the above, will be required to install and maintain the infrastructure taps for the lawful intercept capabilities proposed?

The description of "communications data" (which is more commonly referred to as "communications metadata") given is accurate in some contexts and for some protocols, and downright wrong in and for others. While it is cut and dried for conventional and old-fashioned email - headers were defined in RFC 821, content in RFC 822 - SMS text messages pass over the same SS7 signalling protocol used for call setup.

Further, when considering the plethora of other communications protocols available - IRC, IM, VoIP, embedded VoIP sharing communications channels with model and state data in games, file transfer - and also when considering "double-bagged" email employing proxies and encryption, if communications data is not to be missed, any and all encrypted message data must be decrypted to ensure that no onward communications data remains in encrypted form, at the point of gathering.

Finally, there is the trivial case where communications data is contained plainly within the communication text. Consider an email message from Fred to Sheila, containing text along the lines of "the latest status update is… <several sentences or paragraphs elided>. Be sure to tell Jim about this, too."

[12.]Which public authorities should be able to access communications data under the draft Bill?
Should it be possible for the Secretary of State to vary this list by Order?

I have no comment on this question.

[13.] How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

The plans appear to be neither robust nor realistic. I have heard descriptions of the practical aspects of the "special relationship" between the UK and the US which I will not repeat here, but suffice it to say that "the Internet extends beyond the sphere of influence of any nation state".

As has already been mentioned, there are nations which have no legislation against computer misuse (Singapore has enacted some in the last decade); there are also functionally ungoverned places (I disapprove of the term "failed state") with connectivity to international fibre.

Also, with the rise in consumer-driven Cloud services, it is fairly straightforward to stand up an email service for a smallish number of users, on non-standard ports and with multiple layers of proxying and encryption such that every communication traverses a path involving cryptographic processing in at least 2 countries, using tools no more complex than a credit card and freely-available software. I have not actually done this, but estimate that to do it well, including identifying appropriate cloud service providers and learning their provisioning systems, would take me no longer than 3 weeks. An engineer more practiced in cloud service provisioning could have it done in rather less time; potentially a couple of days.

Even where overseas providers can be pursued, there are further issues to consider, such as mismatch in forensic handling standards; I gather (from discussion, rather than case precedent) that these are not even harmonised across the EU, yet. In the event of a person of interest being arrested in France, for example, if their computer equipment is seized under warrant and examined forensically by the Surete, their procedures for preserving the chain of integrity when handling the data retrieved do not tally with British requirements for same, so there would be issues of admissibility of the data as evidence in a British court of law.

There is also the matter of knowledge required of service provider staff. The list of persons of interest - or the inclusion of a specific person on the list of persons of interest - may well be a matter of national security. Therefore, unless the service provider staff associated with the management and maintenance of the communications infrastructure connected to the data gathering solution have undergone appropriate UK vetting and are cleared, they cannot be permitted to know whose data is of interest. In such circumstances, the whole of that provider's traffic will need to be captured in situ, relayed across relevant links, and only separated out once it is in a trusted environment, in order to provide a capture solution with zero local knowledge.

USE OF COMMUNICATIONS DATA:

[14.]Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

I have no comment on this question.

[15.]Is the proposed 12 month period for the retention of data too long or too short?

I have no comment on this question.

SAFEGUARDS:

[16.] Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should “designated senior officer” be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

I have no comment on this question.

[17.] Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

I have no comment on this question.

[18.] Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

I have no comment on this question.

PARLIAMENTARY OVERSIGHT:

[19.] Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

I have no comment on this question.

ENFORCEMENT:

80. [20.] Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

81. These do not appear to be well-defined.

[21.] Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

I have no comment on this question.

TECHNICAL:

[22.] Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

Unequivocally and emphatically, "No"; see detailed discussions above, and further discussion here.

Even if the technology is developed, the considerable asymmetry of effort between deploying and maintaining it on the one hand, and bypassing or otherwise rendering captured data of no value on the other, is a strong argument for redirecting effort to other approaches and techniques more likely to give results representing value for money.

I note that, even where data is not encrypted, and is a trackable communication rather than one associated with a dead-letter box, a system to separate communications data from communications content would need to understand every communications protocol currently employed by every piece of communications software. There are hundreds of such protocols, many are proprietary, and new ones are produced and deployed in new software releases fairly regularly. The initial engineering effort to produce such protocol parsers, and the ongoing effort to incorporate new ones, would be prohibitive.

Where communications data is "double-bagged" using encryption, such that at point of capture the only discernible information is that Fred is communicating with some server in (say) the Ukraine (which would in turn take off a layer of encryption, forward the message to a server in (say) Indonesia according to the revealed communications data, then the server in Indonesia would act on the revealed communications data to wrap the communication with another layer of encryption and send it to Jim), the communication could potentially be captured reliably (although there are considerable performance considerations to take into account), however it would be of little use.

If GCHQ is sitting on a new branch of mathematics or some remarkable advance in computing which enables them to decrypt AES-256 in practical time, then (and only then) does data gathering have practical use, if the persons of interest have taken the trouble to enable or configure encryption and are using a proxy service. Even then, the whole of the communication woudl need to be decrypted, in order to reveal the encapsulated and encrypted message forwarding data necessary to construct the whole communication path.

Also, Paragraph 73 on pages 30-2 gives a further well-considered view on issues associated with communications data retrieval:

There are a number of features of internet based communications which have an impact on the acquisition of communications data by public authorities:

The technology which is used to operate internet and mobile services, and collaboration between numerous companies may mean that communications data regarding a single communication is no longer retained in a

single place. This fragmentation of data makes it difficult to obtain and aggregate all of the communications data a public authority may need to answer a specific question.

* Companies who provide internet communication services do not always require authenticated identity information, making it more difficult to identify the genuine user of a communication service. Moreover, a range of technologies are available which attempt to anonymise both the location and the identity of service users.

Numerous mobile communication devices can be used to access Internet communication services while on the move, making it more difficult to establish from where a communication was made.

There are a vast range of global internet communication services. It is very easy to communicate simultaneously using multiple services and move quickly to new services.

[23.] How safely can communications data be stored?

This naturally depends on where and how it is being stored. If it is being stored at the service provider, and the provider is untrusted, the whole of the provider's data feed must be stored in order to give a zero-local-knowledge solution.

Various novel methods of dispersed zero-knowledge storage have been developed recently; the most interesting of these (which is not recommended for realtime access, so there are caveats) is detailed at http://www.cleversafe.com/ (Note: I have no commercial interest in Cleversafe, I just find their technology intriguing.)

An equally interesting question which is not asked here (and probably should be), is "How safely can communications data be deleted?" I note that the draft Bill states in several places (eg page 18 para 32) that "The data must be destroyed in such a way that it can never be retrieved", but without providing any prescriptive information on how this might be achieved. There are several standards (eg Infosec Memo 5), for erasure of stored data with an intended outcome of the data being irrecoverable, however if the disks are likely to fall into the hands of a FIS at any point, physical destruction with an angle grinder or similar is the only guaranteed option.. The Bill would benefit from being more prescriptive, here.

[24.] Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

This requires further thinking and discussion. Unfortunately, I've not had chance to give this point the consideration it needs.

[25.] How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?

This depends on the context of the persons of interest wishing to communicate with eachother. In some contexts it could be wholly trivial, in *all* other contexts it would be reasonably straightforward, and achievable for zero or fairly trivial financial outlay.

This is unless GCHQ is sitting on a new branch of mathematics or some remarkable advance in computing which enables them to decrypt AES-256 in practical time, of course.

[26.]Are there concerns about the consequences of decryption?

This depends on what is able to be decrypted. If GCHQ is sitting on a new branch of mathematics or some remarkable advance in computing which enables them to decrypt AES-256 in practical time, revealing the existence of such technology directly, or indirectly by action, would cause worldwide panic. If, however, GCHQ is not able to decrypt AES-256 in practical time, then "double-bagging" communications is a reasonably straightforward and effective countermeasure against the aims of the Bill.

August 2012

Andrew Watson

This submission is being made in a personal capacity, not as a representative of any organisation. The author has over 30 years' experience in the IT industry, and has been following the progress of legislation on communications interception since the debate that surrounding the Regulation of Investigatory Powers Bill (as was) in 2000.

1. I note that "The Joint Committee will also welcome other comments related to the draft Bill, even if not directly addressing the questions [listed in the call for evidence]". This submission does not therefore attempt to respond to the committee's list of questions, but instead lists points that particularly concern the author.

2. I have also read, and completely concur with, responses sent to the committee by Dr Paul Bernal , Glyn Moody and Alec Muffett . I will not repeat the many valid points that they make.

3. As drafted, this legislation permits the collection and storage by public authorities of data about anyone's communications for purposes that include "public safety", "preventing crime", "preventing disorder", "protecting the public health" and "assessing or collecting any tax" (Clause 9(6)). These purposes are so broad as to permit mass blanket surveillance of the population. Independent Judicial approval would only be required in some cases - many authorities would be able to conduct mass surveillance of everyone they chose, even those not directly suspected of any crime, without any contemporaneous external oversight.

4. This draft Bill does not exist in isolation. It must be examined alongside other large-scale data-gathering systems deployed by public bodies over the past decade. There is a comprehensive list in "Database State", a report published by the Joseph Rowntree Reform Trust in 2009 , and which I recommend that the Committee study. In this response I will briefly call attention to just two other large-scale data-gathering systems controlled by Home Office agencies.

5. Police forces in the UK have created a single national database holding information from a network of several thousand Automatic Number Plate Recognition (ANPR) cameras on Britain's roads. Data on every vehicle with a registration plate that passes any ANPR camera is sent to a national database in Hendon, where it is stored for at least two years, even where there is no suspicion of wrongdoing connected with that vehicle . This database therefore holds data on the movements of every law-abiding vehicle user. At the end of March 2011 it held 11 billion vehicle sightings, and was accumulating new sightings at the rate of 15 million per day.

6. As part of its eBorders scheme, the Home Office is creating a database of the movements of every traveller who crosses the UK's borders by any means of transport . All travel details are stored in a database in Wythenshawe, near Manchester, for 10 years. This database therefore holds data on the movements of every law-abiding international traveller.

7. When used with the cross-database search technology described by Glyn Moody in his submission to the Committee , data from these (and other) Home Office-controlled databases combined with communications data gathered under this draft Bill would permit the agencies of a single Government department to track the movements and activities of every law-abiding citizen in near real-time, with no external Judicial oversight.

8. This is clearly a very undesirable state of affairs in a democratic society.

August 2012

Dr John Welford

1. Introduction

1.1 In my approach to the analysis of any proposal I find it useful to subdivide my thinking under two distinct headings, and this is how I shall therefore structure my submission. Firstly I address the principle. This is concerned with the basic rightness or wrongness of what is proposed. Thus, for example, should the proposal in question be ruled out regardless of any other considerations? Secondly I turn to the practicalities. This is concerned quite separately with whether the proposal is feasible with regard to all the other factors, such as cost, complexity, effectiveness, reliability, etc. Basically, will it work and deliver what is promised for the estimated cost? And also importantly, could the proposal lead to any unintended (especially negative) consequences?

1.2 I have cross-linked my comments to just three of your 26 questions.

2. The draft Bill - the principle

Question 16. Are there concerns about compliance with Article 8 ECHR?

2.1 Most people I speak to are truly dismayed and horrified by the very notion behind this draft Bill, the idea that the government wants in future to be able to invade the privacy of perfectly innocent people. And proposing to do this by prying into people's internet and phone use, to find out, for example, whom they speak to and which web pages they choose to look at. Interestingly, it is not so very long ago that the entire nation was united in horror to discover that a newspaper had similarly invaded the privacy of an innocent young murdered girl, viz. Milly Dowler, by hacking into her mobile phone. So why would it be acceptable to the very same people for the government to be going down a frighteningly similar track, but doing this on a global comprehensive scale with the entire population? Basically, what business is it of the government to be doing this?

2.2 Of course, such intensive investigation of internet and phone use could very well be justified in the case of an individual who had come under suspicion of having done something seriously wrong or of being about to do something seriously wrong. And this could, as now, obviously be sanctioned by a magistrate's warrant. But otherwise, I ask again: what business is it of the government to be prying into the internet and phone use of perfectly innocent people? Unless your joint committee has a solid convincing answer to this key central question then I am not sure how much it is worth pursuing any further with your other 25 questions.

2.3 It seems to me that the proposal to pry intensively into the activities of the innocent crosses a very dangerous line, a line which to my knowledge has never been crossed before in this country. Moreover, once you cross this line, and effectively turn everyone into a suspect, then where are you going to stop? For example, the proposal boasts that at least there is no intention (at present) of monitoring the actual text in people's text and email messages. But once the crucial intrusion-of-the-innocent line has been crossed, there is surely no logical reason not to go further and further and further. From there on nothing can be logically ruled out, whether it's reading the text in innocent people's email messages, steaming open all their letters or even installing government CCTV cameras in every room in their houses. And without doubt all of these advances could and I'm sure would be justified for perfectly plausible reasons. For example, both national security and the protection of the young from abuse by paedophiles could be used to justify the installation of CCTV cameras in every room in people's houses. But would this be the kind of 'Nineteen Eighty-Four' society that any of us would want to live in?

2.4 Behind the draft proposal there is, of course, the whole question of trust. In particular, having access to such an intrusive picture of every citizen's life, could any future government ever be trusted not to misuse such information to advance its party position? For example, the information could be readily used to pressure politicians, journalists, whistleblowers and others to maintain silence when they should be speaking out on a vitally important national issue. No, obviously no future government could ever be trusted. In this context a quotation from computer security specialist Bruce Schneier springs to mind: "It is poor civic hygiene to install technologies that could someday facilitate a police state." And I believe that the draft Bill outlines precisely the kind of technology development that Schneier has in mind. (http://www.schneier.com)

2.5 Needless to say, at present trust in our politicians is without doubt at its lowest ebb in living memory. And indeed the very fact that the current proposal is being put forward by a Conservative and Liberal Democrat coalition government only serves to demonstrate the justification for people's lack of trust. For prior to the last election both of the coalition parties were promising "to roll back the surveillance state", and in the coalition agreement they promised that they would "scale back Labour's Big Brother state". So why have they gone back on their promises to the electorate, and why have they shifted their position by a complete 180 degrees? The only conclusion that can be drawn is that once in power our MPs prefer to work to the quite different ongoing agenda of the permanent staff at the Home Office, rather than genuinely trying to fulfill their promises to the electorate that brought them to power. This is therefore a deeply depressing state of affairs, putting into question the honesty and integrity of our ministers and therefore the state of our democracy. So without doubt, if the draft Bill goes ahead it will only serve to confirm people's deep and growing mistrust in their political representatives.

3. The draft Bill - the practicalities
Question 9. Is the estimated cost of £1.8bn over 10 years realistic?

3.1 I have absolutely no idea how this figure was arrived at. But what is certainly well known is that government IT projects are renowned for (a) costing significantly more (usually by several factors) than had been originally estimated and (b) taking much much longer to deliver than was ever projected at the outset. There are several key reasons for this gross inaccuracy:

a. 3.2 The vast majority of politicians are technically naive when it comes to IT projects and engineering generally, and so are not in a good position to be able to understand, evaluate and thoroughly question precisely what is being proposed by the relevant 'experts'. And so they are not in a good position to oppose, or later abandon, technically weak proposals with unrealistic timescales.

b. 3.3 Those who propose, support and seek to implement the project (for example, commercial companies) share an interest in not wanting to frighten people off by suggesting that it will prove to be too costly. So they will aim to supply the lowest figure possible in order to obtain approval, fully aware that once a project is underway reasons for increased costs can always be conjured up and plausibly justified.

c. 3.4 Many government IT projects run themselves into serious difficulties because they are too large, ambitious and technically overly complicated. As such they seriously conflict with the basic KISS design principle: Keep It Simple Stupid. In other words, system complexity should be avoided at all costs; the best and most reliable systems can be developed only where simplicity is a primary goal. My gut feeling about the project proposed here is that it is overly complicated and highly ambitious, and it does not therefore give confidence that anyone will be able to properly guide, control and deliver it. Indeed, the very fact that in your call for evidence you have found it necessary to raise as many as 26 detailed questions is some indication of the project's level of complexity.

d. 3.5 Apart from being overly complicated many government IT projects also suffer from being novel and leading edge. As such, therefore, nobody will be in a good position to predict in advance how things are going to develop and indeed even whether the current objective is going to be achievable and cost-effective. But of even greater significance is that we and the system designers are in the current case confronted with a moving target. In particular, how can we possibly predict the technical developments there are going to be over the next ten years, both in communications technology and systems and how people (including criminals and terrorists) will choose to use them. And to the extent that this cannot be reliably predicted how can an IT system designed today be guaranteed to deal with the changed situation five or ten years hence. This is the designer's major nightmare, the other being politicians' tendency to meddle and seek to change (and usually expand) the design specification part way through.

e. 3.6 Finally, it is possible for certain design features not to be given a proper consideration and not to be properly costed in. In the present case specifically I am concerned that due consideration may not have been given to the proper security of the accumulated confidential data about people's life patterns. Such data could

clearly be of significant value to criminals, and therefore there must be scrupulous care taken to ensure that the data is absolutely safe and will not be leaked or stolen. Achieving this will add considerably to the cost of running this project, and it is vital therefore that it should be properly costed in and not overlooked.

3.7 My conclusion from all these considerations therefore is that the estimated figure of £1.8bn is almost certainly pretty meaningless, and has most likely just been plucked out of the air by someone pressured into doing it for political reasons. And given that such a project has to date never been completed successfully anywhere else on earth, this must place it in the 'very high risk' category. My hunch feeling therefore is that this project could well turn out to be just one more massive IT government project that eventually has to be abandoned. A white elephant in the making.

Question 14. What kind of crimes should communications data be used to detect?

3.8 In the Home Secretary's Foreword to the draft Bill she justifies the need for going ahead with it, viz. "to ensure that the police and intelligence agencies continue to have the tools they need to do the job we ask of them: investigating crime and terrorism, protecting the vulnerable and bringing criminals to justice."
3.9 The most important practical question, therefore, and one which is regrettably not explicitly raised in your call for evidence is whether the project will actually deliver. Will the system work as hoped, and will it achieve its prime objective of successfully bringing criminals and terrorists to justice? If the answer to this key question is 'no' then clearly it would be extremely foolish to embark on it.

3.10 Unfortunately, the harsh truth is that criminals and terrorists are invariably well ahead of the game in these matters. They therefore keep abreast of all relevant technical developments, and they will naturally seek out any system weaknesses that can be exploited. I am not myself an expert in the complex world of security engineering, but I would certainly suggest that the technical viability of the proposed project needs to be scrupulously examined by those with the relevant expertise. One such person would obviously be Ross Anderson, Professor of Security Engineering at Cambridge University, and I trust that his input has already been sought by your Joint Committee and obtained. (http://www.cl.cam.ac.uk/~rja14/)

3.11 Even for the lowest level criminal the state monitoring of all email and internet communications can be readily bypassed merely by stealing or 'borrowing' someone else's smart phone, using it and then quickly disposing of it. But higher level criminals and terrorists will, I'm sure, be constantly developing other and much more sophisticated techniques and strategies for bypassing the monitoring.

3.12 In all crime detection there is, of course, the serious question of 'false positives'. This means that in any system of blanket surveillance and crime detection you will inevitably turn up many innocent people whose internet usage profiles, for example, might incorrectly mark them down as potential suspects. Unfortunately, with very large populations this can reveal so many 'false positive' suspects (typically running into many thousands) that there are just far too many to investigate, and the system becomes completely unworkable. In common parlance this inherent weakness in blanket surveillance is sometimes explained by saying that if you're looking for a needle in a haystack it doesn't help to obtain a bigger haystack. A much more effective and cost-effective strategy would be to opt for intelligence-led monitoring and surveillance, i.e. focusing intensively on your suspects rather than the entire population at large.

3.13 Finally, it is well known that the police at present rely very much on the public for help in detecting and reporting crime. So an obvious question that must be addressed is could the implementation of this state surveillance proposal lead to such a serious alienation between citizens and the police (and the state generally) that people are no longer willing to assist? In other words, a policy intended to improve crime detection might indirectly and ironically seriously impair crime detection. And, of course, there may be many other social and other serious unintended negative consequences of proceeding with this proposal.

August 2012

Wikimedia UK

Wikimedia UK is the Wikimedia Chapter532 covering the United Kingdom. Wikimedia UK is a registered charity with the aim of supporting the development, collection and distribution of "open" educational, cultural and historical, content. Content is "open" when it is available to the general public for no charge, with legal permissions, to view, copy, share, adapt, improve and otherwise reuse (i.e. with 'open' copyright licences).

Wikimedia UK brings together the Wikimedia Community in the UK, to build links with UK-based cultural institutions, universities, charities and other organisations.

Wikimedia UK works closely with the Wikimedia Foundation533, which is the body that operates Wikipedia. Wikimedia UK is incorporated in England and Wales as a company limited by guarantee534 and has no control over Wikipedia or any other Wikimedia Foundation projects535.

Pre-legislative scrutiny

We welcome the fact that the Draft Communications Data Bill ('the Bill') is subject to formal pre-legislative scrutiny by a Joint Committee of both Houses and are grateful for this opportunity to provide a submission of our key concerns regarding the Bill.

Wide scope and lack of clarity in the Bill

Prior to a close reading of the Bill we were unclear of its applicability to us as an organisation and to the members of the Wikimedia UK community. Closer reading of the Bill and the oral evidence given to the Joint Committee during July 2012536 has failed to provide us with much greater clarity or certainty. Our key submission would be that this lack of clarity, certainty, and definition of scope, in the provisions of the Bill are a cause for concern.

We anticipate other organisations, (such as Justice, the Open Rights Group and Liberty)5 that have already provided oral evidence to the Joint Committee, may cover in greater detail the implications of the Bill for civil liberties. We will therefore confine our submission to how we fear the Bill may affect our operations as a charity, our Community and members in the UK.

3. Services of overseas providers

Para 19 of the Bill's explanatory notes states:

'Part 1 builds on existing legislation by requiring telecommunications operators to obtain and retain communications data they would not ordinarily retain for their business purposes for a period of up to 12 months. This might include data relating to (i) the operator's own services which are not within the scope of existing legislation, and from which data is not otherwise retained for business purposes; (ii) the services of overseas providers used by people in this country which transit systems but which the system provider currently has no business to retain.'

---

532 http://meta.wikimedia.org/wiki/Wikimedia_chapter

533 http://wikimediafoundation.org/wiki/Home

534 Wikimedia UK is a Charitable Company registered in England and Wales.Registered Company No. 6741827. Registered Charity No.1144513. Registered Office: 4th Floor, Development House, 56-64 Leonard Street, London EC2A 4LT

535 http://www.wikimedia.org/

536 http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/publications/

Charles Farr, Director General, Office for Security and Counter-Terrorism, Home Office at response to Q48537: confirmed that:

'obligations do apply to overseas providers and in the event, which I regard as unlikely, that co-operation was not possible, an enforcement route would be open to Ministers, if they chose to exercise it, through civil action. This would apply as much to overseas providers as to domestic providers.'

The obligations, under the Bill, which may be imposed on the 'service of overseas providers used by people in this country' is relevant to our consideration of the Bill as detailed below at para 5.

Wikimedia UK and Wikimedia Foundation

We do not have ownership or control over servers that operate the Wikimedia Foundation's projects which projects include Wikipedia. Our public wiki - uk.wikimedia.org - is hosted and owned by the Wikimedia Foundation in the US. All Wikimedia UK staff, some volunteers, and all trustees have administrator rights on uk.wikimedia.org wiki. However, we have no access to data on users from that wiki.

We have access to the contribution history of users on the site, as well as the public communication of users on that site - as does everyone else. The Wikimedia Foundation 'stores/collects' that data.

After studying the Bill we remain unclear as to whether our charity, Wikimedia UK, would be classed as a 'telecommunications operator'.

However we feel it is reasonable to fear that we as an organisation or as individual members of staff, Trustees, or volunteers, who have higher level administration rights in relation to usage data, may fall into the classifications as a Telecommunications Operator.

Such concerns and fears may stifle our operations as a charity, as members and staff who have administration access to usage data, may become fearful, of being subject to obligations under the Bill. In the extreme case the Wikimedia Foundation may become cautious about granting such administrator access to members of the UK community and thereby curtailing the level of participation and activity in the UK. This would affect the charity's ability to achieve its full potential. The charity is a young organisation, with the aim of facilitating the development and dissemination of educational and cultural content. The charity has seen a fast rate of growth in the last year, and has created five full times jobs. Continued growth is forecast. We would not welcome this sort of additional obligations on the charity or its community which could be imposed by the Bill.

The wide scope of the Bill

Francis Davey538, Barrister, writing about the Bill emphasised the worrying scope of the Bill which reinforces some of our concerns:

'the government may do pretty much anything that is at least rationally connected to ensuring that communications data is available. If there was any doubt about this, the rest of clause 1 spells out just how wide the power is, for instance:
requirements ("you must") or restrictions ("you must not") may be imposed on anyone;
the Secretary of State may be given a power to impose requirements and restrictions on anyone by notice

537 10th July oral evidence to Joint Committee http://www.parliament.uk/documents/joint-committees/communications-data/ucJCDCD100712Ev1.pdf
538 http://www.francisdavey.co.uk/2012_06_01_archive.html

those requirements may include forcing the use of particular software, equipment or algorithms …'
'It seems to me that clause 1 is just too wide. It allows far too many things. There are essentially no restraints to stop a determined government doing what it wants.'

Whilst communications data, relating to our community, staff and members, may be more readily acquired by public authorities from ISPs, we remain concerned by the extent of the powers granted to the Secretary of State under the Bill as 'function creep' and 'mission creep' is not entirely unforeseeable should the Bill become law.

By way of example, of mission or function creep, we refer to a point the Chairman of the Joint Committee raised as part of evidence taken on 10th July 2012 (at Q 61) in relation to the existing legislation, Regulatory of Investigatory Powers Act 2000 (RIPA):

'when the Bill [RIPA] was completed there were about 32 public authorities added. Twelve months later, we ended with 500 added and now we have 650.'

Although the above e.g. illustrates the expansion, under RIPA, of the number of public authorities that could request data, we are concerned that under the Bill, more organisations may become subject to notice from the Secretary of State under s1, than may be currently envisaged or intended.

Conclusion

We submit that in its current state the Bill is not fit for purpose for a number of reasons including the ones we have highlighted above. We would draw the attention of the Committee to the fact that the UK would be conspicuous by exception in the democratic world if this Bill was to be enacted. Evidence given to the Committee539 suggests that this extent of collection of data has only been implemented nationally in China, Iran and Kazakhstan and such national scale centralised level of data collection has not been done in a democratic country.

August 2012

---

539 Dr Hosein in response to Q124 http://www.parliament.uk/documents/joint-committees/communications-data/ucJCDCD110712Ev2.pdf

Nic Wisttreich

Modern web services are built around users sharing their personal data and information, in the cloud. This could be sharing photos, videos, status updates, thoughts, feelings, wishes, aspirations and frustrations - and is the lifeblood of the modern digital economy.

Central to the success of this area of innovation - which spans from Instagram to Facebook, Bebo to BlipPhoto - as well as dating and personals sites - is people feeling comfortable and safe about sharing their data and personal information with a server

A 'snoopers charter' which establishes in the mind of the population that they are being watched in public and in private and that anything they say or do will be taken down and could be used in evidence against them - is self-defeating on many levels.

