HOUSE OF LORDS

HOUSE OF COMMONS

ORAL EVIDENCE

TAKEN BEFORE THE

JOINT COMMITTEE ON THE DRAFT COMMUNICATIONS DATA BILL

DRAFT COMMUNICATIONS DATA BILL

TUESDAY 17 JULY 2012

NICK PICKLES, JIM KILLOCK, RACHEL ROBINSON and ANGELA PATRICK

PROFESSOR ANTHONY GLEES and DR JULIAN RICHARDS

Evidence heard in Public Questions 221 - 329

USE OF THE TRANSCRIPT

1. This is an uncorrected transcript of evidence taken in public and reported to the House. The transcript has been placed on the internet on the authority of the Committee, and copies have been made available by the Vote Office for the use of Members and others.

2. Any public use of, or reference to, the contents should make clear that neither witnesses nor Members have had the opportunity to correct the record. The transcript is not yet an approved formal record of these proceedings.

3. *Members* who receive this for the purpose of correcting questions addressed by them to witnesses are asked to send corrections to the Committee Assistant.

4. *Prospective witnesses* may receive this in preparation for any written or oral evidence they may in due course give to the Committee.

Members present:

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Baroness Cohen of Pimlico
Lord Strasburger
Mr Nicholas Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker
David Wright

Examination of Witnesses

Nick Pickles, Director, Big Brother Watch, **Jim Killock**, Executive Director, Open Rights Group, **Rachel Robinson**, Policy Officer, Liberty, and **Angela Patrick**, Director of Human Rights Policy, Justice

Q221 The Chairman: Welcome to our fourth public evidence session. Welcome to Mr Pickles, Mr Killock, Ms Robinson and Ms Patrick. For the record and for the benefit of the public, who may wonder what is happening, Mr Pickles and Mr Killock were giving evidence last week. We did not manage to get through all the questions that we wanted to ask of them, so we have added them to today's session. However, we will ignore them for the first few questions, because we have a few questions we would like to put to Ms Robinson and Ms Patrick first, if we may. Could I start, therefore, by asking you—Ms Robinson and Ms Patrick—to outline your main concerns about the proposals embodied in this draft Bill? What are the areas that you each hope this Joint Committee is going to consider?

Rachel Robinson: I will make a start. Liberty is of course incredibly concerned about effective law enforcement, and particularly the need to protect the public from serious harm. We have never opposed targeted surveillance based on individualised suspicion, but what we have here is really a far cry from that. We have concerns about all areas of the Bill, but really the core of our concerns and the fundamental shift here flow from Clause 1 and from arrangements for collection of communications data. Communications data is already unique in terms of its historical availability to law enforcement agencies. While other countries across Europe are challenging the constitutionality of arrangements as they stand, we are finding ourselves in the position of pushing for a real sea change, a real step change, in terms of the arrangements for collection of communications data. Never before have private companies been called upon to collect data, which they have no business purpose to collect, purely on a just-in-case basis to satisfy potential future arrangements.

We hope the Committee will explore what we identify as the three fundamental assumptions and flawed assumptions upon which this policy is based. Firstly, there is the idea that communications data is, in some way, not particularly intrusive or not particularly revealing. We argue that is incredibly revealing in the current technological environment. Secondly, there is the idea that it even makes sense to draw the distinction conceptually between communications data and content. Thirdly, there is the idea that law enforcement gains would seamlessly flow from these provisions. We would suggest that the law enforcement case is, at best, shaky and incomplete. We hope the Committee will have an opportunity to examine these assumptions.

Q222 The Chairman: Thank you. We will wish to come back shortly on your assertion that countries across Europe are challenging it, but I did not want to interrupt the flow just now. Ms Patrick.

Angela Patrick: This is all going to sound very familiar now you have heard from Ms Robinson, Mr Pickles and Mr Killock, but Justice has worked on these issues for decades. We first reported in the 1970s that we were really concerned that we were racing headlong into a society where technology was advancing so quickly that our privacy laws were not keeping pace. I am new to my organisation, but these arguments are not new to us.