Firstly those who I imagine this legislation is designed to catch - paedophiles and terrorists - will be more likely to use encrypted private channels. Meanwhile the rest of us will grow ever more anxious about using digital services that encourage us to share our passing views and experiences with the world.

There's also the very real issue of how to keep such a database secure. This is the kind of issue that someone who hasn't spent their life in IT will assume is as easy as the IT contractor convinces them it is. But it isn't. It would be a huge database, and filled with information that could be used to blackmail or threaten people. How many people may not want to 'come out the closet' about their sexuality? Or religious views? Our political, religious, sexual, social and idealogical interests are an indisputable part of our human freedom and we have an unbreakable right to keep them private - unless there is good cause to believe we might be doing or about to do something wrong.

Instead, this presumption of guilt - for the whole population - with full-time state surveillance would be a sad, backward, misguided step. It may seem well-intentioned and harmless now, but none of us can predict how a future government may chose to use it - nor indeed do we now the consequences it could have for reducing use of web 2.0 services - and pushing real criminals to better encrypted channels.

I urge you to step back from the brink and take a look at the peaceful passing of the Olympics as clear evidence that we are not in such an emergency as to need such tinpot dictator measures.

August 2012

Ben Woodling

Thank you for taking the time to consider my views upon the Draft Communications Data Bill.

I was alarmed when hearing of early plans for this Bill some months ago and have unfortunately not had the time to follow developments closely.

Looking from a broad perspective, citizens of this country have seen their civil rights eroded in the early years of this millennium at a rapid rate. New police powers to detain terror suspects for 28 days without charge, new stop-and-search powers handed to the police, and restrictions on the right to peaceful protest have all been introduced in recent times. Groups defending civil liberties are understandably shocked by such changes.

In writing to yourselves I wish to write a substantive and informed letter as opposed to merely signing an online petition. Please note, however, that I have been made aware of this consultation process only via contact by the campaigning site 38 Degrees. I will reply to some of the 26 questions in detail but first I will try to surmise my thoughts on what I find most worrying about this Draft Bill.

Crucially, I think that the changes proposed in this Draft Bill would overall have a negative effect on the health of UK citizens and lead to an increase in crime. Paranoia is a serious and increasing problem in our society. The fear that one is being watched is a very common neurosis and mental health complaint. The central provision in this Bill is to enable the state powers and relevant authorities to trace the internet and telephone communications of the public. Once implemented the idea that 'Big Brother is watching you' is given further credence and reality. The Bill seems to suggest to the public that "in order to keep you safe and well, we will police your conversations." It is hard not to infer from this that the Government wishing to make such proposals law is one that is paranoid about its own citizenry.

I don't wish to live in a country where paranoia is such a marked concern. It is because of this that I oppose the Bill. Tragic as the 7/7 terrorist atrocities were I do not recognise the need for heightened security measures in the shape of snooping powers. I want a Government that supports, encourages and believes in its people, not one that mistrusts them.

In reply to the 26 questions:

1. No.
2. No. Theresa May's comments in the Commons: "As criminals make increasing use of internet-based communications, we need to ensure that the police and intelligence agencies continue to have the tools they need to do the job we ask of them: investigating crime and terrorism, protecting the vulnerable and bringing criminals to justice." This is political media-spin. These comments fail to address the significant civil liberties and technical concerns that many interested parties seek answers to.
3. Very poorly. I perhaps can't say too much about the Leveson Inquiry but there have obviously been severe criticisms of the snooping powers of News Corporation and suggestions that both the Metropolitan Police and Labour and Conservative governments have been, if not involved, highly aware that such snooping put that media multinational in a position of much power. With access to communications information through technical gadgetry becoming more widespread and potentially purchase-able I feel the sensible move for the Government and police is to back off from infringing on the public's right to privacy.
4. Plenty of other countries happily work with Judicial warrants for Communications Data, rather than the UK "self-authorisation" approach.
5. Data Preservation for specific, narrowly targeted investigations, restricted to Serious Crimes only, rather than massive Data Retention of almost entirely innocent data.
8. Yes, I think that is quite possible. This could result in higher consumer prices.
9. I very much doubt that forecasting a budget for a ten year implementation can in any way foresee changes to policies, political and economic developments lying ahead, let alone technical difficulties. Financially, I think this money could be better allocated to spending on more conventional public services such as schools and hospitals.

10. No. I would imagine that a select group of company owners and shareholders may for a while make millions of pounds through the contracting out of this scheme but it would lead to a financial loss for the average UK taxpayer.
11. No.
12. There must be no Order making powers at all in the Communications Data Bill.
13. Mostly unrealistic. Not helpful for fighting international terrorism.
14. Serious Crime only.
15. Much too long.
17. Yes. A warrant signed by an independent Judge (not one signed by the Home Secretary or any other politician or senior Whitehall bureaucrat) which can be challenged in Court if necessary should be required for all Communications Data snooping, including the Police and Intelligence Agencies.
18. No.
19. No.
20. No.
21. Failure to adhere to the Code of Practice should not amount to an offence.
22, 23, 24, 25 and 26 are technical questions which are difficult to answer.
25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ? is an interesting question. One would have to have intent to circumvent policing by this method and perhaps technology to get around such methods, or a private telephony network. Serious fraudsters and terrorists would be quite likely to pay to access such methods of avoiding their communications being policed. It becomes easy to forecast that while the implementation of this scheme would cost much, the security services would be chasing those groups working off-the-radar.

I am no expert on these issues. There is such confusion surrounding technology, communications data and state surveillance powers. I think that broadening the range of collection of communications data is a costly and backwards step.

August 2012

Andy Wrigley

Safeguards

The draft bill does not appear to adequately protect the public:

1. We have recent examples of corrupt police officers leaking personal information; and not quite so recent cases of security service personnel obtaining and using information illegally because of their own political persuasion. Likewise telecoms workers have been jailed for obtaining and using personal data in fraud.

This bill would create huge sources of personal data. The Government has a duty to protect our personal data. Evidence shows that personal data is accessed illegally, so controls like "approval" and "warrants" will not protect us.

i. How will you prevent illegal use of this information?

As I see it, you would have to have software monitoring and recording access (true prevention is impossible). To be reasonably effective, and make circumvention harder, monitoring would have to be located on every server gathering and storing the data. To reliably alert on misuse (surely necessary) would require Artificial Intelligence capabilities that don't currently exist.

ii. are safeguards that reliably prevent, or alert on illegal use, to be included in the draft? If so what is the mechanism and how much will it cost?

2. We currently have freedom of expression. You cannot guarantee that the UK will never have a totalitarian Government. I'm sure that in the economic depression of the 1920s the majority of Italians, Spanish, and Germans didn't anticipate their future fascist regimes. Imagine what the Nazis could have done with access to stored information on everyone's correspondence and contacts. These powers are similar to those employed by China and Iran and would be a gift to any arm of the UK Government that wished to abuse its authority.

iii. How can you prevent a future totalitarian Government from ignoring or amending laws to access the information stored as a result of the Act e.g. to weed out and imprison people for views they expressed privately?

Short of issuing all UK subjects with a "stored data destruct button" I cannot see how this abuse could be prevented.

You may view this as a small risk. However, its potential impact, and consequences, on the people you represent, is so great it cannot be ignored.

Political/International Standing

3. The UK has been critical of China's policy towards the internet and its citizens. A few months ago I saw this comment (re draft bill) in the Chinese press justifying their policies "the British government has finally recognized that a balance needs to be struck between freedom and monitoring".

iv. If this bill is passed, how would the Government and the Opposition respond to such comments in the Chinese press?

Effectiveness

4. As someone who has worked in IT and security for 30 years I consider these proposals will have minimal additional impact on preventing or investigating crime/terrorism. The terrorist and criminals we need to be afraid of will be able to circumvent the information gathering.

5. Existing laws already allow monitoring of suspects such as terrorists. Existing laws were also sufficient to quickly identify and arrest the Facebook user inciting a riot, and also the person who tweeted abuse to Tom Daley. They would not have been pre-emptively identified and arrested because of a Communications Data Act".

6. When passed, it might aid in the arrest of a small number of minor criminals, but at the cost exposing your voters private data to risk, personal privacy/freedom; and place us in the same police state camp as China, Iran, the USSR and Nazis.

August 2012

The Information Commissioner

Summary

- It is for Parliament to determine whether the proposals contained in the draft Bill are a proportionate response to the perceived problem of communications data capability;
- If the case is made then the practical consequences of the proposals must be identified and addressed;
- The compensatory safeguards which are to be put in place must have a clear and specific purpose and be effective in practice;
- The extent of the Information Commissioner's role needs to be clear so that both he and the public know what outcomes or assurances his oversight will bring;
- There should be provision for the Information Commissioner to report on his activities;
- Any extension of the Information Commissioner's functions or increase in the volume of work undertaken by his office will need to be properly resourced; and
- There should be some form of post-legislative scrutiny stipulated on the face of the legislation

Introduction

1. The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), together with associated legislation such as the Privacy and Electronic Communications Regulations (PECR).

2. He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals and taking appropriate action where the law is broken.

3. This evidence will focus on those aspects of the draft Bill that fall within the Information Commissioner's regulatory remit, the practical considerations arising, and the adequacy of the proposed safeguards and limitations to mitigate the impact on the privacy of individuals.

4. The Information Commissioner is aware of concerns expressed by both this and the previous government that existing provisions providing access to communications data for law enforcement purposes are becoming ineffective as developments in technology and its use have evolved. But, to some people, proposals to extend further the State's requirements on commercial operators to retain and disclose their customer's communications data would be very difficult to justify on any grounds.

5. The Information Commissioner takes the view that it is for the Government to make a clear case to Parliament as to the necessity of further statutory provisions regulating the availability of communication data to law enforcement and other bodies. If that case is made to the satisfaction of Parliament, and legislation proceeds, then there need to be adequate and effective safeguards in place to minimise intrusion into the privacy of personal information.

6. The Information Commissioner has pressed Ministers to put in place the necessary limitations and safeguards to mitigate the impact of the proposed legislation on people's privacy. Over the past year or so, the Home Office has kept his office informed of the progress of its plans and we have been consulted on the development of its Privacy Impact Assessment (PIA). We are pleased that the Home Office has recognised that it is essential to identify the key privacy issues by using a formal assessment process.

7. The Government has recognised that the proposals raise important issues around personal privacy and that it is for Parliament to determine whether or not the proposals contained in the draft Bill are a proportionate response to the perceived problem of communications data capability. The scrutiny of the draft Bill by the Joint Committee is an essential part of the process of ensuring that there is the fullest possible parliamentary scrutiny of these proposals.

8. In this scrutiny, it is important that the consequences of the proposed new legislation, beyond enabling enhanced law enforcement access to communications data, are adequately identified and addressed. For example, once data are retained for longer than is currently the case, there is the risk that organisations will then wish to exploit this retained data for new commercial purposes beyond current use. Account also needs to be taken of the way in which practices may evolve, such that the proposed arrangements and safeguards could be sidestepped in practice.

9. For example, we are aware that some police forces are now routinely accessing individuals' mobile phones on arrest to gain access to call logs and other information held on the device. This may not only circumvent existing safeguards but also put the personal information of third parties who are not suspected of any wrongdoing into the hands of the police.

10. The Home Office's PIA recognises the need to consider the adoption of privacy enhancing technologies (3.2) and sets out its assessment at Annex D of the PIA. There does not though appear to have been any consideration as to whether specific technologies or procedures could be deployed to restrict the ability for the communications data to be consulted during the prolonged retention period after it has served its business purposes. Such an approach would reduce the risk of the retained data being accessed inappropriately, in particular by telecommunications operators and their staff.

Proposed role for the Information Commissioner

11. Clause 22 (5) of the draft Bill states that the Information Commissioner 'must keep under review the operation of sections 3 and 6 of this Act'. Section 3 refers to data security and integrity and section 6 to the destruction of data.

12. Clause 22(6) requires telecommunications operators who hold communications data by virtue of the Act to keep a sufficient record of things done by them to enable the Information Commissioner to effectively discharge any relevant functions.

13. There is little additional published information, in either the Home Office's background briefing to the legislation or the explanatory notes in the draft Bill, on what this means in practice. Nor is it clear how it is intended that the Information Commissioner should go about his tasks and report on his activities.

14. It is essential that the compensatory safeguards that are stressed in the Home Office's PIA, and which are to be put in place, have a clear objective, are effective in practice and are not merely cosmetic if they are to genuinely prevent unwarranted intrusion and therefore inspire public trust and confidence.

15. It is important to the Information Commissioner that both he and the public know what outcomes his oversight is expected to deliver and how it is intended that this oversight will be delivered in practice, particularly if it is to extend beyond his existing regulatory functions under the DPA and PECR. Any extension of the Information Commissioner's functions or increase in the volume of work undertaken by his office will need to be properly resourced. It is not clear from the Bill where these additional resources will come from.

The duty to "keep under review"

16. In Clause 22(5) it is not clear what the duty to 'keep under review' the operation of sections 3 and 6 is meant to achieve in practice. The explanatory notes provide no additional clarity, mentioning only that the subsection 'provides for scrutiny' by the Information Commissioner of these provisions.

17. If the intention is for the Information Commissioner to play an active role in inspecting and then assessing whether safeguards are being adhered to in practice then this wording falls short of achieving

the desired objective.

18. As is set out in greater detail below, the Information Commissioner's existing powers to assess processing are also insufficient. The Information Commissioner has powers ranging from the ability to assess processing in certain specified areas through to the power to serve information notices in well-defined circumstances. However, these fall short of the powers needed to undertake ongoing, effective and proactive scrutiny of a telecommunications operator's activities.

19. If the intention is for the Information Commissioner to undertake some form of general review exercise, it is not clear what information would be available to him to enable him to arrive at an informed conclusion. It may be possible, with the close co-operation of telecommunications operators and other relevant regulators, to build up an impression of whether the provisions are being adhered to; but that might only be of partial and limited value given the complex technical nature of the proposals. It is hard to see that it would provide the level of safeguard envisaged by those promoting this legislation or as reflected in the Home Office's PIA.

20. The practicalities of undertaking an effective oversight function should be fully understood and addressed in advance.

21. For example, the Information Commissioner already has a limited role in monitoring the security provisions applied to data retained under the terms of the Data Retention (EC Directive) Regulations 2009.

22. One practical problem here has been the reluctance of the Home Office, on the grounds of national security, to supply the Information Commissioner with a list of service providers who are required, by notice, to retain and provide communications data under the Regulations. Not knowing who the relevant providers are and hence who he is supposed to be monitoring clearly restricts the effectiveness of the supervisory regime.

23. Similarly, the draft Bill provides for the Secretary of State to issue notices to telecommunications operators imposing requirements (Clause 1(2)(b)). It is not clear whether the details of the operators to whom these notices are issued will be in the public domain or even available to the Information Commissioner for his supervisory activities. Not only does the Information Commissioner need the powers over telecommunications operators and the resources necessary to provide the oversight he is expected to deliver, he also needs a right to receive relevant information from the Secretary of State.

Current audit powers

24. The Information Commissioner already has a limited power of compulsory audit over 'providers of a public electronic communications service' (service providers) under PECR. Many of these service providers are the same as those who will have enhanced obligations under the draft Bill.

25. Currently, the Information Commissioner's powers are limited to ensuring that appropriate technical and organisational measures have been put in place to safeguard the security of the communications service. This would not cover reviewing the operation of the extended retention periods required under the draft Bill or the integrity of retained data.

26. The Information Commissioner also has a limited power of compulsory audit under the DPA (section 41A). This 'assessment notice' power currently only extends to government departments. In contrast to the PECR audit powers, section 41A of the DPA clearly sets out the scope of the compulsory audit power, and the requirements and obligations of both the organisations subject to audit and the Information Commissioner. It also requires the Information Commissioner to produce a Code of Practice as to how these audits will be conducted.

27. In the Information Commissioner's experience, if there is to be an effective system of safeguarding audits of the compliance by the telecommunications operators with the requirements of the draft Bill, some clear statutory direction as to the powers of the Information Commissioner and the intended scope, detail of and timescales for such audits is needed.

28. This would provide the Information Commissioner with some clarity as to the nature and scope of the work required, and enable him to ensure that his office has the capacity and capability to fulfil its expected role. It would also provide greater clarity to the public and the organisations affected as to what level of scrutiny will be applied to the retention of communications data and what this will mean in practice.

29. Furthermore, it would provide an opportunity to ensure that the various different regulatory regimes to which telecommunications operators are subject operate consistently together.

30. One possible approach would be to use the existing compulsory audit powers in the DPA as a basis and apply them to telecommunications operators. This would build on the existing safeguards detailed in the Home Office PIA (5.3). It would also enable the Information Commissioner to keep under review the application of all the legally enforceable data protection principles.

31. A number of these principles focus on data quality requiring organisations to ensure personal data is adequate, relevant and not excessive (third principle), accurate and, where necessary, kept up to date (fourth principle) and is not kept longer than is necessary (fifth principle).

32. Using the Information Commissioner's existing powers would mean that the telecommunications operators would be subject to a well-established regulatory tool which is already accompanied by a recently reviewed Code of Practice, approved by the Secretary of State. Such oversight would be comprehensive, operable immediately and would also provide consistency with pre-existing regulatory arrangements.

Destruction of the data

33. The Information Commissioner's general concern about safeguards being meaningful and effective in practice is relevant to the provisions at Clause 6. These require a telecommunications operator to:

- destroy data at the end of the retention period (Clause 6(1)) and
- ensure that this is done in a way that the data can never be retrieved (Clause 6 (2)).

34. Clause 6 (3) provides that it is sufficient for the operator to make arrangements for the destruction of data at monthly or shorter intervals.

35. On the face of it the requirement to destroy data so the data can never be retrieved is a welcome one and one that is consistent with the principle that personal data shall not be kept for longer than is necessary. However it is not clear how the requirement to 'destroy' data relates to the way in which operators achieve deletion of existing records in practice. This section, as drafted, seems to envisage the physical destruction of media rather than the routine logical deletion of data in a way that for all practical purposes 'puts it beyond use'.

36. The overarching concerns of the Information Commissioner are how achievable the destruction envisaged in the Bill is in practice and how he can keep under review the operation of these requirements short of a power to inspect the relevant information systems of operators to actually check that data is no

longer being retained.

37. Further, even if the Information Commissioner had inspection and/or audit powers it would still be technically and practically challenging for him to establish that data that have supposedly been destroyed 'can never be retrieved'.

Reporting

38. The draft Bill does not impose any requirement on the Information Commissioner to provide reports on his review activities, either in general or in relation to the supervision of individual telecommunications operators. The Information Commissioner has existing duties to present an annual report to both Houses of Parliament and a power to present other reports to Parliament.

39. In the absence of any specific duties to report on his review activities the provision of reports would be at the discretion of the Information Commissioner. Introducing a specific obligation to report to Parliament on his review activities would assist the ongoing post-legislative scrutiny referred to in further detail below and provide an additional element of assurance to the public.

Scope of powers

40. The draft Bill envisages roles for both the Information Commissioner and the Interception of Communications Commissioner. It is important that these functions are complementary. The Information Commissioner, in cooperation with the other Commissioners responsible for monitoring different aspects of surveillance, has produced a surveillance road map to provide a clear explanation of the differing regulatory responsibilities and how these inter-relate **(Annex A)**. This reflects an increasing level of cooperation between commissioners.

Resources

41. The Communications Data Legislation Impact Assessment recognises, in its section dealing with 'full economic assessment', that there will be additional burdens and workload for the Information Commissioner. This Impact Assessment does not quantify the cost associated with these additional burdens. Given the current lack of precision about the practical extent of the functions the Information Commissioner is expected to perform, maybe this is understandable.

42. The Information Commissioner will need adequate additional resources to perform these functions and it needs to be clear who will provide these resources. If they are not forthcoming, the Information Commissioner's review activities may fall short of providing the safeguards they are meant to deliver.

Impact of new EU data protection legal framework

43. The Committee should be aware that in the next few years the UK is likely to be subject to a new data protection regime. The European Commission's current proposal is to introduce a general data protection Regulation and a separate data protection Directive. The latter will apply to the processing of personal data by law enforcement agencies for crime prevention and detection.

44. Both the Regulation and the Directive are at a relatively early stage in the legislative process. It is therefore difficult to speculate on their possible impact on the framework for communications data retention and access.

45. However, the Committee should be mindful that a new data protection regime is on its way. This is likely to have a significant impact on the Information Commissioner's powers and duties and could have an impact on the nature of the oversight mechanisms for any legislation involving additional retention of, and law enforcement access to, personal data.

Access to communications data

46. The draft Bill provides for relevant public authorities to be granted access to communications data (Clause 9). The definition of 'relevant public authority' includes the police, intelligence services and HMRC. There is provision for the Secretary of State to specify additional public authorities who may have access by statutory instrument, mirroring the existing RIPA provisions (Clause 21(1)).

47. Separate access authorisation arrangements apply to local authorities who must seek judicial approval for each authorisation (Clause 11). The Information Commissioner welcomes the introduction of a more rigorous approach to controlling access to communications data than that currently provided for under RIPA.

48. The Information Commissioner is aware that the Home Office is already in the process of ascertaining whether the additional public authorities currently specified under RIPA should be specified under the new arrangements. This is a welcome step and all such public authorities should be required to make a persuasive case as to why they should have access and why this should be granted without judicial approval.

49. The Information Commissioner has made a case for his continued access. He requires this primarily for the investigation of offences contrary to section 55 of the DPA (commonly known as the 'blagging' offences) where access to communications data has proved to be an essential source of evidence. There could also be a need to obtain communications data in relation to offences such as non-compliance with enforcement notices and offences of altering or deleting records under section 77 of FOIA.

Post-legislative scrutiny

50. The Information Commissioner welcomes detailed parliamentary scrutiny of the draft Bill. The Committee's consideration of the draft Bill is an essential part of that process. However, even if Parliament is persuaded of the need for these measures, parliamentary scrutiny should not end when legislation is enacted.

51. Justification for the intrusion involved in the proposed measures is provided, on paper, by the Government's and the law enforcement communities' assessments of the supposed benefits of data retention and access to additional communications data. These aims need to be realised in practice.

52. Empirical evidence collected and produced must demonstrate that the measures proposed by the draft Bill achieve their intended effect in practice and that the associated privacy intrusion continues to be warranted.

53. Some form of formal post legislative scrutiny should be put in place so that Parliament can undertake an evidence based reassessment of the value of the legislation. The Information Commissioner would therefore welcome the inclusion of a 'sunset clause' requiring renewal of the legislation at a future date.

54. Including a form of post legislative scrutiny is in line with one of the Information Commissioner's recommendations in his report to the Home Affairs Committee on developments that lead to increased surveillance of the citizen **(Annex B)**.

55. Such evidence based scrutiny will help to ensure that the benefits have been correctly weighed against the privacy risks and that the measures enacted continue to be a proportionate response to the perceived problem of communications data capability.

56. It has, in any case, been recognised by government that some form of post implementation review is necessary. The Home Office's Impact Assessment refers to a Post Implementation Review Plan five years after implementation. This would assess whether the new legislation has achieved its objectives, assess the costs and benefits and identify whether there are unintended consequences.[540]

57. This should, though, be a formalised process, linked to effective parliamentary post legislative scrutiny and not just an internal administrative initiative. Furthermore, given the potential privacy intrusive nature of these proposals, Parliament might wish to consider whether the timescale should be shortened and any review report published.

Christopher Graham
Information Commissioner
21 August 2012

[540] Communications Data Legislation Impact Assessment – 'Evidence Base' – 'J. Monitoring and Evaluation'

Internet Telephone Services Providers' Association (ITSPA)

About ITSPA
The Internet Telephony Services Providers' Association (ITSPA) is the UK VoIP industry's trade body, representing over 60 UK businesses involved with the supply of VoIP and Unified Communication services to industry and residential customers within the UK. ITSPA pays close attention to the development of VoIP and IP regulatory frameworks on a worldwide basis in order to ensure that the UK internet telephony industry is as competitive as it can be within international markets.

Please note that certain aspects of the ITSPA response may not necessarily be supported by all ITSPA members. Individual members may respond separately to this call for written evidence where a position differs.
A full list of ITSPA members can be found at http://www.itspa.org.uk/
As the joint committee will understand, it is difficult for a trade association with a broad membership to respond to each individual question with a uniform answer. Members have different experiences surrounding data requests from law enforcement and local authorities and different positions (based on the services they supply) on the proposed legislation put forward by the Coalition Government. We have responded in general terms, following several discussions with our members and highlighted specific points of concern and interest which we hope the Joint Committee can investigate further. ITSPA members would welcome the opportunity to discuss specific points at greater length with the Joint Committee, should it be deemed necessary.

General Comments
ITSPA welcomes the opportunity to provide written evidence to the Joint Committee on the Draft Communications Data Bill. It is an important piece of legislation that needs to be scrutinised effectively to ensure a workable process can be implemented. Law enforcement organisations must have access to the communications data they need to tackle serious crime, however the communications industry must not be overburdened with a regime that causes operational difficulties or infringes on their customers' privacy. Whilst ITSPA accepts the sensitive nature of some of the issues surrounding this legislation, the confidential nature of some areas have made it difficult for our members to respond as comprehensively as we would like. We would urge the Joint Committee to gain greater detail from the Home Office in order to provide industry with greater clarity of the long term implications of the draft Bill.
The main concerns for ITSPA members in terms of scope are the precise type of data sets that will be required in the future and the exact requirements surrounding both third party data and compliance of overseas providers. These are key areas that we believe the Joint Committee should focus on to ensure the proposals can work in practice.

Law Enforcement Requirements
As previously mentioned, ITSPA recognises the importance of communication data for law enforcement agencies as they seek to prosecute crime. We accept that the way people (and criminals) communicate is shifting, due to changes in technology. It is important that law enforcement keeps up with these trends. ITSPA members cooperate fully with the data requests under the existing legal framework.
From an initial perspective, particularly for 'pure' VoIP providers (those providing only IP telephony and not other services like instant messaging), there would appear to be only minimal changes to the current obligations. However we do have concerns surrounding any future requirements that this Bill may bring on the VoIP industry, which is not clear in either the content of the draft Bill or in discussions with the Home Office. There appears to be a lack of clarity as to whether other data sets (not retained for normal business purposes) will have to be retained by telecommunication providers in the future and it is therefore hard for ITSPA to make an assessment of the long term implications for the industry. We accept our responsibilities to support law enforcement agencies but the relationship must be built on trust and effective communication as to how this legislation may affect the industry going forward.

We would also question the suggestion that this draft legislation is merely maintaining current capabilities for law enforcement agencies. Whilst it is true that the draft Bill is focussed on bringing new technologies into the scope of the current regime, there are a number of other areas that strongly suggest an extension of scope. These would include the new filtering arrangements, retention of third party data and the changing of definitions surrounding communications data and telecommunications providers. This does not necessarily impact the majority of our members (at least in the short/medium term) but it will certainly have an impact to the wider communications industry and could potentially impact VoIP providers in the future. This is why ITSPA requests further clarity on the proposals involved and we would ask the Joint Committee to investigate further.