We would like to begin by saying that Justice recognises that surveillance, in many cases, is essential for the purposes of the prevention and detection of crime. In many cases, the work of the police, law enforcement agencies and the intelligence services saves lives. We accept that, but actually the flipside to that is surveillance is of a particular nature. It is accepted by everyone that, by its nature, it imposes restrictions and interferences on individual privacy. This is of different degrees of severity, but the starting point is that it does engage our individual right to privacy, as it is protected not only in the European convention but in the principles of our common law that stretch back centuries.

Those are the two flipsides with which we would like to start off the Committee: surveillance is legitimate, but it does engage privacy and needs to be justified; and surveillance, by its very nature, in order to be effective has to be covert. When looking at the regulation of surveillance, 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. That is our starting point.

Moving to the Bill, and I will be very brief because I know we have specific questions, I would like to put down three markers. Our first is that there is so much uncertainty in what this Bill is asking for that it is impossible for us, as civil society commentators, to pick it apart in terms of trying to help you, as parliamentarians, understand what the real risks are and what the challenges are for the Government in terms of providing evidence. It is so open, in Part 1 of the Bill, that I am finding it quite difficult to range our concerns, let alone ask what the right questions for you to ask are. Actually, when you are starting from a premise that what you are doing is engaging individual rights, that is really worrying. The Joint Committee on Human Rights has routinely called upon the Government, when they are looking at legislation that engages individual rights, to provide information to allow parliamentarians to conduct proper scrutiny. That Clause 1 of this Bill is so broadly drafted must be the first concern for this Committee, we would submit.

The second is, to reiterate Ms Robinson's concern, this is not about data access alone; it is about data collection. Your first 101 lesson, as a lawyer being told to understand the law on privacy, particularly as it applies to the European convention, is that every use of data is a new and interesting issue or set of circumstances, for which you have to look for justification. Here in the Bill, your starting point is: is the new proposal on collection of data justified? Is the proposal on collection accompanied by appropriate safeguards? Are the measures for retention of that data, once collected, accompanied by appropriate safeguards? Then and only then do you move to access, which is almost the final question. As we know, the proposals for access in the Bill are actually based on existing law—the Regulation of Investigatory Powers Act or RIPA. That is the last of my concerns that I would like to raise in opening. Justice has massive concerns about the lack of safeguards in the existing RIPA provisions. We think that building these potentially vast—we do not know, looking at Clause 1—proposals on to the existing RIPA framework is simply inappropriate.

Q223 The Chairman: Do you think RIPA has turned out the way you expected when you looked at it in the year 2000?

Angela Patrick: I think there was massive aspiration for what RIPA could achieve, but as it passed through Parliament, Justice campaigned quite vigorously to point out exactly how much of a mess RIPA was going to turn out to be. It is incredibly complex. Actually, the safeguards that are on the face of the Bill are relatively minimal. What you have is an administrative authorisation procedure, backed up by commissioner upon commissioner upon commissioner, which Justice has done a significant amount of work on. It shows that the degree of scrutiny after the decisions have been taken to access data is pretty minimal. Our concern is that, although the aspiration was to make RIPA, post-HRA 1998 compliance, a shining example of a human-rights-compliant framework for surveillance, it simply is not up to the job.

Q224 Mr Brown: Could you both say something to us, in general terms, about the sorts of safeguards you would like to see?

Rachel Robinson: In terms of our approach to this Bill, before we get to the point of considering potential safeguards, we are incredibly concerned about the path along which we are treading. It is only relatively recently that we took a significant step back in 2009, in requiring communication service providers to retain records for minimum periods, records they already retained for business purposes. Now, we are already seeing the next step and we are very concerned about where this path is leading us potentially.