Filtering Arrangements and Technical Issues

There are also significant concerns as to how a filtering system would work without significantly disrupting communication providers' (CPs) operations, inadvertently capturing communications content, and/or creating dangerous opportunities for the leakage of sensitive data or data fraud.

ITSPA would welcome further investigation into how data will be collected under a notice and how the filter will interact with the CP. There have been suggestions that the Home Office may require a direct feed to the providers' data base. This could cause a number of problems in terms of both consumer data security and for the operations of a CP. There are also question marks surrounding how the interaction with the filter will be affected by any network upgrades or configuration changes that the CP may need to undertake. This could cause both operational problems and have financial implications for the CP; it is unclear as to whether this element of cost recovery would form part of the Home Office's new obligations. Equally there are competition concerns around this point. CPs who have not received a notice and do not interact with the filter, will not be hampered by the potential hazards surrounding network upgrades. Further information on how the filter would work is vitally important. ITSPA members would be concerned if a similar system to the Netherlands was adopted, whereby CIOT (the authority responsible) can require that registered communications providers install a direct feed into their servers so that CIOT can download data every 24 hours. We believe that the Dutch arrangement is not proportional to the need and can result in serious implementation issues for CPs.

In terms of some of the technical queries outlined, ITSPA does believe that there are vendors who are able to offer the solutions to capture the necessary communications data. However, the safety and security concerns cannot be underestimated. It would be an extremely challenging process for the industry to undertake. CPs would be obligated to ensure third party data was captured and that the filter could cope with enormous volumes of data. Such data, when aggregated, becomes important and extremely sensitive information, which increases the business impact level and security threat. Some data may include government data up to the Restricted level (as is allowed over the ISDN). The costs of storing such data can be prohibitive and the risks must be evaluated properly.

Costs

ITSPA does not believe that the Government estimate of £1.8bn over 10 years is realistic. We feel there are too many factors that may contribute to this cost rising significantly. It could cost large CPs hundreds of millions of pounds to integrate and store data correctly, to include third party data and other information that they would not usually store for business purposes. Over time, as data requests are made to smaller providers, the extra costs will also filter down, creating a significant financial burden.

There is also an assumption by the Home Office that access to data from overseas providers will be relatively straight forward. ITSPA members are less convinced this will be the case and we believe the costs could be higher than estimated. Future developments and capabilities within the communications space will also mean that law enforcement agencies may have to shift their focus to other methods of communication and this will inevitably mean a stark increase in overall costs.

We welcome the Home Office's commitment to cost recovery and would stress this as a requirement for any final legislation. This commitment is fundamental to ensure an effective system is maintained. Whilst ITSPA has not had insight into how the Home Office has costed their proposals, we fear the projected figures are too optimistic, given the technical challenges that the wider communications industry may experience.

In terms of cost benefits, ITSPA does accept that there could be considerable savings and suggest that this could even exceed the £5-6bn suggested. The more effective the communications data that law enforcement agencies receive, the more efficient they will become in solving crimes, catching criminals and coping with major incidents (such as public disorder). This will create financial efficiencies within the respective organisations and reduce the financial loss that both individuals and organisations experience when they are victims of crime and fraudulent activity. However, as previously indicated, ITSPA does expect the costs to implement these changes to be more expensive than predicted which needs to be taken into consideration when deciding the true value of the draft Bill for both law enforcement organisations and society as a whole. Given the economic constraints on Government at present, there is a need to ensure the financial costs are truly going to bring tangible benefits.

Safeguards and Oversight

The filter will have access to an enormous amount of data and will need some strong controls to prevent misuse and protect against criminal hacking. There is also the concern that it will be unavoidable in some instances to prevent collating content. Certain information required by enforcement agencies will contain content embedded in the data that cannot be removed without destroying the data. For example, in web access logs the destination urls can contain information that discloses the nature of the content. ITSPA feel that in terms of the existing communications data that is stored or for data that is anonymous, the safeguards currently in place would be sufficient. However a warrant system should be considered for data that included content when it was not possible to supply anonymous access data without rendering the data meaningless.

In terms of everyday oversight, ITSPA members are generally happy with responsibility being devolved to the Interception of Communications Commissioner's Office (IoCCO) and the Information Commissioner's Office, provided they are sufficiently resourced and have the technological understanding of the services being used. There have been questions raised by some members surrounding the amount of parliamentary oversight to the draft Bill and whether too much power will lie with the Home Secretary in this area once legislation is passed. ITSPA members are satisfied that the sanctions currently in place under the present regime will be sufficient under any revised legislative framework

Peter Buneman FRS FRSE & Michael Fourman FRSE FBCS

We are aware of the responses already provided by JANET and by Prof. Ross Anderson on behalf of the Foundation for Information Policy Research (FIPR). We endorse the various points well-made in these submissions.

In particular (question 24), the proposed techniques will not detect people communicating over obfuscated and encrypted channels. Nor is it possible to do so without breaking the internet. Put simply, the proposed bill is only useful against dumb terrorists, not smart ones–but it will increase the risks of privacy violations for all users.

We wish to highlight two further concerns that arise from our particular expertise (databases and telecommunications infrastructure) and experience.

1. The first stems from our research and practical experience in identifying and addressing shortcomings in the UK's digital infrastructure. The UK has been lagging behind other countries in the development of its communications infrastructure, and current initiatives will reinforce a growing digital divide. We are convinced that the only way to bring the UK into the forefront of digital communications technology is to provide an open infrastructure and to encourage, especially in suburban and rural areas, the growth of networks that are constructed and managed by small businesses and communities. This is an approach
that has already been adopted by other countries such as Sweden.

We are concerned that the proposed bill would inhibit the organic growth of the UK's digital infrastructure, by making it difficult or impossible for communities and small enterprises to fill the gaps not addressed by large-scale providers.

28. It will place an extra burden on small organisations to provide, manage and maintain the means for interception and retention.
29. It will implicitly require people in these communities to spy on each other -- or at least require them covertly to sanction spying.

There appears to be no consideration of the unintended costs (negative externalities) that might result from these proposals. We have just given one example. We suggest that the committee should consider what others there may be.

2. The second concerns the technical feasibility of the proposals (questions 22-26). We note that, although the act may specify that a piece of software should (or even must) satisfy a certain criterion, it does not follow that a practical implementation will be able to do so. In general, it will be impossible to check whether any particular implementation does so, and we must anticipate that any failures will be exploited.

In two places (6(2),16(1)(c),) the draft document requires that data 'must be destroyed in such a way that it can never be retrieved', and this 'safeguard' is stressed in the commentary. We assert that this cannot be reliably achieved for a data retention system with the scale, scope and robustness required by the draft act.

Throughout the commentary we see a quaint confidence in the effectiveness of regulation. For example, in paras 96-100 of the commentary we find (inter alia):

- Subsection (1) **will ensure** that only the filtered data relevant to the investigation is disclosed to the requesting agency.
- Subsection (2) **limits** the disclosure…
- Subsection (4) requires that an adequate security system is in place to protect against any abuse of access...The duty in subsection (4) **will ensure that** a Request Filter can only be used in accordance with Part 2 and **is subject to adequate and effective safeguards** against abuse.
- Subsection (5)(a) requires procedures to be put in place and maintained **to ensure that** the any Request Filter is functioning properly, including regular testing of the relevant software and hardware.

In each case, the emboldened words are intended effects of regulation that cannot be guaranteed. We believe they highlight loci of potential failures in the information security presumed by the draft.

Professor Ross Anderson FRS FREng

At the hearing on September 4th, you asked me for a note on what the ETSI documents reveal about government intentions in respect of communications data, and any other matters I cared to add. I also owe you a pointer to our report for the MoD Chief Scientific Adviser on the costs of cybercrime, and to our note to the Interception Commissioner.

The intelligence community and their key suppliers are leading a push in the European Telecommunications Standards Institute to standardise law enforcement access to cloud services. They have a technical committee ('TC lawful interception' or ETSI TC LI in short) staffed by people from the agencies, the telcos, the vendors and interior/justice ministries, with a very strong British contingent. ETSI TC LI has worked in the past on law enforcement access standards for mobile phones (call data, location data, and content); they have switched to working on similar standards for web services firms (who appeared to be unaware of this work until we brought it to their attention in July).
The key document may be :
ETSI DTR 101 567:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_LI/2012_45_Bratislava/SA3LI12_044.doc (the most recent version is at http://t.co/aMKMsd0X). This makes the philosophy clear. "If a Communication Service Provider (CSP) elects to implement a cloud service and becomes a Cloud Service Provider (C(L)SP), their legal obligation to support LI is unchanged; the requirements defined in ETSI TS 101 331 [i.1] still apply. What may be impacted are the technical solutions outlined in ETSI LI standards as the underlying architecture may be changed by the implementation of cloud services."

As I believe I mentioned on the 4th, BT now outsources email services for its residential Internet customers to Yahoo. Previously, law enforcement and intelligence agencies could get communications data, or intercept content, directly from BT's servers with the appropriate paperwork. Now both traffic data and content are stored on Yahoo's servers. Presumably BT's contract with Yahoo supports continued law enforcement access when paperwork is served on BT in the UK; the Home Office is presumably concerned about what happens if a customer switches their email from Yahoo to Google.

The stated goals include 'nomadic access' which means surveilling a Facebook user whether she goes online from her home DSL, her mobile or an Internet cafe (as I noted in my testimony). Service providers will have to build surveillance in: "In order to maintain LI coverage the cloud service provider must implement a Cloud Lawful Interception Function (CLIF). This can be by way of Applications Programming Interface (API) or more likely ensuring presentation of information in a format recognisable to interception mechanisms. Deep packet inspection is likely to be a constituent part of this system."
ETSI DTR 101 567 also makes clear that the policy concern is interception in the large, not just access to communications data. This was the concern of the previous government's Interception Modernisation Programme, and you might care to note the Home Office view that the Labour consultation on IMP forms the necessary outreach for the CDB under Cabinet Office rules on consultations (this was 'Protecting the Public in a Changing Communications Environment', at http://www.official-documents.gov.uk/document/cm75/7586/7586.pdf).

Another emerging aspect of the overall strategy is that GCHQ staff are working to standardise new key establishment protocols using 'key escrow', which the Blair government also advanced in 1997–9, but which appeared to have been abandoned with the RIP Act. You will recall, my Lord, that in the debates over section 3 of the RIP Act the banks strongly objected to the police and intelligence agencies getting covert access to crypto keys lest corrupt officers forge banking transactions, or lest the banks lose the ability to defend themselves against civil suits where a plaintiff disputing a transaction could allege that a bent policeman had stolen the money, and the bank would have no way to rebut this. In debates over Section 3 of RIP, you argued that demonstrating an 'intention after the fact' to impede access to encrypted information should be an essential element for criminality; regrettably the amendment was not accepted by the government (Hansard, 8 May 2000, Column 550). Parliament nonethless in its wisdom decided that an order for the production of a cryptographic key would have to be signed by a Chief Constable and presented to a director of the bank. Covert access to keys

(as opposed to plaintext) was explicitly ruled out, and yet the agencies seem to be trying to circumvent the will of Parliament on this issue. The most recent version of ETSI DTR 101 567, v 0.1.0 at http://t.co/aMKMsd0X, makes clear that the CSP will be expected to make available in cleartext and service, including 'identity management'; banks and telcos are working on new payment / identity management services based on the next generation of SIM cards. (As for the technical details, wiretap targets who use encryption are currently subject to middleperson attacks using man-in-the-middle (MITM) kit from vendors like Cyberoam and fake certificates. This is dynamically triggered when someone on the target list tries to establish an SSL/TLS session. As a result, the latency is noticeably higher and can be measured by an alert target. The Austrian journalist Erich Moechel has collected relevant documents at http://www.quintessenz.at/harkank/relay/ MIKEY-IBAKE/. In the 'UK perspective' document there, GCHQ worries that a MITM attack in the UK is illegal under the Computer Misuse Act (the police are permitted unauthorised access, but not unauthorised modification) and notes: "Furthermore, the fact that communications are modified en-route by an active attack would render any intercepted data unacceptable for evidential use." In any case, Iran spoiled the party for everyone by doing MITM attacks on such a scale that people now look out for it and the big web service firms have decided to not tolerate it any more; as Jimmy Wales said in the following session, "It is mind-boggling to conceive of even thinking that this is rational policy". So the UK is pushing for the adoption of a key management standard for 3g called MIKEY-SAKKE, which is also not rational policy as its adoption would immediately reopen the 1990s debates about key escrow.)

As for access overseas, in my testimony I pointed out that the FBI can get communications data of UK residents that is stored on servers in the USA via a National Security Letter. This is not the only available mechanism. US law enables its intelligence and law-enforcement community to get access to data on non-US persons via even simpler mechanisms. An intelligence agency can get an order from the FISA court under Section 215 of the Patriot Act. This is discussed by James Baker in testimony before the US Senate at http://www.fas.org/irp/congress/2008_hr/042308baker.html. Several Senators who sit on the Senate intelligence committee have gone on record to say that the government has embraced a secret interpretation of Section 215 that would alarm the public if they knew about it; see "Democratic Senators Issue Strong Warning About Use of the Patriot Act", New York Times, March 16, 2012; at http://www.nytimes.com/2012/03/16/us/politics/ democratic-senators-warn-about-use-of-patriot-act.html. (I amgrateful to Chris Soghoian for sending these links.)

Furthermore, as foreigners located outside US territory are not in general protected by the safeguards provided for 'US persons', surveillance can be authorized for reasons having nothing to do with criminality (e.g. in pursuit of US State or Commerce Department policies). This may be of concern to City firms who often face much more severe regulatory action from US authorities than from UK regulators, even for activities taking place on UK soil.

I mentioned our report on the costs of cybercrime, which was compiled following a request from the then CSA at theMoD SirMarkWelland. This is online with commentary at http://www.lightbluetouchpaper. org/2012/06/18/debunking-cybercrime-myths/. Finally, our letter to the Interception Commissioner questioning the arithmetic in his latest report is now online at http://www.openrightsgroup.org/blog/2012/privacy-coalition-write-tointerception- of-communications-commissioner.

Thank you once more for the opportunity to testify before your committee, and do let me know if I can assist your inquiry in any other way.

Index on Censorship

1. Introduction
The Communications Data Bill as currently drafted would directly undermine both the right to privacy and the right to freedom of expression by making surveillance and storage of UK citizens' communications data the norm. These rights are enshrined in Articles 8 and 10 of the Human Rights Act 1998 and in the European Convention on Human Rights and in the Universal Declaration of Human Rights. The UNDR explicitly states that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence".

Collection and filtering of communications data across the whole British population would not only represent an unacceptable breach of privacy but would also undermine freedom of expression. Index on Censorship – as one of the world's leading freedom of expression organisations – has monitored censorship and surveillance around the world for forty years. The goals of widespread monitoring, information-collection and storage, and surveillance of a whole population are aims that are normally found only in authoritarian and totalitarian states, such as Iran and China, not in democracies who are bound, through their accession to the human rights conventions mentioned above, and through their commitments to democracy and freedom, only to limit free expression where it is necessary on clear grounds of national security and public order and to impose any limits in a proportionate and limited manner.

Population-wide collection and filtering of communications data is neither necessary nor proportionate. Monitoring and surveillance of this kind impacts directly and in a chilling manner on freedom of expression, inhibiting and restricting individuals in how they receive, share and impart information and encouraging self-censorship. No other democracy has gone as far as the government proposes in this bill that the UK should go. As well as representing a major undermining of privacy and freedom of expression in the UK, this bill, if it became law, would be a direct encouragement and justification for authoritarian regimes to monitor in detail their entire populations online as well as off. It would make it difficult, if not impossible, for the UK to challenge these regimes on their censorship and surveillance of their populations. It is also remarkable that, in a memorandum attached to the draft bill on the compatibility of the bill with the European Convention on Human Rights, the government sees fit to focus only on the right to privacy and makes no mention of the potentially chilling and damaging impacts of the bill on freedom of expression.

The declared purpose of this bill is to tackle crime and to ensure national security. This type of in-depth monitoring of the entire population has at no point before been used or introduced as an appropriate crime-prevention or security-promoting tool in the UK. It would represent a reversal of the presumption of innocence and an unwarranted intrusion into the privacy of the British population.

Furthermore, the fact that new technology makes such population-wide data collection, filtering and monitoring possible is not a justification for using the technology in that manner. Such data collection would represent a major step-change in the amount of information available on individual citizens and is not, as has been claimed, simply a step to ensure information already available offline is also available from online sources. The distinction between 'subscriber', 'use' and 'traffic' data and data content is also a misleading one. The range of data that would be collected as 'communications data' would enable a detailed picture of individual's habits, activities, interests, and opinions to be built up going well beyond any population-wide accumulation of data that has happened until now in the UK.

2. Rights of the individual
Reversing the presumption of innocence: The bill proposes the storage of vast swathes of data, to be used by authorities as and when relevant. This is justified by the suggestion, for example, that police investigating crimes will need to be able to access communications sent by criminals when investigating crimes retrospectively. However, in its population-wide scope, it carries an alarming undercurrent, enshrining the assumption that because some of us may be criminals, all should be treated as criminals. This is a reversal of the presumption of innocence and is at odds with British ideas on democracy, pitting as it does the state against the citizen.

Undermining rights: Privacy has long been considered an essential element of the right to freedom of expression. It is self-evident that monitoring of speech or written communication is liable to chill free expression. This bill is not consistent with the UK's commitment to human rights, including the fundamental rights to privacy and to freedom of expression. This bill would rather establish the type of relationship between governments and individuals that Index on Censorship has witnessed in its work defending free expression for dissidents from the dark days of the Soviet bloc to our work today in countries such as Azerbaijan and Belarus.

The mass retention of individual data through the Data Retention Directive has been found to be unconstitutional by courts in Germany, Romania and the Czech Republic, and non-compliant with Article 8 of the ECHR. As the Czech Supreme Court found:

> "One of the ECHR's basic requirements, developed by an interpretation of the condition of the legal basis for government interference with private life, is the predictability and availability of such a legal basis. The reason for this is the legitimate and logical requirement for individuals to be acquainted in advance with the circumstances in which the State may, exceptionally, interfere with their private lives, so that they can adjust their behaviour in order to avoid such interference. The blanket nature of the retention of traffic and location data, however, limits, and even excludes, such a possibility."

The court noted that obligation to retain traffic and location data constituted a "serious breach of privacy" as it would "virtually exclude the existence of uncontrolled and unmonitored telecommunications" while the data could be used to determine the "opinions, health status or sexual orientation of a person". This draft bill goes beyond the already too wide powers in the Data Retention Directive and in RIPA.

This widespread data capture also goes against the spirit of UK national security legislation to date. In 1963, Lord Denning stated:

> "…the Security Services …are to be used for one purpose and one purpose only, the defence of the Realm.
> Most people in this country would, I am sure wholeheartedly support this principle for it would be intolerable to us to have anything in the nature of a Gestapo or Secret Police to snoop into all that we do…even at the behest of a Minister or a Government department…[541]"

Undermining anonymity and whistle-blowing: Anonymity is also a key component of individual freedom of expression – as necessary in democracies as in authoritarian states – and an inability to express views or share information anonymously can chill free expression and even put individuals at risk of harm. These points also apply to whistle-blowers speaking out on matters of public interest. The law as it stands is not sufficient to protect whistle-blowers, the public interest defence in the Official Secrets Act was removed in 1989; there is no public interest defence in RIPA nor the Computer Misuse Act. Those speaking out to prevent crime, or malfeasance in public office, need to be protected. The draft bill will make it difficult for journalists to encourage whistle-blowers to speak out – especially about the activities of state agencies – as these agencies will be able to build a picture of the behaviour of the journalist using their phone records, email traffic, and location using mobile phone base-station triangulation or GPS. The chill on freedom of expression would be significant.

Exposing individuals to harm: Another concern is the possibility that data collected under the draft Bill could be passed over to states which breach international human rights standards. A similar recent example of this happening was the handing over of sensitive information by the Polish and Lithuanian authorities which led to the prosecution of human rights defender (and Nobel prize nominee) Ales Bialiatski who now languishes in a Belarusian jail. The state may also decide for politically expediency, or in the case of an emergency, to suspend

---

[541] Hugo Young and Cathy Massiter, 20/20 Vision: "MI5's Official Secrets" (C4 1985)

or ignore its human rights obligations. In this instance, it is not inconceivable to imagine data captured by universal collection to be handed over to governments that do not respect universal human rights.

Even if the government and public authorities with access to the data collected handle it in a secure manner, the data will be at risk of being stolen, sold, deliberately hacked into not least by authoritarian governments, and/or demanded by other governments as part of their law-enforcement activities. If the provisions of the bill for collecting data on non-UK residents goes ahead, this will also open up the strong likelihood of agencies in other countries demanding access to that data in particular.

There are no balancing legislative actions that could take away the deep undermining of the rights to privacy and free expression that the draft bill implies. Nor are there any serious methods whereby individuals can seek redress against inappropriate accessing of their individual data.

3. Technology

The government claims that new legislation is needed to keep up with technological developments but the range of data and the detailed picture of individuals' views, habits, and activities that can be built up from it goes well beyond existing practices. In fact, the new and extensive detail the technology can provide precisely represents a major new problem which enables and encourages proposals such as those in this bill with their intrusive ability to undermine privacy and free expression. As Index on Censorship has pointed out, mobile phone technology can now pinpoint a person's location to within 2.5m, and large amounts of our personal and private correspondence, communications and information-gathering and sharing now take place online. Though the government insists it is only monitoring data traffic and not content, it is very easy to build up a picture of someone's life with this data. It should be incumbent on the government, in the face of the intrusive powers of these new technologies and applications, to actively support people's privacy in their communications and to ensure their right to free expression, rather than hasten their erosion.

The current bill reflects an elision of ease with necessity: we see, in the government's proposals, the ease with which comprehensive data can be retained being translated, falsely, into an imperative. A similar impulse lay behind the prime minister's frankly dangerous suggestion that social networks could be shut down during the riots of 2011. These issues are not technological, but ethical and political. They are about human rights and about the essence of our democracy.

4. Reach

There are two further issues of deep concern about the reach of the bill, in addition to the intent to capture data on the entire population. Firstly, the definition of data is very broad indeed, and secondly, there is a lack of clarity on which "authorities" are allowed to access filtered data. On the issue of "data" the bill defines this as any communication via any communication network, including postal services. As explained above, the enormous range of activities that communications data now reflect, means even data traffic details rather than data content allows an in-depth picture to be built up of individuals in a deeply intrusive way. The bill as it stands also does not identify exactly who among "public authorities" will be able to access filtered data. The filtered data proposed by the bill is also problematic, leaving the door open for the collection of vast amounts of arbitrary data, 'fishing for data', and failing to address the crossover between data and content. The suggestion that HMRC may be one of the core authorities able to access data also suggests a remit that will rapidly go well beyond any limited, proportionate activities that may be necessary for focused criminal or security investigations.

The government should limit and strictly define what kind of data is accessible, for what purpose, and to whom. Such limited data should only be collected on a small proportion of the population not on the entire population.

5. Democratic oversight

There is currently no judicial oversight proposed for the processes sanctioned in the bill. It is vital that there is not unlimited access by authorities who are on designated access lists. Given the intrusive nature of the data collected, the process must be subject to judicial oversight in all cases for all authorities.

It is of deep concern that the bill concentrates immense and ill-defined powers in the hands of the Home Secretary. As the bill is currently written, the Home Secretary could enormously and rapidly extend the reach of the bill, without either consultation or transparency. The Home Office's memorandum on delegated powers states:

"The clause 1 power is required in order to provide the flexibility necessary to ensure the availability of communications data against the backdrop of a continuously evolving communications environment. Communications services are volatile and change rapidly in response to commercial drivers and other technological innovations. Services are increasingly delivered by a variety of commercial and technical relationships which means that communications data is fragmented and dispersed amongst numerous companies. No single solution or implementation strategy will therefore be capable of responding to all future technological developments or market innovations, or of satisfying the range of operational requirements of the law enforcement and intelligence agencies and other public authorities. Any sustainable solution will need to be capable of accommodating a range of different implementation models over time in order to ensure the availability of communications data."

It is unacceptable to instil such flexibility into a law which is about garnering private information from people's everyday lives. The potential for mission creep or plain abuse of this power is all too evident. Even as the bill stands now, the Home Secretary would have the power to issue orders to CSPs in secret.

Appropriate democratic oversight means transparency not secrecy must be enshrined in any such bill. Furthermore, any adjustment in the intent or scope of the powers granted the Home Secretary in this bill must be subject to democratic parliamentary scrutiny and oversight.

6. Setting a precedent

As our lives are ever more reliant on digital network communication, it has become easier and easier to store data and carry out surveillance. The UK must be conscious of the international example it sets as a democratic country. Enabling this bill, giving enormous snooping powers to government without judicial and parliamentary oversight, would undermine the UK's ability to criticise less- or un-democratic regimes. It would embolden those regimes and be used as justification in their own surveillance and censorship of their citizens. Bad regulations are often copied, the UK's Regulation of Investigatory Powers Act (RIPA) 2000 which has led to over 3 million authorisations was similar to Russia's controversial SORM legislation of the same year. In current international debates about internet governance, we also see authoritarian states at the forefront of demands for top-down regulation of the internet – that their motivations are driven by control and censorship is clear. The decisions the UK Parliament takes on this bill will impact on human rights both in the UK and beyond, not least in authoritarian states.

August 2012

Simon Adlem

I write with reference to the government's proposed Communications Data Bill.

Firstly, a little about my background. I am a freelance computer professional specialising in IT Architecture and IT Security. Over the last fifteen years I have worked on systems and designs for many public and private sector clients including the Home Office, the MoJ the MoD, BAA, BT and Cable & Wireless. I have also been involved in the forensic analysis of data from computer systems.

I have serious concerns about the governments plans and it's impact on the individual's freedoms and human rights. I also have concern about the efficacy of this method of gathering information and the potential for misuse of the data gathered, both legally and illegally.

People today have an intimate relationship with the Internet, in many cases more intimate than relationships they have with other individuals.
For many the Internet is their first port of call if they have a concern, for example, about a medical or personal problem. The internet is used to communicate with like minded individuals, to access subject matter of interest, even to persue someone's deepest, most private desires. An individual's Internet usage therefore reflects their entire life, even the most private of things like sexual preferences and other private interests. Collecting data on Internet usage therefore has the ability to expose an individuals private life in it's entirety.

I believe data such as this should be private, safeguarded by the basic human right to privacy that should be offered to every human being. It is accepted that in society the Government, the Police and the Security Services sometimes need to delve deeply into someone's life for reasons of crime prevention and national security. However, this intrusion must be justified. Currently, the law provides this safeguard with the requirement for a warrant to be obtained before this type of data can be collected. In my view it is incredibly important that this safeguard to our individual privacy is retained.

There is also a major security issue in collecting and retaining this information. A leak of this information from an ISP could easily happen.
This could potentially put individuals, particularly those in the public eye, in a situation where they could be blackmailed, threatened, compromised or harmed. For ISPs to handle this sort of information, there is also a wider issue here; should ISP staff be subject to Security Clearance if they have the potential to access this sort of sensitive information? Would it be appropriate for this information to be officially classified as Confidential, Restricted, Secret or above?

Information that could be collected under the Communications Data Bill will not be effective in fighting terrorism and organised crime as has been stated by the government. I can think of many ways that an individual could circumvent these measures. For an organised group the possibilities to avoid detection are even greater. Instead, the data generated will only really be useful for monitoring and profiling the innocent. Fear of being caught for doing something that is completely innocent could do the greatest harm, with individuals, particularly young people, afraid of seeking information for fear of being criminalised for it. Profiling in particular is also a major concern as it effectively criminalises individuals or singles them out for special attention based on probability. It is incredibly important to remember that an individual is not a criminal unless they have actually broken the law. It should also be noted that it would be easy for criminal groups to resort to more traditional techniques of communication, thus circumventing this proposed legislation entirely.

- From a technical perspective, the technical implementation of this Bill runs the risk of harming the internet experience for many, causing slowdown, breakages and difficulty in accessing sites, at least in the beginning. The heavy technical requirements in terms of skill and investment favours the very large ISPs and penalises smaller companies.

Some websites do not function correctly when used via an internet proxy and some ISPs may not be able or willing to make the investment in infrastructure required to provide a performant web proxy solution. I worked on one of the UKs larger proxy deployments for the MoD and I can assure you that the hardware and skill requirements to provide this type of service are significant. Someone has to pay for this and this will always be the public, either by increased internet costs, taxation or both.

This bill also preys on the public's lack of understanding of the technical issues surrounding this issue. Whilst saying these measures will enable the Police and Security Services to catch more terrorists, criminals and paedophiles is very emotive, in the real world I do not expect a statistically significant increase in apprehension rates as a direct result of this legislation. I therefore find it difficult to accept the investment required as there is no real benefit to be gained from it. I also find it impossible to justify this gross breach of individual rights for so little gain. To me this Bill is little more than policing by numbers; monitor enough people and eventually you'll find a criminal. This is not by any intelligent process but pure statistics.

I would therefore urge you to consider opposing the proposed Communications Data Bill in its entirety.

Rodney Aistrop

I urge you to consider the possibility that the best form of government is minimum government.

In the opinion of the writer, the best form of government is that which allows the individual the most freedom consistent with a stable and creative society. We have been more free in our past than we are at present.. The freedoms for which our society has been famous are being eroded at an unacceptable rate such that we are now amongst the least free nations in Europe .

In around1974, Home Secretary Roy Jenkins introduced the Prevention of Terrorism (Temporary Provisions) Act. Note the "temporary" in the title. To the best of my knowledge it has been renewed every year since. The European Court of Human Rights ruled the Prevention of Terrorism Act to be in violation of Article Five, Section Three of the European Convention on Human Rights, which requires suspects to be "promptly" brought before a judge. Being brought promptly before a judge used to be a peculiarly British form of Civil Liberty. Nevertheless, the British government refuses to abandon its preventive detention policy and evades the European Court's ruling by invoking Article 15's provision for countries to ignore the Convention on Human Rights "in time of war or other emergency threatening the life of the nation." The exercise of the not inconsiderable power assumed by the government under the Prevention of Terrorism Act has resulted in a number of miscarriages of justice and embarrassment to the UK in the International arena.

In 1988, the Thatcher government enacted additional laws restricting civil liberties. Television stations were forbidden to broadcast in-person statements by supporters of a legally recognised political party with democratically elected members of parliament (Stormont) ie. Sinn Fein. In my opinion this was abuse of the powers vested in Mrs Thatcher by UK voters. She deprived the voters of the Sinn Fein MPs of a public voice to which all other like electorates were entitled . I believe this action to be undemocratic. I am not Irish nor do I support the Sinn Fein cause. We are supposed to live in a democracy not a democracy that was constrained for the convenience of the Prime Minister and her government.

These are by no means the only instances of the Statutory removal of civil liberties in the UK.

The Draft Communications Data Bill is the next link in this chain to reduce civil liberties. It assumes potential wrong doing by every individual in the nation. The government has the right, under this bill, to monitor all data communications. It may choose not to monitor all data communications but Government is taking the power to monitor all. This sweeping power to monitor all individuals is unnecessary. Existing laws allow the government to ensure the security and safety of the UK but use of the existing statutes require more public scrutiny of government actions and protect the public better by providing checks and balances on government action than does the proposed Act..

This proposed Act is not in tune with the legal freedoms enjoyed by the persons of this country in the past like innocence until proven guilty in a court of Law and Trial by Jury. The freedoms enjoyed by individuals in the UK are predicated on there being checks and balances on the power exercised by the state. "Power corrupts and absolute power corrupts absolutely, (Lord Acton)". Experience shows that power which is available will be used and it will not necessarily be used in the way legislators intended and the chances are, sooner or later it will be used corruptly. The sweeping powers awarded to the government by the government will be used as has been demonstrated in the past by persons representing government or government associated organisations to monitor law abiding individuals for reasons not envisaged by legislators. This is corrupt use of the law A government with no checks and balances on its power ultimately will grow to consume the State which it aspires t o govern.

As an individual, if the state assumes I am a potential wrong doer, I interpret this as being a reduction in the need of the individual to behave in a socially responsible way as was the case previously by individual choice and practice. If the state chooses to take responsibility for controlling behaviour of all individuals, then I have less personal responsibility for behaving properly.

I aspire not to be a citizen of this country by the time civil liberties are eroded by much more and I hope to be long gone when the the government finally consumes the State.

Martin Ammann

I have written an email to my local MP and he replied in favour of the legislation with much the same arguments that the government does. I here attempt to dismantle them for your benefit. MP Vickers' replies are set in quotation marks, my thoughts come behind the arrow:

"I am told that with the pace of technological change, our future capability is very uncertain. That is why, in the Government's Strategic Defence and Security Review, it said it would "introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to obtain data and to intercept communications within the appropriate legal framework."

-> The problem is exactly what this legal framework will look like and what will make it 'appropriate'. In order to enable investigators to catch all forms of terrorist groups, terminology necessarily has to be kept vague and will thus constitute a danger to the civil liberties of everyone.

"It also made it clear that in seeking to ensure our law enforcement agencies continue to retain capabilities to protect us from harm, civil liberties would be respected and protected."

-> That is a noble statement but the new legislation cannot assume that these new powers will not be abused. Abuse of power that the government has invested so-called public servants with is well documented, be it police, magistrates or even MPs.

"The Government therefore proposes to require internet companies to collect and store certain additional information, like who an individual has contacted and when, which they may not collect at present. The information will show the context, but not the content, of communications."

-> So this information is collected on everyone using the internet in the UK, making everyone a potential terrorist. Also, this is a stepping stone legislation. While content monitoring is not yet included in this bill, it makes it easier to be included in a later one.

"So we will simply have for internet-based communications what we already have for mobile and landline telephone calls. The data will be available only to designated senior officers, on a case-by-case basis, authorised under the Regulation of Investigatory Powers Act, and the process will be overseen by the Interception of Communications Commissioner.

-> Again, who watches the watchmen?

"It will be available only if it is necessary and proportionate to a criminal investigation."

-> Once more, 'necessary' and 'proportionate' as well as 'national security' are deliberately vague terms that leave decisions in the hands of individuals, not the law.

"No increase in the amount of interception is envisaged as a result of this."

-> This is a rather naïve assumption. If an institution has been given powers, it is likely to use them.

I can only conclude that the new communications data bill is an unacceptable risk to civil liberties and the freedom of us all in the long run.

Richard Ash

I am writing to you to ask you to ensure that your Committee's report deals with the significant privacy implications of the above bill. As an electronic engineer dealing with communications systems in the course of my work, it is clear to me that a technical, bureaucratic, system of always-on surveillance is unlikely to succeed in it's stated aim (of protecting the population).

However the technical issues are not the ones that I wish to raise with you today. This bill proposes that an attempt should be made to record the electronic communications made by everyone in the United Kingdom, all the time, just in case the state happens to need them in future. This basic design, based upon universal surveillance, is both a fundamental departure from previous powers, and a massive intrusion into the privacy of individuals by the state.

It is right that law enforcement and public protection agencies should have the right to undertake surveillance, at whatever level of detail and intrusiveness is required, where there are suspicions of a specific individual or group. This process is managed by the courts, and appears to work well. Separate debates, like the admissibility of wire-tap evidence, need to be had in their place. It is ironic that at the same time that this bill is proposed, the implementation of smart meters by DECC means that operationally useful data will be denied to electricity network operators on the grounds that electricity usage patterns are covered by the Data Protection act.

However the measures proposed by both the previous government and this one are neither proportionate nor fit for purpose. Enormous amounts of information, much if it which would not otherwise be collected, will be gathered and stored by a variety of private companies. There is no assurance that the companies doing the collection will be ones the consumer has entered into a contract with (e.g. a mobile phone contract from a virtual network operator), so they have no control over the security with which this data will be held, or the commercial uses to which the companies (having been forced to collect it) may put the information.

I do not consider myself to have anything to hide, but that does not mean I wish to pay (either as a taxpayer or a service user) to have my usage collected, stored, scrutinised by any agency of government (not just the security services) and potentially lost in yet another electronic security breach. Needless to say, the perpetrators of the breach will not be stupid enough to get caught by these measures!

Please make the case of rejection of these measures clearly and strongly on the grounds of the privacy of the individual, as well as the technical detail of the proposals.

Daniel Beckett

General:
1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

Yes, they have.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

No, they haven't.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

They 'fit' in the landscape in that they are a gross invasion of privacy that should not be allowed to take place in this nation nor anywhere else.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

That it shouldn't be done.

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

Yes: Don't.

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

It would be preferable to have neither.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

No, there is no compromise with this sort of invasion at all.

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

Yes. Negative.

Costs:
9. Is the estimated cost of £1.8bn over 10 years realistic?

No.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?

Given that this bill is supposedly intended to catch criminals and apparent terrorists, the entire notion of a financial benefit is not only unrealistic, it is impossible.

Scope:
11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

They sensibly *define* the scope of the powers, but they don't make the powers themselves sensible.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

None. And no because there shouldn't be anyone allowed to view them in the first place.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

They should not only be pursued, but if they prove consistent in their breach of duty, they should be barred from doing business within the UK.

Use of Communications Data:
14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?

This kind of communications data shouldn't be used at all.

15. Is the proposed 12 month period for the retention of data too long or too short?

On the contrary, it's far too long. Personally, I recommend a maximum retention period of about 12 microseconds.

Safeguards:
16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

The only entity that could possibly be able to be held responsible over such data and power would constantly have to remain totally altruistic and incapable of coercion or corruption, and as politics has proven time and again, no such human exists outside the realms of fiction and fantasy.

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

If this horrendous bill were to pass, then yes, a warrant would be needed in *every* case.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?

No.

Parliamentary Oversight:
19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

No.

Enforcement:
20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

No. A company that respects its users right to privacy is something to be commended.

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

Could this scope of violation include those who wish to impose such Orwellian laws on us in the first place (such as our current Home Secretary)? If so, then yes on both counts.

Technical:
22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

No. No such safety exists nor will it ever exist. Such is the nature of the internet.

23. How safely can communications data be stored?

It is impossible to keep data completely secure, so finitely.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

No, definitely not, and absolutely not.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?

Tremendously. Even those with a rudimentary knowledge of security in communication could evade this, and any attempts to catch those who evade them will only ever result in further evasion.

26. Are there concerns about the consequences of decryption?

Yes, of course there are.

On another note, despite the sarcasm in this email, my beliefs sincerely are that this bill should not be allowed to pass. This bill would put us only slightly below China in terms of scrutiny of its peoples, and is no different to some ridiculous scheme to tap and monitor Phone communications. If the Government truly respects its people's privacy, then they should throw this draconian bill straight out.

Finally, and on a related note, our current Home Secretary should cancel the frankly stupid decision to extradite Gary Buchanan. The young man has done nothing that warrants an extradition. If any crime was committed (which there wasn't), then it would have been committed on British soil, and should be tried here. The notion of extraditing someone because it is a crime somewhere else is absolutely laughable. If this is a proper course of action, then shouldn't we be extraditing all homosexuals to countries that deem it illegal, or all voting women to countries where that is illegal?

Robert M K Brereton

Given the level of government incompetence when doing anything IT related I find it very disturbing and worrying that you are proposing yet another new layer of surveillance to be imposed on the British public. We are already the most watched nation in the world, even more than totalitarian regimes, with all the CCTV, Speed cameras, police ANPR machines etc.

I suppose you are subscribing to the theory that by keeping us in a state of alarm you will be able to control us. We British will put up with a lot, but the day is fast approaching when the public will say 'enough is enough'.

We survived all the IRA scares in the 60's by being vigilant and taking precautions, in my case by checking under the car each day and varying my route to the TA centre. The IRA was a far more determined enemy than this lot, and did cause a lot of explosions and murders.

The only ones who will feel the inconvenience will, as usual, be the law abiding, who maybe inadvertently accesses a website with some questionable material on it. The criminals and terrorists have better IT skills and will easily circumvent any attempt at surveillance.

I think the term 'snoopers charter' is the correct one especially if the little Hitlers in local authorities are given access also.

Great Britain is now not recognisable as the nation I knew growing up and would have fought for with all my might to defend and I truly hate what it has become. I am fast becoming a 'former patriot'.

National Crime Agency

I am writing to respond to the Joint Committee on the draft Communications Data Bill's call for written evidence. While the creation of the National Crime Agency is yet to be approved by Parliament through the Crime and Courts Bill and you are receiving detailed evidence from the organisations which may transition to the Agency, I write to stress the vital operational importance of a cutting edge communications data capability for the future success of the fight against serious, organised and complex crime.

The Plan for the NCA sets out that the Agency would aim to secure a step change in our ability to protect the public from serious, organised and complex crime, and to build upon and transform the existing capabilities of the Serious Organised Crime Agency (SOCA), the Child Exploitation and Online Protection Centre (CEOP) and others. lt is intended to operate as an intelligence-led law enforcement agency, providing operational leadership and coordination across law enforcement throughout the UK to cut crime and protect the public. New communications data legislation would enable the NCA to maintain SOCA's and CEOP's current intelligence capabilities: without it, the Agency's proposed operational capabilities would be seriously degraded.

Use of communications data is a critical operational tool in tackling crime and saving life, and its continued availability as technology rapidly changes would be vital to the success of the NCA. lt forms an important element in 95% of all serious organised crime investigations. lt enables proactive operations to identify and trace criminals, intervene in their activities, arrest and prosecute them, seize their assets and prevent harm to victims of crime.

lt is also key to managing risk; not only are kidnap operations, for example, hugely dependent on communications data, with a direct correlation between this capability and saving lives, but it is vital in the protection of children, through tackling paedophiles and their networks, who are early and sophisticated users of new technologies as CEOP is finding.

Equally important is that access to and use of communications data are subject to strict controls. By adopting the robust safeguards in place in SOCA and CEOP and through the provisions in the Crime and Courts Bill, NCA officers would only access communications data in accordance with the principles of necessity and proportionality set out in law.

Drawing on my own experience fighting crime, during which communications data were indispensible, I have no doubt as to the necessity of the provisions laid out in the draft Communications Data Bill. As criminals move to internet-based communications, our capabilities must keep pace. The provisions therefore meet an urgent requirement to help prevent the degradation in our ability to acquire communications data.

Yours sincerely

Keith Bristow QPM
Director General

Jonathan Birkitt

The Home Office is has made it clear that their intention for this bill is to extend their powers which they currently possess to store phone and text message data to the internet. The thinking behind the bill makes sense, as those who want to commit crimes will be smart enough to not use the phone and text messaging services to avoid getting caught. The moment this bill takes effect and peoples internet usage starts getting monitored the same criminals will move on to something which the bill does not cover. To avoid my messages being tracked I would just go use an open chat site from a internet cafe, solved you can't read my messages. There are always ways of getting around the internet provider and smart criminals will do this, or start using new forms of encrypted messaging which is not covered by this bill. All that will happen is the government will keep extending this bill further and further violating every aspect of internet privacy a person should be able to enjoy.

You like any other expect to be able to have a cup of coffee in a restaurant with a friend, without someone there timing you with a stop watch, take note of who the person you are talking to and when. But your taking the British peoples right to sit online and have their cups of coffee with non-local friends and family who may even be abroad. Being a person stuck on the internet everyday you would not be far off knowing every single friend of mine not only through use of Facebook but all my communication channels I use. I would love to be able to keep my friends personal and that is not going to happen if this bill gets through. The government is looking into how customers should be able to access what data the companies own about the individual, and I think Europe is talking about giving them the power to request their data to be deleted. On one hand the government is looking to empower people about being able to reduce data stored about their habits by telling companies to open up, but on the other hand the government wants to do it themselves.

Phones and the Internet are on two different levels; on phones people mainly just talk or do a little business. On the internet people shop, enjoy videos and communicate. With the UK's horrific record on data security, it is likely to leak that two Tory, three Lib-Dem's and six Labour MPs had been on X amount of indecent sites which will create another MP scandal. Though you say data will be protected but it wont really, look at the USA they thought their data was safe but, millions of files ended up on Wikileaks. Why? because all it takes is one person to disobey the law, to ruin a reputation or life of another. The bill will store a database about the whole country, just takes anonymous to hack the databases and we have the whole of the UK's internet usage online. The UK is already like Big Brother on Channel 4, with 1/4 of the worlds security cameras, we do not need more invasion of our privacy. This country is far from a liberal society and the thought of introducing this bill just supports this.

Having two pieces of legislation connecting is often flawed, as there are increased chances of a legal loopholes which can be exploited by lawyers in court. These loopholes may be used by individual authorities to access data, so despite completely opposing the bill I would prefer I solid piece of legislation instead of two. You ask about being less attractive base for communication providers, you thinking too small. The UK will become less attractive for all businesses, state monitoring puts off anyone and those thinking of setting up shop will want to be in a liberal society where they know they are free and not being monitored. The UK is just putting up a big sign "Beware we spy on your every move."

It says that it will cost £180m a year, so the public will be paying to lose their right to privacy. And not only this the UK government has a horrific track record for delivering such projects on budget and on schedule, we will probably end up paying nearer £3bn making this an absolute waste of money even if the so called value of this is up to £5-6 billion. It does not state how this is going to be saved, but national security could boosted in far better ways for £1.8bn than using a method that takes our liberties away.

Which authorities, if any? MI5, MI6 and the police. All other authorities including local do not need these. The secretary of state should not have the ability to change these unless under an act of parliament the list will end up twice the size as it started. Overseas providers will be operating under the home countries laws and I would assume they would ignore this new bill, making them more attractive. This will draw customers from the UK over to their providers damaging British taxpaying firms (whose taxes will also be paying for the bill) leading to

less takes and possibly tax losses. It is too risk on too many levels this bill and it really needs to be dropped in the "national interest."

Only a few crimes would deserve access to such data, including murder, large scale fraud, smuggling, hacking and possibly tax evasion. The majority of other crimes are not on a scale that deserves them to lose their liberties to privacy. A person can create a lot of data over the period of 12 months, making this period excessive. The crime agencies need no longer than 3 months and can have 6 months on a judge accepted extension. Whatever the ruling is it needs to be written that it cannot be extended any further in the future, as the governments of the UK love extending periods for police purposes. A judge should not only be used for extensions buy granting access through a warrant to peoples data. Having a judge will reduce risk of misuse of the data being collected and that this is only used for the most serious of cases which I have mentioned above. Yes this is likely to increase cost of the project, but by reducing the data storage period money can be saved on data storage costs.

Though the extra cost will be limited as again this should be only used for the most serious crimes meaning that the data requests would be limited.

I am no expert on technology, but from my experience nothing is bullet proof and if someone really wants access they will find someone to give it them. Remember the British man who was to be extradited to the US for hacking the pentagon? I am sure he would be able to hack the systems and decrypt anything. This means data is never full safe and is it worth the gamble to collect the countries communication for it to be hacked and put online (like I mentioned before), I serious disagree.

Roger H Cook

1. I do NOT believe the Government has made a convincing case for the need for the new powers proposed in the draft Bill. Further I am extremely concerned by the possibilities that this bill represents.
2. I understand fully HM Government's desire to protect the public interest, but we do live in a democracy, and greater importance has to be attached to personal liberties and freedom.
3. This Bill would allow for invasion of ordinary people's lives, and consequent loss of freedom. It would allow innocent people to be spied upon, thus automatically treating everyone as though they were suspected of some crime.
4. It is appropriate to make comparisons with historical precedents, and the obvious ones are the loss of freedoms in the totalitarian states that have bedevilled world history – e.g. Nazi Germany, Soviet Russia, and Communist China.
5. We have literally fought long and hard in this country for the freedoms we have, and I suggest that this bill should be summarily rejected at the outset.

Mr. P. Cromie

I am writing to express my objection to the draft Communications Data Bill. I feel that the intent of the bill represents an unprecedented invasion of privacy and is a price too great to pay for the marginal benefits it might bring.

I find the amount and breadth of data to be collected disturbing and worrying. If Royal Mail were asked to record every letter sent, would that be acceptable? Of course not. Would it be acceptable that the police had keys to every house in the country, just in case? Of course not. I believe that the standards that apply elsewhere in life should apply to electronic communications too.

I also do not believe that access without a warrant is a good idea. The data will be ripe for abuse.

Finally, this is the kind of oppressive policy that one might find in a much less libertarian nation, such as China or Libya, where electronic communications were monitored until the government was overthrown.

This is the wrong bill to present in a free society. I urge the Government to re-think.

N. Dove

I would like to register my objection to the Draft Communications Bill.
My key concerns include:

The potential for mis-use of the data by a future government - do we want a future equivalent of the MacCarthy witch hunts of America's 20th Century?
The size of the database will be vast, there will be problems in terms of cost of storage, and ensuring adequate security.

One Wikileaks style data raid, and every website you even as an MP, have ever visited will be available to the public, every e-mail facebook or twitter comment and purchase you have made will become public- the equivalent of a copy of every letter, phone call,your on-line banking,shopping, hobbies, social events with time and date will be there tax details.

People be it security services or others, incuding third party users,will in potential be able to work out what you have done almost every minute of every day, and this is an invasion of privacy that is almost unbelievable in scope. Hitler or Stalin, could never have dreamed of such complete access to the private lives of their citizens. We are supposed to live in a free society, but invasion of privacy on this scale is utterly unacceptable.

Quis custodiat? Who will guard the guardians of this data? The demand for this data comes allegedly, from our security service, who "need" the data to fight crime,terrorism etc., but there is no clear evidence of this need, and existing laws allow access to most of the data already, enhancing the scope is not needed, especially when it overturns the root assumption of the law, which is Innocent until proven guilty. If this law comes into effect, it effectively means the assumption is of guilt, with innocence having to be proved. I remember when it was claimed the 90 days detainment without charge was ESSENTIAL for successful counter terrorist action, but we seem to do pretty well with 28 days.

Even with the introduction of all the measures suggested by this bill, there will still be plenty of ways for criminals and terrorists to work round them. One only has to look at the continuing threat of viruses, trojan horses,and security breaches etc to see that for every step forward by security, there is a least one step forward by hackers etc. in a race that can never be won. If a human mind can create a puzzle, it can also solve it. It is impossible to have absolute security.

The government has claimed that civil servants need "privacy" from freedom of information claims in order to be able to give proper advice to ministers, if that is the case, the public also need "privacy" for similar reasons - how can they be properly able to advise clients friends family etc. if it is open to scrutiny by security services.
It is arguable that the proposals conflict with the Human Rights Act.

Control of my data

I have no control over my data, once it is collected by third parties' on behalf of the government. The government is placing me at risk without my consent. The risks include
1. That police have access to a record of my political beliefs and social habits
2. That these records could be shared with private investigators or journalists
3. That these records could be unlawfully accessed by foreign governments or criminal gangs, and aid further identity fraud, blackmail or account hacking

This runs counter to everything governments including ours are trying to do through promotion of good privacy practice and data protection policies.

Suspicion should be the test for surveillance

The government of course has the right to intercept and record information when someone is suspected of a serious crime. But these proposals mean collection of data without suspicion: which is in effect mass surveillance.

Accessing big data sets opens up new police surveillance powers

Being able to compare location data, contact histories, websites visited and so on will give the police the generalized ability to track any group, from sports fans to political protesters. This will create extreme risks for whistleblowers, journalists' sources and legitimate but inconvenient forms of protest.

This is not "preservation" of capacity but a huge extension of policing powers, which deserves proper democratic debate, starting with a full public consultation.

RIPA needs to be fixed first

Data retention is already excessive and creating risks. The access policies for police are too wide and lack judicial supervision. There is no notification policy for people who been placed under surveillance.

These problems should be fixed before the government suggests new surveillance powers.

We are in a recession

Spending billions of pounds surveilling innocent people while cutting back on policing seems wrongheaded. I would rather money is spent on front line detection work.

Bad examples to foreign governments

There are no democratic governments that force companies to aid surveillance through collection and creation of new data sets. How can the UK seriously stand up for human rights while abusing the privacy of millions of innocent citizens?

Oliver Colville MP

I have read the draft Communications Bill and' would like to raise some of the issues that I have observed as well as those which have been brought to my attention by my Plymouth, Sutton and Devonport constituents.

I must say that I am agreement with the Government that we must do all we can do uphold the civil liberties of the people of Britain and protect against those who wish to harm others.

I understand, however, that where it is deemed necessary to obtain access to the content of communications a warrant is required which must be signed by the Secretary of State. Whilst I am encouraged that a warrant is needed to gather this additional information I would like to see a judge make this final decision to administer a warrant rather than the Home Secretary.

There are also a number of technical issues about the nature of data itself that cause me concern. For example, whilst I understand that it is not the Government's intention to allow access to the content of electronic messages, isolating the content of the retained data from any search may be difficult or impossible.

I also question the process by which the police would be given the ability to self-authorise access to data. I am concerned that this internal approval system allows collaborating police forces to designate 'authorised officers' which would infringe on ideas of transparency.

I am also concerned that the proposals mean that the data that can be accessed has been widened to include 'operators' not only as those providing a postal or telecommunications service but also any person who controls or provides a telecommunication system, essentially incorporating anyone who owns a mobile telephone, radio or television.

I understand that the deadline for contributions has passed but I ask that the points I have raised be taken into account on behalf of my Plymouth, Sutton and Devonport constituents. I have also written to the Home Secretary.

Cliff Fowkes

I would like to express my concerns and ask that you consider them during your deliberations.

It has oft been said by proponents of the bill that "authorities would only see details of the time and place that a message was sent, or which website was visited" as if this somehow makes it "OK". This sort of tracking is more than enough to develop an in depth profile of a citizen's activities, contacts, location (when and where) , personal business and a host of other privacy invasions

Although the content of actual messages (what was said, or written) would not be accessible to the authorities without a warrant, I understand that a judge's permission would not be required for authorities to see details of the time and place that a message was sent, or which website was visited.

It would be far too easy for the system to be abused - agencies might use it to conduct "fishing expeditions" rather than targeted surveillance against specific threats or individuals.
The wealth of data collected could easily be used to build profiles about individuals' browsing habits - which I believe should remain private for the vast majority of ordinary citizens.

It is plausible that the sensitive databases could themselves attract cybercriminals, (no databases are invulnerable to hacking despite assurances) who might attempt to access them with criminal intent of abusing private information or blackmailing individuals.

Furthermore, the really dangerous criminals and terrorists will have ways of avoiding tracking and need a focussed, in depth approach, rather than this "broad brush" approach. The interest of protecting national security could conceivably be degraded by this unfocussed approach and diversion of scarce resources .