To be quite frank, there is no safeguard that can allay our concerns about the kind of collection provisions set out in Part 1 of this Bill. As I said in my introduction, communications data and its use in law enforcement is a recent boon for law enforcement agencies. It is unique among other forms of surveillance provided for in RIPA in terms of its historic availability to law enforcement agencies. We simply do not accept the premise, the philosophical point, that the state has the right to keep this information about people in relation to whom they have no suspicion of criminal wrongdoing.

Q225 Mr Brown: What about where they do have suspicion of wrongdoing?

Rachel Robinson: We have never objected to even particularly intrusive forms of surveillance, such as bugging or covert human intelligence sources, where they are based on individuated suspicion and with appropriate safeguards. In terms of safeguards around access, we have consistently expressed concern around the access provisions set out in RIPA, which are mirrored in this Bill. We have consistently expressed concern about internal authorisation processes, the breadth of the permitted purposes for which this information can be accessed, and the range of public authorities that have access. These concerns are, of course, thrown into really sharp focus by the increase and the real difference in the nature of the data that would be retained under these provisions.

Q226 Mr Brown: Is that the same for Justice and is there anything you would like to add?

Angela Patrick: Justice did look very closely at the RIPA provisions. Before I outline our position on that, we are concerned that Clause 1 of the Bill is a game-changer. It could be, because we just do not know. People are very concerned and quite rightly because, as I say, if you are going to keep information about someone, it has traditionally been done for a purpose. It is almost beginner's lessons in the common law: we do not do things unless there is a reason to do it. The big question here is whether accessing every piece of information about anyone's use of the internet, in particular, is justified. We would say it is the starting point for this Committee's deliberations and must be.

Moving on to RIPA, we have had exactly the same problems with the RIPA framework in terms of its breadth of gateway, particularly for access through non-law enforcement agencies but also in terms of the mess and the jumble of authorisation mechanisms that exist in RIPA, in terms of different types of surveillance and the different types of authorities that have access to different powers for different purposes. The severe lack of judicial or other oversight of how those powers are used in practice is a point of real concern for us. Administrative authorisation is the norm for communications data access, and will continue to be so, except in connection with local authority use. That is a major point of concern for us, and we just do not understand how you could expand access to communications data without redressing that balance, even if there is evidence for further expansion.

Q227 The Chairman: Thank you very much. I think that is going to lead nicely into what Mr Ellis wants to ask you about. Before that, I neglected to ask each of you to say who you are and where you are in your organisation, just for the record. Ms Patrick first.

Angela Patrick: My name is Angela Patrick. I am Director of Human Rights Policy at Justice.

Rachel Robinson: Rachel Robinson, Policy Officer at Liberty.

Q228 The Chairman: We will ask you as well, Mr Killock, to just do that bit at the moment, and then we will ask you to be silent for a few more minutes.

Jim Killock: Jim Killock from the Open Rights Group, Executive Director.

Nick Pickles: Nick Pickles, Director of Big Brother Watch.

Q229 Michael Ellis: Going back to the issues that you both were speaking about in terms of authorisation, you say that there is no purpose that you can detect in this, but no doubt you will accept the police or the security establishment would say that there is a purpose, and the purpose is to help them detect offenders for the prevention of crime and to assist them in their work to keep the country safe. That would be the purpose that they perceive. I do not think it would be accurate to say there is no purpose to the Bill, would it? One would hope that there would be some counter-proposal to that suggestion.

If I can ask you both about your views on the authorisation system, the draft Bill has been criticised by you and others for not requiring public authorities, other than the local authorities—councils and the like—to seek any independent authorisation, by which I mean people like magistrates or judges, to obtain communications data. Instead, the mechanism envisaged by the Bill is a senior designated officer within the security organisation in question, so a senior police officer, say of the rank of superintendent or the like. Do you think that independent authorisation should be required outside of the scope of each organisation? If you do think that, how can you maintain those thoughts when we are aware that there are over 550,000 requests per year? Would that not clog up the whole system?