Thomas Frampton

I am writing to you to provide my views, a British Citisen and taxpayer, regarding the Draft Communications Data Bill.

This is an issue I feel very strongly about and I believe it is important for the government to listen to the views of its people as it should always address the needs of the people first and foremost.

It is paramount that the government of a free state such as the UK should not have the ability to peer into the private lives of any and all its citisens without good reason and thorough approval sought prior i.e. without a warrant, for each individual case. To allow free access by the government to a citisens emails and internet browsing history decreases the security and safety of a citisen, their personal freedom to privacy and their trust in the government. There are of course cases when this is an exercise which is necessary, such as for national security, but again it should always require a deserved warrant. We got by without such a bill previously in states of national security i.e. the IRA, and the government did not snoop into the post of its citisens without a warrant then, so we should not need to now.

To allow this Bill would put a huge amount of power into the hands of the government where it may obtain sensitive and confidential yet not illegal details which may even end up with third parties. Of course this is something which should not happen, but it is a risk, and not one that I, or likely anybody else would happily take. The cost of this would also come to a huge amount 'estimated cost of £1.8bn over 10 years', which results in a double blow of breaching our freedom to privacy while wasting public money in times of such austerity.

I have briefly highlighted my key concerns regarding the bill; too much additional power for the government, breach of our freedom to privacy and the potential for the information the government obtains to fall into the possession of a third party and be used in a malicious manner.

Y Guinan

The Snoopers Charter undermines our human and democratic rights to privacy and violates the Human Rights Act. That is the bottom line and in a democracy, where personal freedom and rights to privacy are inalienable, the plans would never even have made it to "Draft" form. "Crime-prevention arguments must not unquestionably trump the privacy of law-abiding citizens" (Liberty 2012).

By treating everyone as if they were criminals, by monitoring all electronic communications and building up a databank of all online and telephone activity, the proposed system will turn our society into a nation of suspects: "Guilty until proven innocent". Britain is already the most monitored nation on the globe and this latest plan is just one step short of having mandatory CCTV cameras fitted inside all our homes.

Technology experts say that the only feasible way of completing the task would involve a blanket approach to the information going through internet service providers. This would mean that all online activity is potentially being intercepted by the government and raises serious questions about privacy and motives. Technology firms have also warned that if they are forced to apply the plans, it will be harder for them to turn down similar requests from authoritarian regimes overseas (Whispers of Discontent 2012).

Expert opinion has established that invading people's rights to privacy is not the way to go about apprehending criminals, either on or off line. Ironically, both Liberal Democrats and Conservatives fiercely opposed very similar measures when they were in opposition; indeed, the Conservatives promised that they would reverse the mass surveillance culture if they came into power.

Civil liberties campaigners in parliament, including David Davies Conservative MP and Lib Dem MP Julian Huppert, have started to organise their opposition to the plans. Over 250,000 citizens have already signed online petitions expressing their abhorrence of the Government's plans to invade personal privacy.

The proponents of the Snoopers Charter have presented the need for this legislation as being a necessary evil to protect us against "terrorism and paedophiles".

However, the need to resort to emotional blackmail and scaremongering tactics in order to manipulate people on-side suggests a weak argument. It does not take an expert in computer technology, psychology or criminology to expose this argument as being worryingly naïve and uninformed.

- The Charter will only succeed in driving the tiny minority of actual criminals further underground, making them more difficult to detect and apprehend and thereby placing the safety and security of all us potential victims at even greater risk than we already are. The technologically savvy will always be one step ahead, which may or may not prove fortunate for the rest of us. Any criminal worth catching will already be plotting his evasion and circumvention tactics (some of which may even cause an escalation in crime) – proxy servers, wi-fi cafés, pay-as-you-go (even stolen) sim cards, etc., etc. Experiential evidence in Germany shows that authorities apprehended more criminals only after the stringent surveillance was lifted when resources could be redirected toward actual criminals.

- It is not only those with criminal intent that will be searching for ways to protect their anonymity. Any British citizen who values and respects his or her individual right to privacy will also be investigating ways to protect their sacred space, in exactly the same ways as they already use anti-malware software to protect their personal computers and electronic communications from the omni-threat of internet trolls, phishers, stalkers and the like and fortify their home security with locks and alarms. We continue to retain the right to do so. Innocent victims of this Charter will be forced into an uncompromising corner, compelled to avail themselves of whatever means necessary to keep unwanted intruders at bay. Will these victims then be accused of being criminals for resorting to these security measures?

- It is illegal for anyone to open someone else's land mail. The same rules should apply to all forms of private communication. Although we are being assured that the actual content of our conversations and emails, etc. will not be read (yet), this offers no consolation. Being harassed by a stalker, or arriving home or waking up to a burglar in my bedroom, reassuring me that he wasn't going to nick anything or violate me - that he was "just having a snoop around, honest", simply does not cut the mustard. Learning that I have no right to call 999 is not the sort of "protection" that any citizen should be expected to endure. It is the stuff of nightmares: the classic case of law-enforcer turned perpetrator.

- It is astronomically expensive and the country simply cannot afford it in these "austere times". This Charter will not only cost us our civil liberties but also financially. Start-up costs alone are estimated at over £2 billion. Annual running costs would be at least £200 million a year at the prices estimated in 2009. The taxpayer is simply not willing to pay this price in exchange for their loss of freedom. The real criminals having fled underground, law enforcers will find themselves searching in a very expensive haystack. As employment increases and people are already losing their homes, lives and livelihoods as a result of the spending cuts (and more apparently on the way), this audacious proposal is ludicrous.

- The Snooper's Charter is in itself a threat to our personal and national security. Aside from the risks already mentioned above, indiscriminately stockpiling vast amounts of our personal data places our identities at risk and is open to misuse and manipulation by anybody who assumes or is awarded the power to access them. Successful hacks are already commonplace. Our personal data may even be inadvertently left on a train! The consequence of this information falling into the wrong hands does not bear thinking about. Tory MP Dominic Raab warns, "This is a stark warning. Far from improving our security, these flawed plans to privatise Big Brother surveillance will subject every citizen to intrusive monitoring, and expose us to the risk of massive fraud on an unprecedented scale".

With the facts established, and with all presupposed arguments that promote and condone this intrusion into and violation of our personal rights to privacy and safety, and our democratic rights to freedom of speech rendered thereby obsolete, what now could be the justification for these proposals?

Government threatened by democracy? The internet has given people the power and freedom to avail themselves of and exchange information and to connect with others all around the globe. Online petitions already allow people to act with immediate effect in response to political injustices.

Such an advance in human and technological evolution would clearly be perceived as a threat in recognised despotic countries such as Iran and China. But the Government of a western democracy would surely welcome and celebrate the democrats' desire to become more involved in the making of decisions and policies that affect their lives. The increased opportunity that the internet provides to people to become the Masters of their Own Destiny as extolled by the Big Society manifesto should be welcomed by any Government that values freedom of speech and not perceived as a threat to democracy.

Effective, cost-effective and non-intrusive ways to deal with the threat of terrorism and paedophilia, which do not threaten and undermine the principles of democracy, need to be found.

Nobody would disagree that crime remains a serious issue in our society and needs to be addressed. However, before opening a can of worms and having taken a much-needed reality check, Big Brother could utilise this cooling-off period to return to the drawing board and, armed with all the facts regarding the potential pitfalls and dangerous implications of his latest move to curtail our civil liberties, develop realistic ways to deal with the problems that befit a democratic nation.

He should present revised justification for proceeding with his way of dealing with crime and terrorism, which we all agree is unwelcome in our society (but two wrongs do not make a right). The electorate also requires him to justify the spending of £billions taxpayers' money, especially in times of so-called austerity – on a system that has already been "proven" ineffective. We are apparently in a double-dip recession and £trillions in debt. The

Government should, therefore, instead be focussing on investing in crime prevention methods that include sustainable economic growth, environmental protection and basic welfare for all of its citizens.

A pilot study may be useful. Before spending the astronomical £billions it will cost the taxpayer to plunge the nation even further into debt, the Government might consider a pilot study whereby the public (the Government's employers) gets to scrutinise the Government's private electronic communications. Should that turn out to be a wild goose chase, and the criminals remain Scot-free, then we can all agree to abandon the whole scheme altogether.

This country is renowned for its "innocent until proven guilty" stance on justice. The passage of the Snoopers Charter into the British statute books would turn that precedent on its head. Every single person would be perceived as a criminal. It does not take a scholar in the fields of the studies of the human psyche to know that, if you hold a weak-minded person in a certain perception/expectation for long enough, they are compelled to fit that bill. This Charter is just asking for people to literally fit the Bill and become the very criminals it is purporting to want to catch.

"If people haven't broken the law then they haven't committed a criminal act" (Ken Clarke, Question Time 22nd June 2012).

Spreading the seeds of distrust, paranoia and discontent cannot be the way to repair the dysfunctional relationship that already exists between the Government and its electorate; an electorate that has long-since lost confidence and trust in the custodians of its human and democratic rights.

References

http://www.politics.co.uk/news/2012/04/03/whispers-of-discontent-rebellion-builds-against-snoopers-cha

http://38d.qs/38-lib

Clement Guitton

My name is Clement Guitton, and I am a doctoral candidate in the department of War Studies at King's College London. I would like to offer my brief comments and observations on the technical possibilities of circumventing the bill (question 25). I will focus solely on transactional data pertaining to the Internet and on the fallacy that the proposed bill is a solution to help identify actors on the Internet.

The current bill, by allowing access to transactional data, may encourage Internet users to hide further their data (e.g. IP address, location of server storing their e-mails) using techniques that would make it impossible for law enforcement agency to identify users. The use of anonymising techniques can thus defeat the purposes of the bill, showing the inadequacy of the bill to respond to the current technical possibilities. The Joint Committee should therefore consider other policy solutions that are outside the technico-legal realm to ensure appropriate attribution (the assignment of an action on an information system to an agent).

In the past already, legal solutions to ensure identification have counter-balanced the relative anonymity offered by technology. For instance, the Finish authorities forced Johan Helsingius, the owner of the first remailer anon.penet.fi, to give data on users at least two times, in 1994 and 1995. The service anon.penet.fi allowed users to post comments without showing their actual e-mail addresses. The authorities then successfully identified the authors of posts they were interested in. But techniques to prevent identification further evolved, and there are currently many possible ways to anonymise traffic: from single proxy solutions (similar to anon.penet.fi), to the implementation of onion routing services with Tor or I2P. In the case of a single proxy, if the proxy is located in the UK, the bill is applicable as the proxy has the technical capacity to retain the real IP address of its clients. This implies that there may be an economic loss for British providers of anonymising services and an incentive to delocalise. Clients of anonymising services would know that the company could no longer offer them protection of their transactional data, and hence of their identity. In the case of Tor and I2P however, there is no current possibility of circumventing the masking of traffic data.

Tor and I2P are free services that function similarly to one another. The final destination of the traffic is encrypted within a packet. The only information contained in the packet is its next destination node. Under the bill, it implies that law enforcement agencies need to contact all the intermediary nodes that a packet has gone through to identify the real IP address of a packet. If any one of these nodes is located outside the UK, that node would fall outside the jurisdiction of the bill. The operator of the node would be unlikely to retain traffic data unless a similar legislation existed. All Internet users can operate these nodes functioning on the principle of a peer-to-peer network. It is therefore also difficult to consider the operator of intermediary nodes as telecommunication providers and to enforce the application of retention of data for all users operating Tor or I2P as relay.

Tor and I2P also offer services known as 'hidden services'. Hidden services offer similar functions to the Web (e.g. forums, web-pages, e-mail services). However, these services do not communicate between each other using an IP address, but use the overlay network functionalities of either Tor or I2P. In practical terms, this means that it is not currently technically possible to determine the location of the server hosting hidden services. Two people sending each other e-mails from Tor Mail, a Tor hidden service for mail, know that no law enforcement agency can force Tor Mail to give them access to its users' mail, as no one can even know under which jurisdiction the service is located.

Users have different reasons for using anonymising services. They range from evading attribution from law enforcement agency because of the illegality of their actions, to ensuring ways for businesses to carry out research on competitors without raising their suspicions. But in any case, it is already very likely that criminals and potential terrorists use these anonymising services, against which the bill is rendered useless. Yet, the main point of the bill is exactly to use transactional data in order to 'investigate crime and terrorism, protect the vulnerable and bring criminals to justice'. It appears to be the wrong answer to the problem, and may even yield unwanted effects: to render the use of anonymising services on the Internet as the norm rather than the

exception. Other legislations already enacted can push Internet users towards this direction, such as the enforcement of the Digital Enforcement Act 2010 to identify copyright offenders.

Putting much emphasised on traffic data, while yielding from time to time genuine intelligence for law enforcement agencies, can misguide them. There have been countless examples of hijacked public wireless Internet communication spots that have led to wrongful indictments. For instance, on 27 July 2008, terrorists used an unsecure wifi spot in India to send an e-mail to the media five minutes before detonating a bomb killing 45 people. Less consequential, in 2010 in Germany, a woman's wifi was used to download copyrighted material while she was on holiday, and she was still held accountable (see I ZR 121/08 – Sommer unseres Lebens, Bundesgerichtshof). Instead of helping law enforcement, these cases demonstrate the easiness to spoof traffic data and its unreliability.

As mentioned above, and acknowledged in the introduction of the draft bill, there are discrete instances where the use of transactional data proved to be useful. The French enacted a similar law on 1 March 2011 (décret n° 2011-219) to regulate the retention of traffic data for a 12-month period by any communication providers. In March 2012, an individual went on a killing spree shooting seven people in the streets of South France. One of the victims was supposed to meet a potential buyer for his motorbike that he had met via a French website, where he had advertised the motorbike. The police contacted the website to obtain the transactional data of the visitors on the specific advertisement, and used the information to identify Mohammed Merah, the perpetrator of the killing. Such cases are rare, rely on the low technical skills of the instigator of criminal activities, and do not justify ubiquitous retention of traffic data. In light of my previous point, it can appear that the benefits of the bill are dwarfed by its incapacity to respond to more elaborate attempts to hide from law enforcement, and by the damage that it potentially causes to privacy.

The mere retention of traffic data does not lessen privacy. But the lessening of privacy can happen in at least two different ways: if the access and coordination of different data yield unexpected results, or if unexpected individual have access to the data in an unauthorised fashion. Both ways of lessening privacy are very likely to occur with the bill. The number of fines administrated by the Information Commissioner Office as well as the number of recent high profile leakage of personal data (e.g. Sony in 2010 and 2011, Zappos in 2012, LinkedIn in 2012) show that private and public sector organizations face difficulty in ensuring the confidentiality of personal data. By increasing the number of personal data retained (the IP address falls within the definition of personal data of the Data Protection Act 1998 and EU directive 95/46/EC), and the number of entities forced to keep such personal data, one can only foresee the number of breaches to rise. With techniques in data mining producing increasingly relevant and new information from low value input, we can only assume that breaches revealing even merely revealing transactional data will have important consequences. Instead of enhancing the cyber security landscape by giving a way for law enforcement agency to gather intelligence to start investigations, it increases cyber insecurity by creating more threats than there already exist. A long retention period also increases the threat of breaches and the likeliness of violation of privacy. In the case of the example of Mohammed Merah's capture, the French killer, the police accessed traffic data dating less than a month, as they investigated directly as a result of the shooting. The accumulation of data during one full year appears to be relatively long for the purpose of the bill. Most of the data retained for a long period of time will have no use and will simply represent a threat to users' privacy. Despite the bill's mention of measures supposed to ensure the security of the data, such as compliance with standards (article 1.3), the Joint Committee should consider two points. First, it is difficult to ensure the enforcement of the standards. Second, compliance with standards does not ensure that no individual will succeed in breaching the data.

As a conclusion, the current bill can render the gathering of intelligence on the Internet by law enforcement more difficult, as many technical solutions exist to users to evade attribution. The Bill is disproportionate in its approach, by creating important potential privacy breach by requiring all communication providers to retain all transactional data. Following the US legal scholar Lawrence Lessig's book entitled Code, regulation of the Internet can have four elements: law, technology, norms and market. As any law on attribution will face the technical difficulties mentioned above, the Joint Committee should rather turn to normative and economic solutions to enhance the capacity of law enforcement in their use of data transiting via the Internet. The solutions can be complex, as they involve inter alia giving incentive to users for not using anonymising services

or for fostering norms of appropriate behaviours. But they can also be more sustainable and balanced than 'quick' legal fixes.

Roger Heathcote

I would like to register my strong objection to the Draft Communications Bill.

In this country we are free to do as we like unless there is a law preventing us from doing so. When accused of a crime we are held innocent until proven guilty. Why then should we, as a nation, be subject to mass surveillance of a type more powerful and broader in scope than that of the Stasi? It seems un-British to me; fundamentally at odds with the personal and political freedoms Britain has been famed for over the centuries.

I believe power often corrupts, and that routinely surveilling the entire population and stockpiling all that data is asking for trouble. It won't be long before the police are routinely "data mining" the corpus and giving access to private investigators. Directly or indirectly this stockpile of information will contain pretty much every personal detail anyone could want to know: political beliefs, habits, tastes, interests, associates, financial information, times of movements, locations frequented, and so on ad nauseam. Reassurances that the content of email will not be stored miss the point completely - it is already more than enough data to allow serious abuse and access to this kind of info makes further "hacking" trivial. Indeed thousands of computers and accounts are hacked every day by hackers working with a tiny fraction of the information this legislation proposes we routinely collect and store - I worry some politicians don't really grasp that.

Although undoubtedly useful to the police, recent history has shown that access to such vast collections of data cannot be effectively controlled - from Bradley Manning's wikileak to the hacking of Sony and 77 million of their user's accounts last year to HMRC losing disks containing 25 million UK citizens personal details. It's no exaggeration to say that barely a week goes by without a huge institution or company getting hacked and losing tens of millions of account details. Valuable data on that scale cannot be contained - it simply can't be done - whether it is held by the state or the private companies this legislation plans on forcing to collect it. Such systems are inherently porous for both technical and human reasons. Ask anyone in IT (who isn't tendering for the contract!) and they will tell you perfect security is either impossible or impractical and indeed recent history shows us that - more often than not - adequate security has proved impossible for some of the worlds largest companies and governments.

We are talking about sensitive and valuable data here. We should bear in mind at all times that, as well as the police, this proposed mass of information would also be of incalculable value to blackmailers, identity thieves, corporate spies, terrorists, foreign powers, stalkers, hackers and a hundred other types of ne'er-do-well - as such the creation of such databases is MASSIVELY irresponsible, their very existence puts the nation and it's every citizen at risk.

Personally I think the events of the last year show the police are far from incorruptible and I do not believe they have shown they can be trusted with such an enormous increase in their powers of surveillance, especially where those powers are unrestrained by the judiciary and those who are surveilled are never informed of the fact even after they are cleared of any suspicion. I would argue that rather than massively extending surveillance powers we need to re-examine those we already have (i.e. RIPA) as they are deeply flawed and already give far too many people access to sensitive personal data without adequate safeguards, consent or transparency. Such law already increases the public's exposure to all the problems outlined above and until we can fix that we have no place creating new laws that massively expand surveillance - historically the favourite tool of the police state - without pointed suspicion or judicial oversight.

George Hoggarth

It is clear that this bill forms part of the greater movement towards a state that hold detailed information about every citizen. It can track movement, location, contacts, interests and as it treats everyone as suspect, allows the state to use "private" information as a form of control.. It seems symptomatic of a government that fears the electorate, in a whole range of issues, increasingly government seems to be more about control and less about representing the people.

There are already ways of gathering information related to suspected criminal activity but IT systems allow for trawling of data about everyone, automatically everyone is then, a suspect.
Interestingly the German government is also interested but recognises that with their history with Nazi's and the Stazi they would have problems. This says a great deal about such systems. This government when in opposition seemed to recognise the danger of becoming a police state but has not lived up to its commitment to reinstate civil liberty's. Talking about some sort of "quid pro quo" bargain in relation to civil liberty strikes me as bizarre, this Bill is not needed.

The costs of such a system will be passed on to the people, its like being executed in China, when the condemned have to pay for the cost of the bullets used. Adds insult to injury. Britain is already referred to as the surveillance superpower of the world, not very flattering in a supposed democracy.
Would business be happy to operate in an environment which might severely compromise its privacy, doesn't sound like a serious question really, I imagine the financial sector will leave skid marks.

Costs:

Where have the estimates of benefit come from? Figures plucked from the air. Experience of government estimates would suggest we multiply cost by 10 and divide benefit by the same number. What benefits are envisaged other than employing people to do it?

Scope:

The definitions are so broad they could mean anyone.
Once the data is available it will be public knowledge, see the Leveson inquiry. Local authorities and the Police both misuse any power they have been given within hours of getting it, the potential to interpret meaning makes this almost inevitable.

While the UK seems happy to allow people to be held responsible for breaking the laws of other countries, even when it is not illegal in the UK and allowing other countries like the USA to extradite UK citizens with no real safeguards, I think we are perhaps the only country that allows its citizens to be treated this way. Attempting this control internationally will require other countries to change their law before it could possibly work
It will be impossible to control overseas providers without increasing the ability to censor international traffic. The UK will join such countries as Iran and China in using such controls.

Use of Communications Data:

Safeguards:

The only designated officer should be a Judge and such decisions should apply to all requests and be justified by a statement of suspicion.
If all communications are treated in this way a commissioner is irrelevant, data protection safeguards already in place do little to inspire confidence.

Parliamentary Oversight:

Enforcement:

Current data about the Polices response to their own staff who break the data protection rules suggest such breaches are common and rarely result in any significant action being taken against the people involved.
As there is no person in public authorities help responsible and fines are simply passed on to the public setting it out as an offence has no effect. A code of Practice, they already have to ignore so many. This information shouldn't be collected.

Technical:

People will increasingly use security systems that make such data collection difficult and it will of course inspire innovators to improve such systems. A technological arms race will develop which will not only interfere with collection but will also make the data collected unreliable and unusable. This would inevitably lead to a legal arm race as some of these systems will need to be made illegal and new ones developed.
It is difficult to separate the type of data sent and therefore collected, it also makes it easy to just add content at a later data. This law I suspect, will need to father many more, just to play catch up. I also wonder about the issue of decryption, surely this implies that the interest goes beyond the patterns of communication and into content. There are already good systems available that could prevent such tracking, like now the only people who will be caught out by these systems will be idiots. Which goes back to the function of these systems as more to do with social control than the prevention/detection of crime.

All data held on networked systems is inherently insecure and systems like this will be a prime target for activists. We could expect to see details of the communications of MP's, Police commissioners etc made public which might be interesting. Any search of a system like this that holds raw data would result in that data being organised for presentation to the inquirer, any hard copy would then be of organised and usable by anyone.
It also seems that for a small fee such information would be easily available to journalists or other security/tracking companies.

It is difficult to believe that this Bill will do anything to reduce crime and the only people who will feel a sense of increased security will be the people with access to the information and even this will be a chimera.

Lisa Kavanagh

Please make sure the Committee's report tackles the big questions about our right to privacy.

I oppose this snooping policy because my Grandparents went to two world wars so that their children and grandchildren and their children did not have to be living in a police run state.

The police already have the power to put people that they suspect under survailance and there have been many cases where the system have lost important documents, and military information and laptops that have been left in cars and the information has fallen into the wrong hands.

We are all aware of the political issues and threats that face us as a country everyday, but there are CCTV cameras everywhere so why would you need to put every single person under survalance I just do not know, but of course to control every single person who lives and breaths to the point where you would be invading peoples personal space and taking away our human rights. We are not cattle that the government needs to brand because it might seem mellow dramatic to say this but one day I fear you will go to the step of branding everyone and everywhere we go, we will have to go past a machine that logs who you are etc like in the sc-fi films, or maybe putting survalance cameras in our home because every single human being has the potential to commit a crime. You seem to want to know what is going in on in every single persons mind in the UK from private conversations on the phone to emails and texts messages. You can build a picture of peoples political tendancies, which websites interest them, what they look at and if you deem it to be a threat what would you do,... put them in prison because they looked at a website about the muslim religion so they might just turn out to be a terrorist. In recent years you the government have lost 25 MILLION child benifits records, myself in recent months have sent paperwork off to DWP and they informed me and my partner that they had lost the paperwork and they will send more out for us to fill in, my argument there is that the information on these forms have not only our address and date of birth but our National Insurence numbers along with our ID documents. And now you want to build a data base full of our personal information. I as a UK born citizen DO NOT SUPPORT THIS.
You have also lost witness statements in criminal cases which puts the witnesses in grave danger, danger to the point of death with these criminals.

I am also aware of the fact that local authorities have also used intrusive surveillance techniques to work out whether a family lived in the right school catchment area.
Building such a comprehensive database of the web habits of the whole population leaves us all at risk of bureaucratic error and even fraud.

In recent years polotitions themselves have been found to break the law by claiming expensess for such things as gardeners, moets, and even toilet seats, the list just goes on.

I am first and formost a HUMAN BEING and do appriciate my FREEDOM and would not like to have it taken away.

Sorcha Lenagh

Please make sure the Committee's report tackles the big questions about our right to privacy.

The Bill amounts to mass, blanket, surveillance of the population outsourced to the private sector, turning us all into a nation of suspects.

Courts in Germany, Romania, Bulgaria, Cyprus and the Czech Republic have found similar arrangements in their respective countries to be unconstitutional. It would surely be perverse if the citizens of Britain - a country with a tradition of protecting the liberty of the citizen that goes back several hundred years - were to to discover themselves to be less well-protected than those of Bulgaria and Romania!

The proposals grant access to communications data to local authorities and hundreds of other public bodies for a wide range of purposes that have nothing to do with crime fighting. This kind of blanket intrusion is indefensible .

If the data loss scandals of recent years have taught us anything, it's that the building of huge and unwieldy databases carries real risks. In recent years the government has lost 25 million child benefit records as well as the personal information of those serving in the armed forces, witnesses in criminal cases and prisoners. Local authorities have also used intrusive surveillance techniques to work out whether a family lived in the right school catchment area. Private companies have also been responsible for a large number of data loss scandals in recent years.

Building such a comprehensive database of the web habits of the whole population leaves us all at risk of bureaucratic error and even fraud. These proposals smack of the worst kind of totalitarian regime, which assumes a right to monitor and spy on all its citizens, regardless of their rights to privacy and liberty - and are not worthy of consideration by any civilised democracy.

Gordon Logan

All the main political parties have a commitment to total surveillance and the new 'STAZI' Britain, which is absolutely inimical to the British way of life. Vast amounts of money are also being wasted. Bankrupted by the fractional reserve banking system and Wall Street crooks, successive British governments are forced to tax and borrow to find the billions to pay for the new STAZI Britain and catching would be terrorists.

Ostensibly STAZI Britain is needed because of Al-Qaeda and Osama bin-Laden. Voice prints of Mr. Bin Laden proved long ago that he had ceased making recordings in 2001, and had either retired or was dead. The late Foreign Secretary Robin Cook was told by intelligence officers that Al-Qaeda didn't exist. Several documentaries have proved that the 7/7 bombings were carried out by a Gladio type state conspiracy, similar to the bombings that took place in Italy thirty years ago. A police intelligence analyst, Mr. Tony Farrell has also come to that conclusion independently.

Lord James has admitted in the House of Lords that he personally financed Irish and North African terrorism to the tune of 'billions', when he worked in the Bank of England. This is in Hansard. So British taxpayers were made to pay for both the IRA and the terrorists that invaded Libya and Syria. Before he died, former President Cossiga of Italy admitted that 9/11 was the work of Mossad. So we can forget about the Al-Qaeda threat.

What Britain clearly does need is a system of surveillance that will thoroughly monitor the British state, in particular its traitorous secret services, which work for Mossad and the EU, when they should be working for Britain. We also need to get the SAS out of Syria and get them to knock up criminals like Tony Blair in the small hours.

Awad Mackie

There are many issues with the bill _and_ it's presentation thus far, so I shall go through a list of objections:

- The idea that this is in anyway less serious that the previous governments' plans does not hold up to scrutiny. Separate private companies holding different databases is in no way safer, spreading the data does not make holding it any more safer.

- Holding the data in itself is merely making yourself vulnerable to attack. A fundamental principle of data security is not holding data you do not require, and this would not be required at the point it is collected.

- The data will be accessible to any provider/personnel working with it. It takes merely one person to reveal a lot if not all that data. The memory of data loss scandals and others does not fade easily from the mind.

- Not storing the content, but merely the details. There are a few misunderstandings here. Internet data is more akin to a postcode than a letter. Once you start looking and storing the address, the content comes easily. This is complicated by the technical nature of some data which will require looking in the 'content' part of the data.

- This leads to another point, it can be said that most of the blocks of the modern computing 'revolution' were enabled by computers being able to process much more data, faster than the old methods. Merely storing 'header details' will allow much of the same analysis about an individual, leaving aside the fact that header details on the web allow for much more fine-grained analysis anyway.

- In fact, this is the precise point this bill is aimed at. The information gathered by this bill will be analyzed by relevant agencies and for all functional purposes be available to everyone who wishes to see, as detailed above.

- Storing the header details, therefore, is substantially _more_ information than has been required before. It is incorrect to say that this will change nothing.

- Finally, and most importantly, proposals such as this are a significant infringement on civil liberties and the privacy of individuals. It amounts to a full state-wide surveillance solution, not just of suspects.

- The police and other authorities can already gain access to existing records from private companies. Requiring those companies to go above and beyond requirement is a dangerous precedent.

P Main

Has the Home Office made it clear what it hopes to achieve through the draft Bill?

1. Nothing the Home Office has said will do anything other than increase the surveillance on innocent members of the public. It will do nothing whatsoever to facilitate the apprehension of 'terrorists' or 'paedophiles' the usual suspects brought out when the government wishes to increase surveillance of the public and reduce the right to privacy.

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?
No. This is being done not because it is needed, but simply because it can be, using the hyped up fear of terrorism by vested parties to enhance their position an control over UK citizens.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?
They are an unnecessary and unforgivable expansion of interception of surveillance by unaccountable government departments and other authorities with little or no regard for the rights of the public.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

Costs:

9. Is the estimated cost of £1.8bn over 10 years realistic?

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5-6bn. Is this figure realistic?

Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

Use of Communications Data:

14. Are the circumstances under which communications data can be accessed appropriate and proportional?

What kind of crimes should communications data be used to detect?
There are no circumstances where this level of interception is appropriate or proportional.

15. Is the proposed 12 month period for the retention of data too long or too short?
The longer data is retained the more the danger of loss or misuse is probable. The record of Government departments and other authorities is not one to be proud of. Lost any flash drives lateley? The 12 month period is too long by 12months.

Safeguards:

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?
The UK has shown little interest in complying with the intentions of Article 8 ECHR.

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

A warrant system is the ONLY way any form of interception SHOULD take place. Evidence should be presented to prove that interception is required. There must be no 'fishing expeditions' by government departments. There must be no use by Councils or other public bodies for the type of enquiries published in the press of councils checking for 'dog fouling' and 'school catchment areas'. Every request for interception SHOULD be made through an independent judge with the presentation of proper evidence. This does not mean that this level of interception is in any way acceptable.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible?
It is my own personal experience that the Information Commissioner's Office is completely useless and a disgrace. They are unable to understand the basic regulations they are supposed to enforce. I have absolutely no faith in the ability of the Information Commissioner to protect mine or anyone else's rights in the face of this bill. The man responsible for investigating the Google Streetview fiasco, where no sanction was applied to Google, now has a job with Google. Just one example of the revolving door between regulators and the companies they are charged with overseeing. How could such an organisation deal with the work load when they themselves have stated they do not have the technical knowledge at their disposal to do the job they are presently tasked with. They are ineffectual and contaminated.

Parliamentary Oversight:

Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory?

Enforcement:

20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?
It is not the job of Communication Service Providers to be the police force or security arm of a repressive government.

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?

Yet AGAIN a 'CODE OF PRACTICE' . Not a law with proper legal and extensive penalties,just a code of practice. That would be the same sort of code of practice that states civil servants and go vernment ministers must make notes of every meeting but is routinely ignored? This again is my personal and recorded experience through the FOI Act.

Technical:
22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

23. How safely can communications data be stored?

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ?
Are there concerns about the consequences of decryption?

The Home Office colluded with BT and Phorm to allow a commercial organisation to intercept internet users private browsing and data for profit.

The CPS failed to act against BT and Phorm
The City of London Police failed to act against BT and Phorm
Various government departments paved the way for BT and Phorm. You have to ask why Phorm received so much help from the government. Only public pressure prevented this.

What makes you think I have any faith in the UK Government to take my concerns into account ?
Not one regulator stepped forward to protect the public what makes you think that I have any faith in the 'protections' afforded me in this bill?

Jim Nash

1, apart from a few small news articles there has been no attempt by the Home Office to make people aware of this. It covers a large proportion of the population and I believe needs the same coverage should be given as was given to the ID Cards did a few years ago.
2, There hasn't been a convincing case at all, with the use of VPNs and FTP sites and IP hiding programmes anyone who want to use or misuse information can do so with out it being recorded against them.

I would like to go through all point that need addressing, but I don't have time.

Richard Owens

The overarching abilities, as would be bestowed upon the government by the passing of the communications data bill, to surveil on innocent people (or more specifically, those not yet proved guilty of any crime) greatly worries me. The ability of others to intrude on the existence of private conversations is not in and of itself the scariest aspect, but more what can be done with the data.

On one hand, yes, it can be used to discover terrorist plots and provide evidence in criminal investigations. These legitimate uses of the data however do not make worthwhile the possibility of the loss of personal data. Once the data is collected it could be stolen, inappropriately accessed or even appropriately accessed for unethical purposes. The government's track record in keeping data private leaves a lot to be desired

By observing whom I contact online in any given day it is possible to deduce my medical conditions (as would evidenced by frequent email contact between myself and my neurologist and endocrinologist), my partners (whether or not I have made such relationships public) and even my sexual fetishes by having a record of the pornography sites I visit and the online communities I am a member of. These items of my personal information are something I wouldn't allow even my closest friends to know, let alone a government employee or potential hacker.

Nearly all of the positives of this bill can already be fulfilled by a court sanctioned surveillance request. With such a court order it is possible to obtain the information needed to thwart criminal behaviour and as such, this bill if passed will not give significantly greater ability to fight any crime.

In short, the gains are low and the risks are way to high!

George Pender

The extension of surveillance we would see under this bill would be deeply wrong. British Government should be (verbally) encouraging private enterprise to produce secure encrypted email systems which are as near to impossible to intercept and decrypt as possible and which are verifiably secure. Then those companies should be encouraged to export the product to China and across the world.

At the moment the suspicion exists that Government would prevent such a product from being developed, or that Government would insist on a ?back door?. This perception can be removed or severely lessened and individual freedom can be expanded hugely as a result but it will require great courage.

It is not good for Britain (either politically, or for the individual mental health of British people) to have greater snooping laws, it will also likely cause greater radicalisation of terrorists as they decide that we do not really believe in the mantra of ?freedom? that we preach (although it is, of course, better to do stuff within a framework of Law than outside of such a framework but that should not be the choice)

Instead the Government will feel free to ignore the opposition because it will be able to tell itself that, "if only these people knew the threats? they would then agree that the powers were necessary. Instead decision makers are in danger of being bounced into making the ?correct? decision.

In other areas of government policy people of all different professional backgrounds have decades to learn about, and ask questions about, to read commentary about and to check the veracity and representativeness of information about government policy before they are ever called upon to make important decisions about policy or to advocate certain causes.

This is one of the major advantages of an open society.

In matters such as these though, people can never know that they are being told more than half the story and people are called upon to learn very quickly and make important decisions within a matter of days, months or, I don?t know, perhaps even hours, of learning information. Furthermore the person presenting it may have had much longer to select and prepare the information presented.

So it is important that there is an absolute minimum of government secrecy and a maximum of transparency of approach, we cannot survive as a nation if we end up with a situation where the correspondence of every citizen are searchable and those under surveillance are never told about it, meaning the effects of worry may be much much wider than the actual surveillance.

Robert Stirrups

I am writing to register my objection to the Draft Communications Bill. You are, no doubt, already aware of the key objections- surveillance without suspicion violates every principle of democratic society, and in an era of austerity, spending billions on a completely unnecessary assault on our basic civil liberties is obscene. In fact, this puts a lie to the whole claim that we need to make cuts, or that 'we're all in this together'. To even suggest spending billions on this while talking of the need to cut basic services shows that the government do not believe their own rhetoric about the cuts.

We regularly see stories of government departments losing valuable data, and regularly hear of police misconduct at political protests (attacking people without any reason, arresting people for non-crimes, kettling children, etc). These laws will only cause these problems to increase. Furthermore, by creating what is essentially, a deliberate hole in our security systems, you create the risk of that hole being abused by fraudsters and other criminals.

In addition to this, I would add that NOT spying on everybody willy-nilly is the default position. It's up to the proponents of this legislation to provide an argument in favour of it, not for its opponents to argue against it. They have singularly failed to do so. In fact, all I've really seen is a lot of fear-mongering about terrorists and paedophiles. While these are of course serious issues, they deserve to be taken seriously, rather than used as a cynical means to give the police more powers. In fact, it's worth bearing in mind that in some intelligence matters, too much information can be as big a problem as too little. Giving the police access to everything raises the risk of swamping them and preventing them from preventing serious crime.

In conclusion, this Bill should be abandoned as a bad idea immediately.

While I'm at it, though, I want to point out how thoroughly sick I am of the current situation: It seems like at least once a year, the Government - regardless of party - suggests a really, really stupid law to restrict basic civil liberties on the internet, and I have to write to you people telling you to knock it off already. So how about, as a general principle, you guys just accept that the internet is not broken, and it doesn't need a bunch of people with no technological background whatsoever to come along and fix it? I mean, there are actual real problems out there which could do with fixing - healthcare, housing, the economy. An excess of privacy on the internet is not one of them. Neither is people sharing files with each other. The only real problem the internet has is a bunch of clueless yahoos trying to regulate it.

Crown Prosecution Service

1. We have been asked to provide a written submission to the Joint Committee on the draft Communications Data Bill. This submission provides information about the role of the Crown Prosecution Service (CPS) and the use of communications data in prosecutions.
2. The paper also addresses a number of the specific questions where the CPS is able to help, and which have been asked by the Committee in its invitation to give written evidence.

The role of the Crown Prosecution Service

3. The CPS was created by the Prosecution of Offences Act 1985 and is headed by the Director of Public Prosecutions (DPP), Keir Starmer QC.

4. The CPS is the principal prosecuting authority in England and Wales and is responsible for:

- advising the police and other investigators on cases for possible prosecution;
- reviewing cases submitted by the police;
- determining any charges in more serious or complex cases;
- preparing cases for court;
- presenting cases at court.

5. The DPP operates under the superintendence of the Attorney General, who is accountable to Parliament for the Service.

6. The CPS is divided into 13 geographical Areas across England and Wales. Each Area is led by a Chief Crown Prosecutor (CCP). A 'virtual' 14th Area, CPS Direct, is also headed by a CCP and provides out-of-hours charging decisions to the police.
7. The CPS has four Casework Divisions: Central Fraud Group, Serious Crime and Counter Terrorism Division, Organised Crime Division and Welfare, Rural and Health Division. In addition to cases investigated by the police, they deal with the prosecution of cases investigated by Her Majesty's Revenue & Customs (HMRC), the Serious Organised Crime Agency, UK Border Agency, the Department for Environment, Food and Rural Affairs, the Department for Work and Pensions and the Department of Health. They are also likely to be key partners with the National Crime Agency in due course. The Casework Divisions deal with terrorism, organised crime, fraud and other challenging cases that require specialist prosecution experience.

8. The Code for Crown Prosecutors, issued by the DPP under section 10 of the Prosecution of Offences Act 1985, sets out the principles to be followed by prosecutors when they make case decisions. The decision about whether to go ahead and prosecute a case is based on the following two stage test the Code for Crown Prosecutors ("the full Code test":

- The evidential stage: Prosecutors must be satisfied that there is enough evidence to provide a "realistic prospect of conviction" against each defendant on each charge. This is the first stage in the decision to prosecute. A "realistic prospect of conviction" is an objective test. It means that a jury or a bench of magistrates, properly directed in accordance with the law, will be more likely than not to convict the defendant of the charge alleged.

- The public interest stage: If the case passes the evidential stage, Prosecutors must then decide whether a prosecution is needed in the public interest. They must balance factors for and against prosecution

carefully and fairly. A prosecution will usually take place however, unless there are public interest factors tending against prosecution which outweigh those tending in favour. The CPS will only start or continue a prosecution if a case has passed both stages of the test in the Code for Crown Prosecutors.

9. Every individual case is considered on its own facts and merits, and the case will only be prosecuted if it meets the test set out in the Code for Crown Prosecutors. Each case must therefore have sufficient evidence and be in the public interest to prosecute, if it is to proceed to court. In many cases, communications data will provide the evidence to ensure there is sufficient evidence for a case to have a realistic prospect of conviction in court.

The use of communications data in prosecutions

The current statutory framework

10. Communications data refers to any data generated by the use of a communications device or method. For a prosecutor, communications data is the who, where, when and how of a communication. This for example includes the sender, recipient, time, location and duration of a phone call. Communications data does not include the content (of any phone call or email) which is the substance of a communication, or what was actually said or written.

11. Communications data can be evidence of association, location, timing and the identification of individuals. Communications data is often crucial to investigators and can form powerful evidence in all kinds of cases for prosecutors.

12. The current statutory framework is regulated by the Regulation of Investigatory Powers Act 2000 (RIPA). Under the present rules communications data is currently retained by the communication service providers for their own business purposes and access by public authorities to any of that data is tightly regulated by RIPA.

13. Communications data is normally admissible as real evidence recorded by a computer or as business records hearsay. Unless it is downloaded directly from a device, communications data such as billing will come from the business records of the Communications Service Provider. If it was recorded by a computer without any human input it will be real evidence of the communications, otherwise it will be hearsay admissible under section 117 of the Criminal Justice Act 2003. Part 34 of the Criminal Procedure Rules 2010 makes it clear that a hearsay notice is not required for evidence that is admissible under section 117 of the Criminal Justice Act 2003.
14. In presenting such cases, prosecutors should ensure that the evidence is as clear and simple as possible by using maps, schedules and timelines to highlight key points to the jury.

15. Recognising that many of our cases involve the use of communication data, the CPS has developed two communication data e-learning training modules to ensure that our prosecutors are equipped to effectively prosecute such cases.

The problems for criminal investigation caused by the changing nature of the communications industry

16. Existing access to communications data by the police, security and intelligence agencies and by others helps protect and safeguard the public. Due to the technological changes in the communications industry, companies in the UK that operate the existing communications networks, will have no need to retain data or provide agencies and the police with access to it. Consequently, it will become increasingly more difficult to obtain communications data.

Level of use of communications data in prosecutions

17. The CPS does not have management information on the numbers of cases where communications data is part of the evidential case. However, we can say that communications data is used as evidence in a wide range of cases. In order to help the committee, we have however looked at cases in the CPS

Organised Crime Division (OCD) from April to July 2012 (the 1st quarter of 2012/13) by way of a snapshot.

18. In this period, OCD prosecuted 53 cases involving 101 defendants. In 46 of those cases, OCD relied on communications data in evidence.

19. In July 2012, OCD had 436 cases in process, which consisted of 273 pre-charge cases and 163 post-charge cases.

20. The CPS expects 263 of the 273 pre-charge cases to involve communications data.

21. Below we have provided case studies of where communications data has supported successful prosecutions.

Operation Wipe

22. This case arose from an operation against a gang (or "organised crime group") assessed by the Serious Organised Crime Agency as falling into the most dangerous category. The conspirators prosecuted were involved in the supply of at least 25 kilos of heroin imported in two consignments through Heathrow on 28th May and 10th June 2011. The shipment was intercepted at Heathrow and the drugs replaced with powder. It was tracked electronically to a house in Slough which had been rented by one of the conspirators as a safe house from which to distribute the drugs. Initially two lead defendants were arrested at the address and charged. As a result of forensic investigation and the accumulation of extensive telephone evidence a further ten defendants were charged.

23. Of these five pleaded guilty, four pleaded not guilty but were convicted, and three were acquitted. It was the pattern and extent of the communications data used as evidence which enabled a number of the defendants to be charged. For example, there were around 3000 telephone calls between the conspirators in three weeks. All except one of the defendants was sentenced at Reading Crown Court in June 2012. The sentences ranged from 8 years to 19 years imprisonment.

Operation Occasion

24. This multi-handed drugs case involved a gang who were actively importing and distributing cocaine and laundering the criminal assets created by the distribution network within the UK. The investigation spanned 18 months and involved the co-operation of a number of law enforcement agencies. A range of covert tactics were employed including the use of surveillance, the deployment of listening devices, and the use of communications data. Several £ millions worth of cocaine was seized during this investigation.

25. Twelve defendants were prosecuted; eight of whom pleaded guilty, two out of the remaining four defendants were convicted. Out of the ten defendants who either were convicted or plead guilty only two were actually arrested in possession of cocaine. The only way that the prosecution were able to establish their involvement in the conspiracy was through communications data. When that data was taken together with the banking and probe evidence it ultimately led to the top six defendants on the indictment pleading guilty. The ten defendants received sentences for their part in the conspiracy ranging from 2 years to 13 ½ years imprisonment.

Operation Disorient

26. This case concerned the importation from Brazil of 250 kilograms of high purity cocaine. The drugs came into the UK in eleven holdalls which were dropped into the English Channel by container ship and later collected by small fishing vessel with a four man crew. The communications data regarding the activity of the boat at the significant time, namely when the fishing boat was getting into position to make the collection and then reporting safely away, was of overwhelming weight for the prosecution to

show the intention behind boat's manoeuvres. There was also key telephone evidence which allowed the prosecution to show the defendant's connections.

27. Given the absence of any direct evidence to link the eleven holdalls of cocaine recovered with the defendants on the fishing vessel and the movements thereafter with others who remained on land, it was the communications evidence which undoubtedly secured the convictions in this case. The defendants were convicted after trial.

Response to specific questions asked by the Joint Committee

Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

28. We are content with the proposed definitions.

Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

29. At present the Bill provides for law enforcement and intelligence agencies to have access to communications data. The CPS also prosecutes criminal offences investigated by the Department for Work and Pension (DWP) who presently request communication data under the section 109B (2A) of the Social Security Administration Act 1992. This is an alternative route to RIPA and the powers are used to obtain subscriber data and to extend to call logs and more detailed and in depth caller information.

30. Schedule 2 of the Bill abolishes this power. However, benefit fraud investigators deal with around 364,000 referrals and there are around 56,000 cases sanctioned (by the application of a caution or administrative penalty) or prosecuted each year. Communication data provides important evidence for many of these criminal investigation.

Are the circumstances under which communications data can be accessed appropriate and proportionate? What kind of crimes should communications data be used to detect?

31. We are of the view that the circumstances under which communications data can be accessed are appropriate and proportionate given the importance of ensuring that those who commit criminal offences are brought to justice.

32. There are sufficient safeguards in respect of the use of communication data and therefore its use should not be limited to the investigation of particular types of crime. The fact that communication data can only be obtained in a case when it is necessary and proportionate to do so, by an authorised public authority for the permitted purposes set out in the Bill, should be sufficient limitation in itself. The purposes have to be approved by Parliament and are consistent with the European Convention on Human Rights.

Is the proposed 12 month period for the retention of data too long or too short?

33. The proposed 12 month period for the retention of data should be appropriate. However, any shorter period may affect the investigation of a small number of serious cases such as terrorism, murder, sexual offences, and bribery and corruption.

How is communications data used in prosecutions?

34. Please see the earlier section of our response in paragraphs 19 to 29 concerning how communications data is used in prosecutions.

Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill?

35. The penalties are civil in nature and enforceable by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any

other appropriate relief. There appears to be sufficient powers in the Bill to ensure that communications service providers comply with their obligations.

Are the proposals for the filtering arrangements clear, appropriate and technically feasible?

36. This is a matter mainly for criminal investigators, and so we are guided and reassured by the views of law enforcement colleagues, who are of the view that the filtering arrangements will be effective.

How easy will it be for individuals or organisations to circumvent the measures in the draft Bill?

37. Communication data has been used in criminal cases for a number of years now. We use such data in a range of cases to support prosecutions and obtain convictions in court. The measures outlined in the Bill should ensure this continues to be the case. However, the future proofing of legislation in anticipation of future technological developments is very difficult, and it may be helpful to ensure that the provisions are reviewed periodically so as to ensure that they are keeping pace with technological and other developments.

Crown Prosecution Service
September 2012

Lucian Holland

I would like to register my objection to the Draft Communications Bill. We are assured by those involved that this is nothing to be concerned about since it is just bringing legislation up to date with the internet age. This is highly disingenuous. The bill would establish an enormous database of highly sensitive information about the entire population of the UK, without any requirement for judicial oversight required to access it. This is the behaviour of a totalitarian state, not the measured response of modern liberal democracy.

It is argued that since it is not the content of communications, but merely the destinations, numbers and addresses accessed that will be recorded and accessible, this does not constitue an undue erosion of individual privacy. Really? How would we describe a state that routinely recorded every movement of every one of its citizens; who they met, when and for how long; where they shopped; what clubs they joined; at which churches they worshipped; what events they attended? This sounds like an advanced police state of the sort that we are in the habit of decrying, and occasionally bombing. But how is this any different from what is being proposed in an age where an increasing proportion of our lives is being lived through the medium of the internet?

The home secretary complains that without this law we will be forcing the security services to "work with one hand tied behind their back". Good. That is exactly how the security services should work in a well balanced democracy. That is how you avoid becoming a police state. Are we really trying to argue that "only those who have something to hide have anything to fear from surveillance"? Surely our esteemed leaders haven't fallen for this oldest of totalitarian fallacies? We grant the state the right to police us on the understanding that the power this entails is strictly limited; partly because history has taught us time and again that this power will repeatedly corrupt those who hold it; and partly because the overly strict enforcement of the status quo ultimately inhibits positive social change as well as negative, disruptive behaviours. An absolutely central component of this limitation is that private individuals should be free from routine surveillance unless there is a defensible suspicion that they are guilty of serious wrongdoing. This bill would radically undermine this principle.

Then there is the sad practical fact that the state and its security services are some of the least qualified entities to defend such an enormously sensitive dataset. I have worked as a technical consultant on IT projects of many different complexions, including major projects for UK government bodies. I have watched successive governments decimate their internal IT capabilities through outsourcing to enormous, inefficient and incompetent consortia of corporations, to the point where "Government IT" has become synonymous with institutionalised failure. The idea that the government and its agents are qualified to maintain a database of this level of sensitivity is frankly laughable; far better to steer clear of the minefield altogether and keep the state where it belongs: in a small support role in the background.

Finally, to the claim that the absence of this new law will increase the risk (or at the very least, fail to decrease the risk) from terrorism and other organised crime, I have two answers. Firstly, this is simply false; for serious criminals there are plenty of ways around these constraints; while highly inconvenient and impractical for ordinary people to use in the day-to-day activities, routine use of anonymising tools and high-grade encryption would be a no-brainer for someone engaging in criminal activity, and would render the provisions of this bill useless. Secondly, it is time we faced up to the fact that liberty has a price; that price is the risk that those to whom you grant freedom will seek to harm you. If you wish to retain liberty, you must pay that price. I am willing to do so, and I believe that the majority of people in this country are too.

Phil Vellender

My uncle was a decorated Wing Commander who flew countless bombing missions over Nazi Germany to defend those liberties that marked our country out from the dictatorships of 1940s mainland Europe. He risked his life and lost over 330 comrades in the process so that we could remain free. Neither he nor they made the sacrifices they did to enable parliament to spend its time considering passing into statute liberticide legislation such as this.

It is essential that the Committee's report tackles the central issues about the awful fragility of our rights to privacy.

There are two pressing reasons to vote this dangerous bill down:
1. The government's plans would turn us all into a nation of suspects.
2. The government doesn't track our letters or face-to-face meetings. Why should it assume the right to track us online?

The self-evidently disingenuously named 'Liberal' Democrat/ Tory-led Coalition came to power making a huge fanfare of how as a Coalition it would distance itself from Blair and Brown's anti-libertarian tendencies and would set out to correct the blatant excesses of its New Labour predecessor's record in the curtailment of civil liberties that was the shocking by-product of New Labour's support for President Bush's 'War on Terror' after 9/11.

This proposal completely gives the lie to any pretensions of a return to 'liberal' governance and values. This legislation adds up to the most shocking intrusion into the private communications of all the citizens of this country in living memory, one that any repressive state anywhere would be delighted with.

Of course, the 'powers-that-be', like powers-that-be throughout history, always clutch at some imaginary 'straw' to justify further violations of our hard-won rights to free speech, assembly and, now, private communication. There has never been a state on the face of this earth or any police force, or similar 'law enforcement agency' for that matter, that would not say 'yes please' in response to the offer of more powers: for that is one of the primary reasons for 'security forces' existing - the accretion of power at the expense of the liberties of ordinary citizens.

One expects little better from the secret-state-friendly Tories, but it is quite painful to watch a party descended the proud traditions of 19th and 20th century social liberalism abjectly fawning and snuffling at the trough of the secret state along with all the rest.

In common with the demolition of state-sector education, the tripling of tuition fees and the destruction of the NHS I, for one, do not remember such a law being placed before the electorate in any party manifesto.

Indeed this measure only serves to point up once again the nature of the 'very British coup' that was reality of the agreement that sealed the Condemolition's arrival in Downing Street in May, 2010.

I therefore urge you to reject this dangerous, undemocratic and unnecessary addition to the powers of one of the most unaccountable, 'democratic', states in what used to be called the 'free world' and consign measure to the dustbin of history where it clearly belongs.

J Wheeler

Having seen various press reports and been alerted to the present call for comments by 38degrees, I am registering my objection to the proposed legislation. This is a complex issue and I can only make a short comment.

National security is not an absolute and the extent to which security can be increased is always a matter of judgement. It would be foolish to lose important civil rights because of the threat of terrorism: that is partly what terrorists are trying to achieve.

It is clear from recent press reports that the authorities seem unable to take a reasonable view of risk (vide the man dragged through the courts because of a silly remark on a social networking site). If the authorities are unable to stand back and ignore the trivial we must not let them have trivial data in the first place. Too often we are now seeing citizens being forced to defend their innocence against accusations which are without substance.