Rachel Robinson: We think independent authorisation should be required. It is not enough to remedy the problems here, but it is very difficult to see how an independent decision can be made by somebody within the law enforcement agency in question. We are not suggesting for a moment that there are routine abuses going on or any sort of purposeful misconduct on a routine level, but what we are suggesting is that there is an organisational culture problem. If you are working within an organisation, your primary concern is going to be with the operational capacity of your organisation. When it comes to conducting the delicate balancing exercising that takes place under Article 8—necessity, proportionality—an independent member of the judiciary with experience of weighing up these problems and,

principally and most importantly, with the prerequisite independence is the only authority in the proper position to take those sorts of decisions.

Q230 Michael Ellis: If there are over 500,000 data requests, would that not be, first of all, extremely expensive and, second of all, simply not feasible because of the sheer number of requests to a traditional authority?

Rachel Robinson: The first thing to say is that the sheer number of access requests, which has remained at the 0.5 million mark for a long time now, is indicative and just reveals the sheer scale of surveillance that is happening here. That is just on the basis of our current arrangements, and that is a real cause for concern.

Q231 Michael Ellis: Can I just challenge you on that? Just to come back on you to give you the chance, we heard evidence from a previous hearing that, although 0.5 million sounds like a lot—it is a large number—there are something like 25 million recorded crimes in the country. Many crimes nowadays require the use of data of this sort to be solved. To put it in context and perspective, would you not say that the figure is not actually as high as it might be?

Rachel Robinson: There are always steps we can take to reduce crime and produce law enforcement gains. These steps could be things like imposing a curfew on all males aged between X and Y for a certain period. There are always things that we can do that have law enforcement aims, but they are not the kinds of things that we would find acceptable in a liberal society.

Angela Patrick: Can I take a step back? Before you asked your question, you actually made a separate point, which was that you have already heard evidence from Home Office officials, law enforcement agencies and others about why they think these proposals are needed. I would like to clarify and I started at this point: of course some surveillance is necessary. Some surveillance is crucial and justified, but I would like to remind the Committee that under RIPA there are already very wide powers to access information.

This is not about starting from scratch and saying, "Let's open up key gateways to ensure that we are helping the police solve crimes effectively." What we are really talking about is whether the proposal in Clause 1, which is to create new mechanisms for collecting and retaining new information, about everybody potentially and anybody potentially—we just do not know—just in case, in order to expand the pool of information that may be needed for criminal investigation purposes and may expand the pool of information that is available for those purposes, is appropriate and justified. That is the real question here, not whether it is appropriate for the police to have access to surveillance powers for the purposes of crime prevention. Of course it is.

The question is: what should the powers of data collection and retention look like in order to enable the police to use those powers at a point that is most justified? The question is: how do you approach the balance between infringing the rights of those who might never be suspected of crime, by collecting data about them and retaining it, and on the other side reaching the optimum and most effective mechanism for crime prevention? There has to be a balance there.

Q232 Michael Ellis: I appreciate what you are saying. Can I bring you back to the authorisation point and whether you feel that there should be independent authorisation outside of the organisations and how you marry that up with the issue of the quantity of requests?

Angela Patrick: I am happy to do it. Justice reported last year, having looked at the whole of the RIPA mechanisms, that prior judicial authorisation, in most circumstances,

should be your starting point. In terms of communications data, we again said an independent judicial authorisation should, in most cases, be the default. However, we did also say that we recognised, as was explained by ACPO and the Home Office when they gave you evidence, that there are clearly going to be some circumstances where there is an emergency—where there is a pressing time-sensitive issue that requires action to happen now. We accept that, in real terms, those circumstances might arise. We said that, in those circumstances, if you have a law enforcement agency, the police or others, we can see the benefits of having administrative authorisation that is subject to retrospective judicial scrutiny within a reasonable timeframe. We have said two days or thereabouts would be reasonable.

Q233 Michael Ellis: You would agree that there might be permitted purposes for which you would not seek independent authorisation, and particular types of data, so for example subscriber data—just the raw fact of who is subscribing to the use of an instrument. That is not such sensitive information as other types of information.