Another point is that data communications are international. Whatever this government thinks, it will in practice have no control over this data when it has been collected. It will be handled by international contractors who are bound to obey the dictates of foreign jurisdictions.
It will be held in places where data protection laws are weak (and we cannot be proud of the protection of private data in this country where losses are occurring with alarming frequency). Computer hacking and data mining are international too and there are many people keen to make money out of selling data, personal or not, legally protected or not.
And the long arm of the US government means that nothing is safe from them; their excuse is that they have national security to consider and it would be no surprise to me to find my data scrutinised by computers in the US once it had been collected here.

We should have nothing to fear if we have done nothing wrong. But the US government arrested and harshly treated a man who had done nothing wrong at all and was not even easily confused with the man they actually wanted. People here are arrested and no one gives them back the months or years of their lives that have been lost in fighting the false accusations.

Privacy is important to us, it is what distinguishes us from totalitarian societies. Do not let laws be introduced that cause our private lives to be snooped on. There is to be a list of organisations allowed to look at the data. Each of those probably contain hundreds if not thousands of people, each employing contractors to sift, store, analyse and report on the data. Amongst all those people are a few who are corrupt, a few who are curious and a few who are interested in me personally. We will not be able to find out what is being seen and by whom, if we ask we will not be told, even if we know or suspect that our privacy has been compromised.

All these are risks that easily outweigh any conceivable benefits to our society.

Finally, I notice from your website that the government is proposing that there is some sort of payback to the cost of this scheme. I cannot see how this will be. All my professional life I have seen proposers of schemes inflate the benefits, sometimes to a laughable degree. Do make sure that these figures are scrutinised by yourselves and by the public.

We need to know what the economic case truly is because my belief is that there will not be one.

S Wheeler

I hereby register my objection to the Draft Communications Bill. My key concerns include:

Control of my data

I would have no control over my data, once it is collected by third parties' on behalf of the Government. The Government is placing me at risk without my consent. The risks include, but are not limited to:
1. That police and other State agencies have access to a record of my political beliefs and social habits 2. That these records could be shared with private investigators or journalists which, as evidence set before the Leveson Inquiry has made crystal clear, means that they will be routinely made public without reference to me and could be presented in a manner harmful to me as a free and honest citizen and with criminal intent 3. That these records could be unlawfully accessed by foreign governments or criminal gangs, and aid further identity fraud, blackmail or account hacking

This proposal runs counter to everything that democratic governments' of free citizens should hold dear. The Government needs to completely re-focus its efforts in this area and begin promoting proper privacy practice and data protection policies, in accordance with our human right to a private civil life - yours and mine.

Suspicion - on the basis of evidence - by properly constituted, trained and managed agencies using transparent guidelines in a legal framework, answerable to the courts, should be the test for surveillance. This is the format for criminal intelligence and evidence gathering that we have arrived at by many years of legal evolution. The Government has advanced no evidence, indeed no credible case whatsoever, for the replacement of this model. Nor do I see any Government proposal as to how our rights as free people, with a right to a private life, are to be protected in an area - Information and Communications Technology - which cries out for new safeguards and the extension of our rights.

On the above basis, Government has the right to intercept and record information when someone is suspected of a serious crime. The proposal is for the collection of data without suspicion, in effect, mass surveillance. This is totalitarian thinking that must be resisted at all costs. My grandparents did not defeat fascism, and my own generation did not fight and win the Cold War, simply to have totalitarian government imposed by this spineless, back door, method.

Being able to compare location data, contact histories, websites visited, and the proposed ability to track any group, from sports fans to political protesters, will give Government agencies - including any agency that any future Government might conceive - unprecedented power. Such a vision is so nightmarish that I am confident that some will discount it as beyond the pale. Reflect; it will take only a simple change in the law to turn such a data collection regime into a system that will make the Russian Communist NKVD look like a bunch of amateurs.

The very fact that the ... supposedly ... democratic Government of Britain can even consider such a defeatist, authoritarian and decadent policy is, frankly, astonishing for its complete lack of critical thinking, evidence-base judgement and rectitude. This policy plumbs the very deepest depths of moral turpitude.

Such a policy will create extreme risks for whistle-blowers, private citizens and journalists investigating, and highlighting, legitimate information that is inconvenient to those in power. This, it must surely be clear to even the meanest intelligence, is antithetical to good, open, pluralist government. The Government appears to have made no consideration for that fact that minority political protesters are very often found - in the fullness of time - to be correct. Free speech and the right of assembly are the first and most fundamental political rights. I have seen no argument set forth, no evidence presented, no criminal intent, that persuades me that people's on-line activities need to monitored and recorded. Indeed, history would seem to present us with the precise opposite position.

This policy has been presented as a “preservation” of existing capacity. This is a clear lie. The policy advanced would be a huge extension of policing powers, which deserves proper democratic debate, starting with a full public consultation.

Data retention in Britain is already excessive and creating risks. The access policies for police are already far too wide and there is a sad lack of judicial supervision. There is also no notification policy for people who been placed under surveillance.

These problems should be fixed before the government suggests new surveillance powers.

We are in a recession. Spending billions of pounds on the surveillance of innocent people while cutting back on proper policing is, straightforwardly, barmy. Money should be spent on front line detection work where, as the Polices' record of recent years has clearly demonstrated, results can be obtained and the public protected.

No democratic governments force companies to aid surveillance through collection and creation of new data sets. How can Britain seriously stand up for human rights while abusing the privacy of millions of our own innocent citizens?

This policy suggestion is so obviously deeply flawed and immoral that I can find no words to adequately describe what a complete and utter waste of time it is - nor how wrong-headed and lazy the assumptions that underpin it must be.

T Wright

You requested comments on this bill, here are some. I have pasted this below rather than including a word document.

In what role am I writing

This bill is not particularly related to my profession, not any organisation I am a member of. I submit these comments as a member of the public, and a user of communications.

Has the Home Office made it clear what it hopes to achivve through the bill?

Yes. The governments stated aim is the prevention of serious crime.
In particular, the opening section of the bill does not suggest that it intends to use these powers for investigation into low level crime (e.g tax evasion and council matters).

Has the Government made convincing case for the need of these new powers?

No. A detailed scan and search of the document shows no evidence for the claim that it is becoming harder for police agencies to obtain communication data.
One would assume that has become easier since:

- Mobile phones collect more data
- Phone companies keep more records
- Automation has made it easier to obtain data
- More phone calls are made
- More data exchange is text based (e.g sms's and e-mail)

If anything it has become easier.

It may however be true that it may become harder in the future - however this is not the claim the draft makes. There is no evidence of this either, though I would find this slightly more plausible, though unlikely to be true (given access to a machine it is quite easy to install keyloggers). Should the government be responding to problems ahead of time, I'm not sure - but I think they will make worse legislation if it is for a possible problem.

Would it be preferable to have one overaching piece of legislation that governs the retention of communications data?

I don't feel qualified to comment on this, since I don't work in the application of law. My only opinion is that bills that amend previous bills greatly obfuscate the ability of the public to understand the bill, so amending other legislation would prevent the ability of the public to understand the bill.

If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

I don't have detailed knowledge of this. However I feel that scraping the following legislation would in some way rebalance civil liberties.

i) Bodies not related to deal with serious crime should not be able to access this data. (E.g councils, hmrc, education services and medical services)

ii) People should be informed after a reasonable delay if there communication has been monitored.

iii) Misuse of these powers should have criminal penalties attached to them.

iv) Costs could be attached to the use of these services.

This would act as some disincentive to the abuse of these services.

Is the estimated cost realistic?

No working is included. No reference is given to where the numbers come from. The estimate is therefore probably wrong.

Are the benefits realistic

Again, no working or references are included in the draft, so there is no reason to trust the data. The estimate is therefore probably wrong.

Are definitions suitable?

These are quite complicated technical issues. One point I would make is that there is no mention of whether HTTP URLs are being kept or HTTP headers.
This is very significant, since access to this information (which might be considered addressing information) is more or less equivalent to complete browser history. This is a vast amount of data.

Are the circumstances of access to data appropriate

No, the are far more general that the stated aim of the bill, and can be interpreted very broadly.

"preventing disorder" is very vague. I do not consider policing protests an appropriate use of these powers.

Market abuse doesn't seem consistent with the claimed purpose of the act.

"in the interests of the economic well-being of the United Kingdom" is ludicrously vague, and again not consistent with the claimed purpose of the act.

"in the interests of public safety," - this is again inconsistent with the would allow for example councils to investigate safety matters. Also it has applications to preventing protests, which is something the act should specifically not do. (The police seem to often misuse powers to harass protesters who are causing work for them).

"for the purpose of protecting public health," - this is ludicrously vague again, and not consistent with the claimed purpose of the act.

"for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, " - again inconsistent with the claimed purpose of the act.

In summary, these reasons are far too broad, and wholly inconsistent with the claimed purpose of the act.

Safeguards : designated senior person

I don't see why this shouldn't require authorisation of a judge. Internal authorisation is untrustworthy and prone to abuse. This action should also have a cost associated with it.

Does the technology exist to capture the data, store it safely and separate it from communications

This depends. Recording all traffic makes it a great deal easier for other people to also monitor this data - it is difficult to not make this the case, since people who repair the system need access to parts of it.

How safely can data be stored

I think the answer is very securely. The difficulty lies in providing easy access while keeping the data secure. For this to work you must only provide a limited number of people with access to this data.
This is directly at odds with making access to this data easy.

How easy will it be for individual to circumvent these measures?

This very much depends on the details. A plausible broken system consists of the senior officer 'reviewing' data requests when a large number of data requests data place and auditting of data requests. Automatic auditting is unlikely to work wel.

General concerns

I don't think that location of mobile phone calls should be considered traffic data! This is an awful lot of data.

Rt Hon David Willetts MP

Thank you for your letter of 6 September regarding your Committee's concerns about the possible consequences of the draft Communications Data Bill for businesses established in the UK.

My officials are in touch with the Home Office about the potential impact of the draft Communications Data Bill on business. The Department for Culture, Media and Sport is responsible for the competitiveness of the UK communications sector, including those companies who would be directly affected by the draft legislation. You might, therefore, like to approach Ed Vaizey for his comments.

However, you are right that as this Department has overall responsibility for supporting growth we would have a concern about administrative burdens that have an undue affect on business in the UK. We are also responsible for attracting and retaining investment from overseas so would be equally concerned if an overseas company decided to leave the UK, for whatever reason.

We are assured by the Home Office that the number of communications service providers (CSPs) subject to retention obligations is and will remain a fraction of the providers in the UK. Most of those concerned about the obligations that could be placed on them may never have any contact from the Government. Indeed, if they were contacted there would be a period of extended discussion and consultation before any obligations were placed on them.

While the Bill would increase the amount of communications data that some Communications Service Providers are obliged to retain, requirements for mandatory data retention have been in place since 2007 and for internetrelated communications data since 2009. We are not aware of evidence that these communications data requirements have had a negative effect on innovation, or UK companies, large or small.

Unlike in many other countries, the UK reimburses CSPs for reasonable costs incurred in meeting their obligations. We do not, therefore, believe that the obligations proposed in the draft Bill will drive business overseas or make the UK sector a less attractive place to invest. If the Bill is approved by Parliament, the Government will keep the impact on business of any new obligations under review.

The Impact Assessment for the Bill estimated the additional costs to the private sector resulting from implementing the legislation would be £869 million over ten years but with these costs being defrayed by Government the net impact on business would be minimal. The independent Regulatory Policy Committee has validated this assessment as fit for purpose.

Paul Bradshaw

1. As a journalist and journalism tutor I am enormously concerned about the ability of third parties to access data about those I and my journalism students have been in contact with. It effectively removes the protection of sources that is essential to the operation of journalists and their sources, a process that is essential for people to confidently air their concerns and for democracy to function.
2. As the Leveson Inquiry has shown, there is no effective guarantee that those with access to the information will not pass it on. And if it is passed on, knowledge of 'contact' information such as this is much harder to establish than the sort of leaking of facts by police officers that has been explored in the Leveson Inquiry.
3. This is in addition to the obvious consequences for people's perception of their freedom of expression and association.
4. The access being granted is too broad, and the penalties too vague. Oversight of the process should be as stringent as the oversight being imposed on every individual in this country, rather than merely being permission based or reliant on attention being brought to it. Who is accessing data, and for what reason, should be made public to highlight potential abuses in the system. Individuals whose data has been accessed should be notified of what access was made in detail, even if a time delay is necessary. Any other sort of oversight is subject to abuse.
5. Finally, there are obvious ways for those who are genuinely under suspicion to avoid these measures. It will be an expensive and ineffective measure for what it is supposed to achieve. Any cost calculations around the bill need to take account of the increased cost of doing business which will fall on those who, to take just one example, wish to keep their contact and movement details safe from commercial competitors who may hire a private investigator, and so would have to adopt anonymisation processes. Or those who stop using online services because of their discomfort regarding how that information might be used. They should also take into account loss of business from those who do not wish to use UK services because of these vulnerabilities.
6. The Bill runs contrary to the policies around relaxation of data held about individuals espoused by both parts of the coalition government in their election manifestos.
7. Ultimately, the measures undermine public trust – not just between journalists and sources, but also between politicians and the citizens they are supposed to represent.

August 2012

Alex Burr

1. I am a software engineer with 12 years experience working on telecommunication devices. This submission is my own opinion and does not necessarily reflect the opinion of my employer.

2. Before embarking on detailed comments, I would like to offer the following analogy: Most people accept that the police must be allowed to occasionally break down a door. Suppose that the government, worried doors were becoming increasing difficult to break down, proposed a Bill requiring everyone to give the police a copy of their keys. Just as in the current case, the government could claim that legally, the situation is the same as before: the police would only be allowed to use the keys, in situations which they would previously have been allowed to break down the door. But it is obvious that the under the new law, abuses would be possible which were never possible before. The situation is the same with this Bill. It may not legally authorise mass surveillance, but it would place the keys to mass surveillance in the governments pocket.

   Q2: "Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?"

3. The government has not made a convincing case. The case it has made is in terms of preserving access to the same level of data as was available in phone networks – numbers dialled. The powers it is proposing go beyond this in two respects.
4. Firstly, the data that the government proposes to collect goes beyond that currently collected by phone networks. Almost any site on the internet could be used to exchange personal messages, even if that is not is primary purpose. For example, newspapers such as "The Daily Mail" or "The Guardian" have comment facilities which could be used for this purpose. In order to track who is exchanging messages with whom, visits to all such sites would have to be tracked. What web sites you visit is much more revealing than who you talk to, since it will likely reveal your political beliefs, health issues, etc.
5. Secondly, the infrastructure necessary to do what the government proposes would, necessarily, be capable of being used for mass surveillance. There would no longer be any practical or cost barriers should a future government decide, legally or otherwise, to engage in mass surveillance. Indeed, doing so would be cheaper than maintaining the level of scrutiny required to prevent it.
6. See also below under Q22

   Q7: If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

7. It is sometimes suggested that the powers of the police should be balanced by having all their actions recorded. Apart from anything else, it would be instructive in this context to find out what safeguards they would consider necessary to their own privacy.

   Q16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

8. The proposal that senior officers in the same authority which wants the data should also authorise it is too susceptible to abuse. One reason is because as noted in 17, ensuring that the system only obtains the data asked for would require a lot of detailed work, which an official whose objectives are getting other things done will always under-resource.

9. It is difficult to see what kind of oversight would be sufficient. It is commonly noted that any regulator is prone to capture by those who it regulates, because their influence is concentrated, but the influence of those who benefit from the regulation is dispersed. This is particularly a problem in this case, because since police and other investigations are confidential, those who need to be protected will not know about it until later, if ever.

   Q17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be?

10. As noted in 17, ensuring that the system does not collect more data than necessary will require fairly extensive detailed technical work.

    Q22: Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content?

11. On the internet, communications data cannot be separated from communications content by a simple process, unlike the case of the phone network. In the case of the phone network, there was a strong separation between the two. Only the owner and operator of a telephone network was allowed to modify the 'protocol' by which the phone network operated, which allows calls to be routed from one phone to another.

12. A 'protocol' is the definition of the grammar and syntax of messages by which a computer program can understand what another computer program intends. On the internet, it is a trivial matter for any person to devise a new protocol, by which messages might be sent from one person to another. High-school level programmers can and do do this in a few weeks.

13. In order to separate communications data from content, it is necessary to understand the details of such protocols. New protocols are continually being created, and the existing ones are continually being modified. This has several consequences:

14. No purely automated solution exists. Any device for performing this separation would have to be continually updated with new software.

15. Such updates would be fairly expensive: There is no guarantee that the author of the protocol will provide any assistance, since they may be foreign.

16. In the case of web sites, the data which will be observable by the system will not be intended for a computer to understand as a self-contained message. For example, instead of representing “send this message to Mr Bloggs”, it will represent “send this message to the person whose name was written to the screen earlier”. It would then be necessary to infer 'communications data' from other data not really intended for this purpose. In this case, not only will the extraction be error prone, but it will be hard to bring the data up to evidential quality. It may only be useful for the purposes of investigation, not trial.

17. Because ‘communications data’ and ‘content’ are very mixed on the internet, any system for separating them will be fragile. Validation that the separation software does not leak any details of

communications content will require great deal of detailed work, several times more work than verifying that it obtains the data of interest. That is because it is always easier to show that software does something, than that it does not do something.

18. For this reason, cost pressures will work in the direction of allowing more content to be observed.

August 2012

Ray Corrigan

Home Office vague on justifications for the Bill and the Bill does not solve the complex problems it has been posited as addressing

In multiple media engagements the Home Secretary and other supporters of the Bill mention "protecting the public" from all four horsemen of the infocalypse - terrorists, drug dealers, child abusers and organised crime - and more, on several occasions quoting the Met police chief as insisting passing this legislation is a "matter of life and death".

Building multiple massive databases of intimate personal communications data makes the public more vulnerable to the four horsemen not less so. That such mass surveillance will not work can be demonstrated mathematically.

Floyd Rudmin, Professor of Social & Community Psychology at the University of Tromsø in Norway, analysed President Bush's authorisation of the National Security Agency's (NSA) secret monitoring of the email messages and phone calls of all Americans (The Politics of Paranoia and Intimidation Why does the NSA engage in mass surveillance of Americans when it's statistically impossible for such spying to detect terrorists? May 24, 2006 by Floyd Rudmin http://www.counterpunch.org/rudmin05242006.html)

"The US Census shows that there are about 300 million people living in the USA. Suppose that there are 1,000 terrorists there as well, which is probably a high estimate. The base-rate would be 1 terrorist per 300,000 people. In percentages, that is .00033%, which is way less than 1%. Suppose that NSA surveillance has an accuracy rate of .40, which means that 40% of real terrorists in the USA will be identified by NSA's monitoring of everyone's email and phone calls. This is probably a high estimate, considering that terrorists are doing their best to avoid detection. There is no evidence thus far that NSA has been so successful at finding terrorists. And suppose NSA's misidentification rate is .0001, which means that .01% of innocent people will be misidentified as terrorists, at least until they are investigated, detained and interrogated. Note that .01% of the US population is 30,000 people. With these suppositions, then the probability that people are terrorists given that NSA's system of surveillance identifies them as terrorists is only p=0.0132, which is near zero, very far from one. Ergo, NSA's surveillance system is useless for finding terrorists."

Rudmin takes one basic statistic – 300 million people in the US – and takes a conservative guess at some others e.g. the proportion of terrorists in the population. He then does wonderfully simple analysis to prove mass surveillance is useless for finding terrorists. The kind of conditional probability calculation done here by Rudmin is based on Bayes' Theorem, taught in most introductory college statistics classes and is mathematically very sound.

Mathematically the 4 horsemen are not problems that lend themselves to data mining. Even highly accurate data mining systems will swamp investigators with false positives when dealing with a large population. Law enforcement authorities end up investigating and alienating large numbers of innocent people. Finding the horsemen is a needle in a haystack problem and you can't find the needle by throwing infinitely more hay on your stack and/or creating multiple giant and exponentially growing data haystacks.

That such mass databases are useless for finding terrorists is clear. That they also make the public less safe is associated with the impossibility of securing mass silos of valuable personal data. Computer scientists simply do not know how to keep databases of the magnitude of those envisaged in the Bill secure from external hackers or the multitude of insiders who have access to these databases as a routine part of their jobs. Security experts like Ross Anderson, Peter Sommer, Bruce Schneier and Richard Clayton have written extensively about this. To understand this you have to think about how such systems can fail - how they fail naturally, through technical problems and errors (a universal problem with computers), and how they can be made to fail by attackers (insiders and outsiders) with malign intentions eg the four horsemen. When the inevitable hacks, leaks, data contaminations happen, what then?

Part 1 of the draft bill is indefensible

Part 1 of the draft bill gives the Secretary of State unlimited powers to mould data access regulations in perpetuity without the need to consult parliament in any meaningful way:

(1) The Secretary of State may by order—
(a) ensure that communications data is available to be obtained from telecommunications operators by relevant public authorities in accordance with Part 2, or
(b) otherwise facilitate the availability of communications data to be so obtained from telecommunications operators.
(2) An order under this section may, in particular—
[...]
(b) impose requirements or restrictions on telecommunications operators or other persons or provide for the imposition of such requirements or restrictions by notice of the Secretary of State"
There is no mechanism for amending such Henry VIII orders and they usually get rubber-stamped by Parliament without material scrutiny. The Secretary of State and her successors get to order anyone to do anything that can be related to facilitating access to communications data:

If you combine this with, as barrister Francis Davey points out (see 'The Communications Data Bill (first look)', Sunday, 17 June 2012 at http://www.francisdavey.co.uk/2012/06/communications-data-bill-first-look.html), with the broad definitions given in clause 28 of the bill, e.g.
""person" includes an organisation and any association or combination of persons
[..]
"telecommunications operator" means a person who—
(a) controls or provides a telecommunication system, or
(b) provides a telecommunications service,
"telecommunication system" means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy,
"telecommunications service" means a service that consists in the provision of access to, and of facilities for making use of, a telecommunication system (whether or not one provided by the person providing the service)"
- this Bill could theoretically, as currently drafted mean that we might be obliged to keep "who, what, when and where" records of family and friends social gatherings which involve listening to music, TV watching, internet or mobile phone use, electronic gaming or just chatting. Unlikely though that might currently seem and far though it may be from the current government's intentions, the wording of the bill must be viewed in the light of the inevitable progressive function creep (discussed below) and through the lens of a less benevolent future government.

Inversion of innocent until proven guilty principle

The notion that the day to day activity of every citizen should be recorded in the expectation that those records can, in future, be mined for nefarious activity is anathema to a healthy functioning liberal democracy.

Control of my data

I have no control over my data, once it is collected by third parties' on behalf of the government. The government is placing me at risk without my consent. The risks include
1. That police have access to a record of my political beliefs and social habits
2. That these records could be shared with private investigators or journalists
3. That these records could be unlawfully accessed by foreign governments or criminal gangs, and aid further identity fraud, blackmail or account hacking

This runs counter to everything governments including ours are trying to do through promotion of good privacy practice and data protection policies.

Suspicion should be the test for surveillance

The government of course has the right to intercept and record information when someone is suspected of a serious crime. But these proposals mean collection of data without suspicion: which is in effect mass surveillance. Due process requires that surveillance of a real suspected criminal be based on much more than general, loose, and vague allegations, or on suspicion, surmise, or vague guesses. To instigate the new set of legal norms envisaged in the Communications Data Bill which subsequently give the entire population less protection than a hitherto genuine suspected criminal, based on a standard of reasonable suspicion, is indefensible. The gathering of mass data to facilitate future unspecified fishing expeditions is unlawful.

Accessing big data sets opens up new police surveillance powers

Being able to compare location data, contact histories, websites visited and so on will give the police the generalized ability to track any group, from sports fans to political protesters. This will create extreme risks for whistleblowers, journalists' sources and legitimate but inconvenient forms of protest.
This is not "preservation" of capacity but a huge extension of policing powers, which deserves proper democratic debate, starting with a full public consultation.

Undermining of Fundamental Rights

The proposals fundamentally undermine the right to privacy guaranteed in the Human Rights Act and article 8 of the European Convention on Human Rights. The Bill also undermines fundamental rights relating to freedom of assembly, speech, religion and association.

Comms data and traffic data cannot be separated simply in the way that the Bill assumes. See Professor Peter Sommer's analysis at http://scramblingforsafety.org/2012/sf2012_sommer_commsdata_content.pdf

Function Creep

I can only echo the concerns on function creep expressed by Paul Bernal in his submission to the consultation : "when a system is built for one purpose, that purpose will shift and grow, beyond the original intention of the designers and commissioners of the system. It is a familiar pattern, particularly in relation to legislation and technology intended to deal with serious crime, terrorism and so forth. CCTV cameras that are built to prevent crime are then used to deal with dog fouling or to check whether children live in the catchment area for a particular school. Legislation designed to counter terrorism has been used to deal with people such as anti-arms trade protestors – and even to stop train-spotters photographing trains.

In relation to the Communications Data Bill this is a very significant risk – if a universal surveillance infrastructure is put into place, the ways that it could be inappropriately used are vast and multi-faceted. What is built to deal with terrorism, child pornography and organised crime might creep towards less serious crimes, then anti-social behaviour, then the organisation of protests and so forth. Further to that, there are many commercial lobbies that might push for access to this surveillance data – those attempting to combat breaches of copyright, for example, would like to monitor for suspected examples of 'piracy'. In each individual case, the use might seem reasonable – but the function of the original surveillance, and the justification for its initial imposition, can be lost."

The temptation for public and commercial services to use the data gathered for purposes not originally intended will be overwhelming. If it can be done it will be done regardless of original good intentions.
RIPA needs to be fixed first
Data retention is already excessive and creating risks. The access policies for police are too wide and lack judicial supervision. There is no notification policy for people who been placed under surveillance.

These problems should be fixed before the government suggests new surveillance powers.

We are in a recession

Spending billions of pounds surveilling innocent people while cutting back on policing seems wrongheaded. I would rather money is spent on front line intelligence, policing, detection and emergency response work.

Bad examples to foreign governments

There are no democratic governments that force companies to aid surveillance through collection and creation of new data sets. How can the UK seriously stand up for human rights while abusing the privacy of millions of innocent citizens?

Conclusion

The government has failed to make the case for the need for the new powers proposed in the draft Bill. There is a significant danger in measures like the CDB of stumbling by default into a police state, just because the technology of mass surveillance is now more readily available and nominally more sophisticated. We need to avoid deploying these technologies blindly in response to some perceived threat. Without sufficient reasoned analysis of the purpose and detailed requirements of the technical systems we propose to build to counter these threats, we could find ourselves building technological monsters. Building an infrastructure of surveillance makes our citizens and our state more vulnerable not less so to attacks by criminal elements such as the four horsemen of the infocalypse and rogue states with malevolent intent.

August 2012

Peter Marcham

Response to questions

General:

1 Has the Home Office made it clear what it hopes to achieve through the draft Bill? The rational is not clear ; it is unclear as to what the need is over existing legislation.

2 Has the Government made a convincing case for the need for the new powers proposed in the draft Bill? No, they have more than enough powers; this bill gives disproportionate power to the government ; when trust of government is at an extreme low. See page 5

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy? No comment [nc]

4. What lessons can be learnt from the approach of other countries to the collection of communications data? The bill goes too far

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider? nc

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data? Simple answer YES :in general there is too much overlapping of legislation addressing different aspects of the same issue which makes it very hard for anybody to fully and easily understand!

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties? Yes RIPA

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business? It is not only comms providers but the users of comms both over their own private networks and the use of public networks : banks , commodity brokers, Oil companies, defence companies, Supermarket chains, Embassies ,etc all use comms and could be subject to the requirements of the bill if the government so wishes.SO it may deter or cause some businesses to relocate

Costs:

9. Is the estimated cost of £1.8bn over 10 years realistic? Intuitively it is likely to be out by a factor of 2 : it depends on the scope of the networks covered the level of reimbursement of operator costs. The bill is a little vague on this.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5 6bn. Is this figure realistic? How it intends to make savings is a mystery .
Scope:

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill? No there needs to be more explanation as to what the governments intentions are regarding which networks: private networks, MOD networks , Government network, email, cloud users etc .
12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order? There is a problem here as to what are the security services as aspects of policing become privatised or outsourced. Only the Police and Security forces.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty? They will not bother with the UK directly and outsource any connectivity requirements to others.
Use of Communications Data:

14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect? I don't believe they will be able to detect any crimes ; but will only be useful after the event. Anybody wishing to seriously avoid using current geographic based services will make use of other comms.

15. Is the proposed 12 month period for the retention of data too long or too short? Probable okay

Safeguards:

16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR? Reading of the draft it is very unclear as to who can be authorised ; from my reading even the toilet cleaner within a public authority could be authorised.

17. Would a warrant system be more appropriate? If you favour a warrant system should this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be? A warrant system should ensure that due care and attention is given to requesting one and be more traceable and fit with current systems.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible? nc

Parliamentary Oversight:
19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory? Oversight should be by a panel of normal folk as well ?

Enforcement:
20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill? If they are told clearly what the requirements they are meant to follow.

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence? YES of an organisations “CEO”

Technical:
22 Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content? Yes but it will depend to a large degree what is exactly being asked to record and may disrupt comms

23. How safely can communications data be stored? Logically this is easily possible.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible? No the purpose is not clear other than for data fishing trips.Technical feasibility will depend on the data.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill ? Depends on which measures; need drives ingenuity.

26. Are there concerns about the consequences of decryption? nc
You need not address all these questions.

Other points
A-There appears to be the possibility of confusion over data that is normally collected and that which is required under any order?

B-And what does it mean consult OFCOM ?

C- Will the result of OFCOm's deliberations be made public?

D-The designated senior officer can grant access or "section 9(2) conduct”" for themselves or others within their organisation. That is, they can authorise other in their organisation to engage with telecommunications operators to get what they need. This is rather a blank sheet !

E-The responsibility under 9(1)(b)(ii) seem out of place and should be the responsibility of TAB?

F-Any request cannot require (additional) interception of communications and cannot authorise anyone outside the senior officer's organisation in (9) (5). However, there are powers for senior officers in one force to authorise officers in another under Clause 19 Collaborating police forces in England and Wales. This doesn't make sense unless it applies to sharing data, the acquiring of data has no geographic limitation?

G-The list of purposes are outlined in 9(6). It must be "necessary" to gain the data for at least one of these purposes: The terms need very careful definition otherwise they become catch all opportunities ?

H-Would have thought all requests would have to be in writing?

I-12 Duration and cancellation of authorisations Authorisations last a month but can be continually renewed. It doesn't specify how renewal is achieved?

J-5 Use of filtering arrangements in pursuance of an authorisation
The designated senior officer also has to be satisfied that this would be proportionate. This should be an independent person not the person requiring the data? I get the feeling that all authorised data could be passed to an outsourced body [like a Serco] who would then do the filtering as required by “others”: just a feeling?

K-20 Certain transfer and agency arrangements with public authorities
Clause 20 outlines that the powers in clauses 14-16 (filtering arrangements) can be delegated by a "designated public authority" by order (Statutory Instrument).
Does this allow for outsourcing?

L- Identification of a computer file or program which is accessed or run by the communication is not traffic data (although identification of the apparatus where the file or program is stored is traffic data) Note sure what this means for example Skype encodes the voice ;is this a programme?
Trusting Politicians
The Prime Minister, David Cameron said before the election: “Faced with any problem, any crisis – given any excuse – Labour grasp for more information, pulling more and more people into the clutches of state data capture… And the Government doesn’t want to stop with the basic information. They want the most complex, important, personal information there is… Scare tactics to herd more disempowered citizens into the clutches of officialdom, as people surrender more and more information about their lives, giving the state more and more power over their lives. If we want to stop the state controlling us, we must confront this surveillance state.”1
The Conservative Policy Document, ‘Reversing the rise of the Surveillance state’, 2009.

Fewer personal details, accurately recorded and held only by specific authorities - on a need-to know basis only, and for limited periods of time. Immediately submitting the Home Office's plans for the retention of - and access to - communications data to the Information Commissioner for pre-legislative scrutiny.
The Coalition Agreement states: "We will implement a full programme of measures to reverse the substantial erosion of civil liberties and roll back state intrusion."
"We will end the storage of internet and email records without good reason."

August 2012

Montgomery Vaughan

General:
2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?
No, I do not believe they have. As with all other bills related to terrorism & crime prevention, it is extremely vague & easily open to misinterpretation. This leaves it wide open to abuse.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?
I think it is a blatant intrusion into an idividuals privacy. Unless the person is already under investigation there is absolutely no reason for the retention of an individuals data & absolutely no excuse to infringe on a persons right to privacy by the tracking and storage of what websites an individual decides he/she wants to look at.

Costs:
9. Is the estimated cost of £1.8bn over 10 years realistic?
No, As with all Government contracts & financial estimates, there always seems to be an over inflated price put onto IT contracts, & once the system has been in place, these costs then begin to inflate even further.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5 6bn. Is this figure realistic?
No, I don't see where they get these figures from, how will this money be made from retention of this data unless they are actually actively monitoring this data in realtime without a person being under investigation in the 1st place. The real criminals will now be more inclined to use complex encryptions & secure communications systems in order to hide their activity, which means they will not really make much impact on the organised crime front. This I think will be more abused by the users to scope out potential incriminations instead of Law Enforcement doing proper detective work in the 1st place.

Scope:
11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?
No, I don't. I think as usual, they are too vague & easily open to misinterpretation & abuse.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?
No, public authorities should have access to this data if the bill goes ahead. If it is to be used for Crime & terrorism prevention, then it should only be High ranking Police officers & Government Intelligence services that have access to this data, & only if they are transparent about it's use & if that person is already under investigation in the 1st place. It should not be used to detect a possible crime or to spy on a person to see if they are committing a serious crime.

As we have seen with RIPA, it has been abused by civil services & local councils & used in ways it was not designed for. Local councils & non government or private companies should have no access to this information & should not be able to get access to this information either as a 3rd party or other means.

I foresee that other private media firms such as FACT, MPAA, BPI will also try to gain access to this information, & has seen recently these companies are relentless in their efforts to prosecute for civil action suits & have paid police forces for information & to investigate. This is an abuse of the system, they are private companies & should NEVER be allowed to influence investigations or PAY for private prosecutions, neither should they have the power to be allowed to access personal data of a private individual without that persons permission. They are not Law Enforcement, & paying police authorities to obtain this information in the 1st place should be Illegal!

Use of Communications Data:
14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect?
It should only ever be used for serious crimes & terrorism. & should be clearly defined both in script & in it's nature. This the way it is proposed is so vague it can be easily openend to misinterpretation leading to abuse of the system & used in ways it was not meant to be used.

Enforcement:

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence?
Failure to adhere to a well defined code of practice should be treated as a severe criminal offence leading to possible imprisonment if it is found the access & treatment of information obtained has not been used for it's intended purpose.

Technical:
23. How safely can communications data be stored?
Define Safe! Can be communications be stored safely? Yes. But can a company state that their systems are 100% secure? NO, certainly not. & no amount of encryption will protect that data if a server is compromised & those encryption/decryption keys are stored on the server or on computer connected to the same network that the server is connected to. Should a breach happen, it would be likely the keys would also be accessible & in such a case, the security of the data becomes a risk.

August 2012

M Neal

General:
1. Has the Home Office made it clear what it hopes to achieve through the draft Bill?

It is important to understand that terroism – presently posses little to no risk to UK citizens.
The average number of deaths from terrosim is so miniscule that spending billions on reducing it is difficult to justify compared to other risk which are more cheaply and without harming other rights easier to change.

Failures by the police to efectivly maintain, ameleate and use intelligenece already in their possession should never be used as a justification for more surveillance which seems to be the case here .

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?
No Britain is a safer place now than it has ever been.

3. How do the proposals in the draft Bill fit within the wider landscape on intrusion into individuals' privacy?

Britain has indifference of lazy and corrupt regulators and MP's become a place where intrusion into personal privacy has become so ubiquitous it exceeds the dystopian of George Orwell's 1984. At the same time, the opportunities for redress when public & private sector organisations overstep the rights of citizens have been completely undermined by timid and corrupt regulation & law enforcement. There is no effective protection or remedy when the law is broken.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

The Joint Committee might be wise to look at history The activities of the Stasi bear comparison. The Stasi operated one of the world's biggest mass surveillance operations. The Stasi used mass surveillance to identify political dissent among citizens. Because citizens were aware that their government was spying on them a culture of mistrust resulted. Politics were only discussed where surveillance could not reach, and only with close family. Is that really the example you think the UK should follow? A database that encompasses the private communications of all UK citizens? If so, I fear you're ignoring history at your peril.

5. Are there any alternative proposals with regard to the technique and cost of obtaining communications data that the Government could consider?

Interception of communications should be a last resort, used in only the most serious cases of criminal misconduct, and only when a warrant has been obtained. Mass surveillance will compel the unconditional use of encryption, ultimately driving up the cost of mass surveillance in an escalating self-destructive spiral of countermeasures.
That impacts both the costs to Government, and the cost to UK telecommunications users (including commercial and personal users).

6. The draft Bill sits alongside the Data Retention Regulations. How will these two pieces of legislation interrelate? Would it be preferable to have one overarching piece of legislation that governs the retention of communications data?

It would be preferable if the Joint Committee were to recommend that legislation complied with the European Convention on Human Rights article 8, which stipulates; Everyone has the right to respect for his private and family life, his home and his correspondence.

Retaining communications data of innocent people (and we are presumed innocent untilproven guilty of a crime) is not proportionate. Unless you consider the UK a nation of criminal suspects.

7. If it is concluded that the provisions of the draft Bill are essential, are there any other measures that could be scrapped as a quid pro quo to rebalance civil liberties?

Any attempt to justify increased mass surviellance by a reduction in other powers is just a slight of hand to achieve a predetermined goal.

8. Will the proposals in the draft Bill pose a risk that communications service providers see the UK as a less attractive base. What might be the effect on business?

The additional costs and reputaional risk associated with storing such large amounts of persoanl data will obvioulsy force business to relocate oversea to less regulated environments.

9. Is the estimated cost of £1.8bn over 10 years realistic?

Hard to tell but that sum could save an awful lot of lives if spent in other ways.

10. The Home Office suggests the benefits that could be delivered by the enactment of the draft Bill could be worth between £5□6bn. Is this figure realistic?

I don't believe the Home Office could ever justify that figure. The money would be better spent addressing the deficiencies in police investigative procedures, intelligence handling, the child protection register, and eliminating rampant police corruption.

11. Are the definitions of communications data and communications service provider appropriate? Do they sensibly define the scope of the powers in the draft Bill?

The lines are becoming increaslily blurred and the definitions in the bill are hard to determine, particularly in reargd to the processess needed to get the data in question.

12. Which public authorities should be able to access communications data under the draft Bill? Should it be possible for the Secretary of State to vary this list by Order?

Serious offences only suggest only those liable to a sentence in excess of 5 years.

13. How robust are the plans to place requirements on communications service providers based overseas? How realistic is it that overseas providers could be pursued for breach of duty?

Essentially, it is a nonsense to believe that you can ever police overseas providers, or impose effective constraints on them. King Canute had more success turning the tides. The belief among some Members of Parliament that there could ever be a 'global standard' for communications regulation is simply delusional. Inconsistent regulation will always exist between democratic nations on one hand, and the corrupt authoritarian nations on the other. The issue is more about determining whether the UK becomes a model of a democratic nation, or a model of a corrupt authoritarian nation.

In the new world order nations will also compete on regulation as well as tax rates.

Use of Communications Data:
14. Are the circumstances under which communications data can be accessed appropriate and proportional? What kind of crimes should communications data be used to detect? Communications Data should be used to detect any serious criminal offence. It should not be gathered from innocent people until a crime is suspected.

15. Is the proposed 12 month period for the retention of data too long or too short? Communications Data should not be retained without a warrant obtained in advance. The evidence should be destroyed once a police investigation has concluded. And retained no longer than that.

Safeguards:
16. Applications for accessing communications data will be subject to a series of safeguards including approval by a designated senior officer within the public authority making the request. How should "designated senior officer" be defined? Is this system satisfactory? Are there concerns about compliance with Article 8 ECHR?

Every supposed 'safeguard' failed when BT conducted illegal covert surveillance of its subscribers using Phorm's Russian developed spyware in 2006, 2007 and 2008. The ICO refused to intervene. Ofcom claimed it had no powers to act. The various Surveillance Commissioners claimed they had no role to play. And the police refused to investigate. The CPS refused to prosecute. So if British Telecom can covertly intercept the communications of 200,000 of their subscribers and the businesses who serve them, using Russian developed spying technology, with complete impunity… Why do you think anyone would have any confidence in the supposed 'safeguards' the Home Office claim will guarantee protection from abuse?

17. Would a warrant system be more appropriate? If you favour a warrant systemshould this apply to all public authorities including law enforcement agencies? Should a warrant be necessary in all circumstances? And what would the resource implications be? Yes, a warrant based system would be more appropriate.

18. Is the role of the Interception of Communications Commissioner and the Information Commissioner sensible? The Investigatory Powers Tribunal has historically upheld few if any complaints; In addition, they claim they have no role overseeing the actions of private sector organisations that engage in unlawful surveillance. Until the oversight demonstrably includes robust enforcement of the law, and the scope of the oversight is extended to private sector organisations, the measures are utterly insufficient.

Parliamentary Oversight:
19. Are the arrangements for parliamentary oversight of the powers within the draft Bill satisfactory? Parliament has demonstrated no capability to effectively oversee communications surveillance. I do not believe MPs have the technical expertise required to understand the means or extent of unlawful surveillance. Why do you believe that situation would change as a consequence of this bill?

Enforcement:

20. Are the penalties appropriate for those communications service providers who fail to comply with the requirements of the draft Bill? No, they are too weak. Evidence suggests that the police & regulators will not enforce penalties against people who violate the law, and will even cite the trivial nature of penalties as reason not to engage in enforcement.

21. Are the penalties appropriate for those public authorities that inappropriately request access to communications data? Should failure to adhere to the Code of Practice which is provided for in the draft Bill amount to an offence? The unlawful interception of communications is already a criminal offence. But few people are ever prosecuted.

Technical:

22. Does the technology exist to enable communications service providers to capture communications data reliably, store it safely and separate it from communications content? Outside my knowledge

23. How safely can communications data be stored? Very safely. Until it is compromised. I fsont and US government cant keep it safe and secure what makes you think your better.

24. Are the proposals for the filtering arrangements clear, appropriate and technically feasible? No.

25. How easy will it be for individuals or organisations to circumvent the measures in the draft Bill? The bill will simply hasten the blanket use of encryption and/or onion routing… which will entirely defeat (or at least substantially impair) the value of mass surveillance. In addition, counter surveillance tools will likely further diminish the value of retained data by creating a blizzard of unusable noise (that will also need to be retained).

26. Are there concerns about the consequences of decryption? If encrypted streams are routinely intercepted and decrypted, confidence in any form of UK telecommunications – encrypted or otherwise - will be lost. At that point, any use of the UK communications network becomes wholly compromised, and the infrastructure becomes inherently untrustworthy. There then remains no basis for assuming that UK telecommunications are private or secure against unauthorised surveillance. Which would be a tragedy.

August 2012

Charlie Pearce

I think many of us in the look upon the activities of some foreign governments that actively spy on their citizens with disgust. It's fair to see that we consider that we have the moral high-ground over the activities of countries like Iran, Syria & China.

Passing this bill means that we no longer do. And in the long term this sets up a potentially disastrous future. While the current government says that it will not abuse this power, who knows what the future may bring. We in the UK like to think that we are long past any chance of a government with racist, fascist views coming to power, that we'll never see a dictatorship running this country. But history should surely teach us that no country is immune to this, who knows what the decades will bring. But we should not pass bills which so easily play into the hands of such people in the future, don't put in place the conditions that make it easy for the corrupt to flourish.

And for what? The government is actively cutting police funding, and you do not have to look far to find direct evidence of how that will harm people. But times are hard, so we must cut-back and this is understandable. Which makes the cost of implementing the surveillance measures required for this bill all the more hard to swallow.

As an IT geek I can offer some technical perspective: It is perfectly possible for any ordinary citizen, criminal or terrorist to take steps to hide or encrypt their activities online. To communicate with other like-minded people with little-to-no chance of anyone spying on them. This is, from a technical perspective, not impossible (and if you know what your doing, quite easy). The one saving grace that law enforcement have in this respect is that for the average citizen, criminal or terrorist - it's not trivial at the moment. They have to know that they can hide/encrypt their activities, and find out how. I'm sure that many don't, and so when these people are under suspicion - surveillance will work.

If this bill is passed, then it makes people like myself want to take the above steps to hide my activities. Not because I have anything to hide, but because I simple to not feel comfortable with what other people can know about me. It will make many others wish to do so as well. You will see new tools developed to make it effortless for the average person to do so.

It'll be commonplace. And your average citizen, criminal or terrorist will have to do very little to ensure their activities are not tracked by the government. Even if they are under suspicion - the police won't be able to track them. This bill will then only effectively target the innocent and the stupid. Sure the stupid can do damage, but why create an environment that makes life even easier for those dangerous people who aren't completely stupid?

Finally, I ask you to please tell me who exactly is pushing for this bill to be passed? I would like to see the evidence that such measures are needed. It's hard not to be suspicious that those who stand to benefit the most from this bill are those who will be contracted to implement the equipment required. Those companies have already made big business selling such equipment abroad. It's hard not also to be suspicious that those who will be signing the contracts to these companies will also benefit somewhere along the line.

August 2012

Three

Summary.
Three welcome the opportunity to comment on the draft Communication Data Bill.
We have support the Government's desire to strike the balance between protecting the public and safeguarding civil liberties.

We have some practical concerns regarding the details of the draft bill, in particular the provisions on third party access and the role of magistrates.

Draft Communications Data Bill.
As the UK's largest provider of mobile broadband services we recognise the shift from traditional methods of voice and text communication to internet enabled communications, and the subsequent challenge this presents to law enforcement and security authorities.
We welcome the Government's recognition that the current system works well and the important role Mobile Network Operators ('MNOs') continue to play in ensuring the security and safety of the public.
However we have some practical concerns regarding the proposals, which are detailed below:

Filtering.
Clauses 14-16 would enable the Secretary of State to establish a 'filtering arrangement', which will be operated either by Government of a third party. Due to the highly sensitive nature of the data involved we question whether it is appropriate to devolve responsibility for this data to a third party.
It is not clear who would take the ultimate responsibility for this data being held and used appropriately.
It should also be considered whether such a body would have the specialist knowledge to interpret the information being provided. Communication data sets and formats vary between different Communication Service Providers (CSPs) – it would have to be ensured that any third party would have to be able to interpret information from all operators correctly.

There is also the question as to who would take responsibility that the data, when provided, would be of evidential quality. Currently we vouch for the quality of the data but clearly this could not continue if a filtering body was introduced.
The Clause also states that any unrequired data should then be disposed of by the third party body. However there are no details as to how this will be done and, crucially, how operators would be assured that this unneeded data had been disposed correctly in accordance with existing laws.

Magistrates.
The Bill proposes that Local Authorities who wish to access communications data can do so via an application to a magistrate. While we recognise the reasoning behind this clause, we question whether a magistrate is the most appropriate body to scrutinise such requests.
The handling of communication data is an extremely sensitive issue and if responsibilities for these requests were handed to magistrates there would need to be assurances that a significant amount of time and resource would be dedicated to training magistrates to the required level. It must be ensured that the magistrates fully understand both the request and how to interpret the data.
There would also be an extra administrative burden on the CSPs who would need to check that the request had been approved at an appropriate level, unlike the current system where there is a clear audit trail.
Alternatively, we suggest that consideration be given to these requests being handled at a higher judicial level. Whilst we recognise the additional burden this might create, consideration should also be given to the repercussions of such requests not being, or not being seen to be, handled correctly.

Data Handling.

We agree that the proposed period of 12 months is a suitable period to expect operators to hold communication data and oppose any additional increase in this time limit. In our experience the vast majority (55%) of communication data requests occur within first 3 months and 80% within the first 6 months.

Destroying of Data.

The Bill proposes, in clause 6, a new requirement that Communication Data must be destroyed by CSPs a month after the 12 month period has elapsed. Whilst we recognise the reasoning behind this clause, there needs to be clarity as to what communication data it refers to. Some data is retained for over a year for business purposes (such as billing data) and the Bill should make clear that retention beyond 12 months for other purposes is permitted.

When a request is made, we also currently keep copies of both the data and the application for longer than a year. It would be useful if the Committee could consider whether this practice should be continued or whether this data should also be covered by this new legislation.

Obtaining Data.

We would prefer to maintain the use of RIPA to request communication data. This is the process that is currently used and we believe contains the right balance between allowing the necessary data to be requested and ensuring that there are sufficient safeguards in place to ensure data is not released unnecessarily.

In particular we have concerns surrounding the wording of Clause 9, which permits data to be requested 'for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data.'

This is an extremely vague clause and we have concerns that unless replaced by a more definitive wording that it could be open to abuse or disproportionate use. It is important that operators are not bombarded with less urgent requests, for example to facilitate training, which may impact on how effectively we deal with requests relating to an investigation.

It should be borne in mind that these powers are far reaching and should be exercised proportionately.

Subject Access Request.

There should be consideration as to how the proposals in this Bill sit alongside existing data legislation. For example would data that is generated by a request could also be made available through a Subject Access Request from a third party.

Conclusion.

Three remains committed to supporting Government and other agencies in protecting the public. We do have specific practical concerns regarding some proposals in the Bill. In particular we have concerns over the proposals to create a new third party body to handle the filtering process. We also are unsure whether magistrates are the best people to handle Local Authority communication data requests.

We would also be keen to explore further the reasoning behind the new proposal regarding obtaining data which replaces the current RIPA requirements.

If the Committee has any additional questions regarding this evidence, or would like Three to give oral evidence, please do not hesitate to contact us.

August 2012

Robin Trudge

I am the author of the No Nonsense Guide to Global Surveillance and would like to submit my own answers to the following questions from the questions listed at:
http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/news/call-for-evidence/

2. Has the Government made a convincing case for the need for the new powers proposed in the draft Bill?

Not in the least. May has dismissed criticism that the bill binned fundamental rights such as living free from arbitrary state suspicion and surveillance, or the right to hold investigators to account and their acts to judicial scrutiny, arguing that the only freedom being defended was that of 'criminals, terrorists and paedophiles', which is classic fear mongering.

4. What lessons can be learnt from the approach of other countries to the collection of communications data?

Plans to introduce such a bill in Australia have faced much civil opposition and been shelved until after the next Parliamentary election, which has annoyed the Australian Security and Intelligence Organisation, a supposedly public body but which seems to feel free to criticise elected governments for not giving them more surveillance powers on demand. The proposals themselves bore striking resemblance to other surveillance laws being wielded elsewhere.

In Canada earlier this year, police backed the 'Protecting Children from Internet Predators Act' that sought to have telecommunications providers give them subscriber data on demand, without a warrant, on the grounds that they needed such data quickly to stop children being groomed over the internet and suicidal people killing themselves. Funnily enough, while children and paedophiles often loom large in arguments supporting the set-up of all-invasive surveillance states for these children to grow up in, the bill did not mention children beyond its title, while the touchy-feely concern for suicidal people was a new twist on the 'ticking bomb' fear tactic that accompanies so much other draconian legislation.5 The bill was the latest attempt of many since 1999 to secure 'lawful access' and failed like the others, not least because, as federal deputy privacy commissioner Chantal Bernier said, the law 'could impact any law-abiding Canadian citizen' with its demolition of privacy and the presumption of innocence. However, Canada's Public Safety minister Vic Toews denounced one critic of the bill, saying: 'He can either stand with us or with the child pornographers.' And this remark was curiously echoed by Theresa May to opponents to our own 2012 Communications Act bill with her 'criminals, terrorists and paedophiles' barb (see above, and more in my article http://www.newint.org/features/web-exclusive/2012/08/16/internet-surveillance/)

As there have also been very similar bills going through the US Congress and Senate of late, one wonders if there hasn't been some broader agreement between the US, UK, Canada and Australia, the intelligence services of which we know have long worked together (along with New Zealand) under the UKUSA Agreement. "The signals intelligence community is very close, we share our intelligence overwhelmingly with the US, UK and Canada," a former Australian Defence Signals Directorate officer said as per a recent scandal of a Canadian naval officer leaking top British, US and Australian intelligence.
http://news.yahoo.com/canada-spy-sold-us-australia-uk-secrets-report-043443350.html

The evident lack of stomach seen for these measures among a good many of the MPs and Senators in the US, Australia and Canada at least suggests it was not our elected officials who came up with this warrantless surveillance caper.

August 2012

David Walter

1. I would like to express my great distaste for Theresa May's proposed Communications Bill, dubbed the "Snooper's Charter".
2. The bill is an example of how our civil liberties are being threatened by an undemocratic minority playing the politics of fear using threats of terrorism, drugs, and child safety in order to force the public into accepting to a supervised nanny state. This is an insult to the public's intelligence.
3. This move is a breach of everyone's human rights; as I'm sure you are aware, everyone has the right to a private life. Cataloguing everyone's digital communications in an age when people spend an ever increasing amount of their lives online is a massive intrusion of our freedom.
4. Now it is even more evident following the Murdoch-Cameron affair and cash for honours scandals that any government simply cannot be trusted with such valuable information.
5. Everyone I have spoken to oppose this bill, yet it is the taxpayer who will pay, costing at least £1.8bn by Home Office's own estimates.
6. One would like to think that this government has evolved beyond Jacqui Smith's vision of a 1984-style surveillance society. On behalf of the silent majority of the British public, I urge you to scrap this bill immediately.

July 2012

NOTES

[i] Joint Committee on the draft Communications Data Bill
http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/news/call-for-evidence/

[ii] There are companies offering retrospective decryption tools for TLS (where Diffie-Hellman exchange is not used) which might be why it is imagined feasible. For example Wireshark and Network Instruments Observer offer this facility.
http://www.networkinstruments.com/support/html_doc/current/index.html#page/Observer/decoding_encrypted_network_traffic.html
http://wiki.wireshark.org/SSL

[iii] Diffie–Hellman key exchange, Wikipedia https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange

[iv] Perfect Forward Secrecy, Wikipedia and Google Blog
https://en.wikipedia.org/wiki/Perfect_forward_secrecy
http://googleonlinesecurity.blogspot.co.uk/2011/11/protecting-data-for-long-term-with.html