Angela Patrick: We have said that there is a sliding scale. At one end of communications data you are looking at subscriber data, which is your name, your address, and how you are attached to your account, and, at the other end, user data and traffic data, which becomes, we would like to reassert, much more intrusive. We have in our report said, in terms of subscriber data, if you were simply looking at administrative approval, subject to other safeguards, that could perhaps be justified. In terms of these other forms of communications data—user data and traffic data—we think that the default should always be, except in that very narrow band of circumstances where there is an emergency, judicial independent authorisation.

Q234 Michael Ellis: Do either of you have any evidence about any individuals who have suffered harm as a result of their communications records being accessed by an investigator?

Rachel Robinson: The first thing to do is probably talk about the latest Interception of Communications Commissioner report. Hundreds of errors are identified, even on the basis of the small sample here accessed on the basis of retrospective scrutiny. Two people were detained and accused of crimes on the basis of inappropriate use of their communications data.

Q235 Michael Ellis: Two people out of how many points of data access—hundreds of thousands?

Rachel Robinson: We need to not lose sight of the fact that this came from provisions that were designed, or allegedly designed, to keep us safe from harm. We are seeing repercussions like this but, before we even get to that point—before we even get to errors, abuses or mistakes, in terms of processing or accessing data—we need to look at the very real harm that comes from the retention of the communications data of potentially everybody resident in this country at the moment. We need to think about where we are heading as a society and what is going to be the next step when we build an infrastructure that has certain capacities. What is the next step along that line?

Q236 Michael Ellis: There is not going to be a database as such for this information. The plan is to ask the service providers to retain the data for a period of time, which is not quite the same as a government database. It is not at all the same as that, is it?

Rachel Robinson: We would query the conceptual distinction between that and several smaller databases linked together by government-run processing.

Q237 Michael Ellis: I appreciate that you would query that, but would it not be the case, a possibility at least, that companies could, and in other jurisdictions may well, keep data for their own purposes, without the safeguards that this Bill might envisage. There may not be a time limit, for example, as to how long they would keep data and things of that sort.

Rachel Robinson: Obviously there should be protections around data retention in other contexts also. I think we really do have to recognise the step change here, from a position where companies keep information for their own commercial purposes to a situation where we are effectively contracting out responsibility for keeping records on the entire population for future law enforcement purposes.

Q238 Michael Ellis: Finally from me, is there anything about this Bill that you feel would be non-compliant with the provisions of the Human Rights Act? I think you said, Ms Patrick, that you were the Human Rights Director for Justice. Is that right?

Angela Patrick: I am. Can I simply come back to your last question before I answer this one? Is that okay? I know we are short on time. I agree with Rachel's position that there are wider implications, not simply of individual cases, about potentially creating a vast storage of data. I will not repeat what Rachel has said, but I will take you back to my first point. Surveillance is particularly special and states, in the case law around human rights, have been put under a particular obligation because these types of powers take place in circumstances where they are, by their very nature, covert. People who may be subject to surveillance may never know. If you are never prosecuted, if you are innocent but somebody has had to have a look around in your files or used these particular powers, rightly or wrongly, you may never know.

In fact, there is almost a higher burden on the state to look at the safeguards to make sure that they are clearly defined, strict and designed to ensure that only those powers that are necessary exist. Otherwise, the individual themselves may or may not be in a position to seek redress, as they might be in terms of false imprisonment or something else where it is pretty obvious that your rights may have been infringed. They might never know.

Actually, on the question about harm, as Rachel comes back to it, we have often only found out about an error when somebody has let slip that something has gone wrong and that you have been subject to surveillance. Therefore, you have been able to seek some form of redress. That is a very simplistic answer to your question, "Has anyone ever been harmed?" Even if we do have figures or evidence of error or not so much misconduct but mistakes having been made, there is a bigger question and a much more baseline starting point for the Committee's consideration.

Moving to your second question about human rights compliance, I am again going to say it is a sliding scale. We have looked at RIPA like this. The wider the gateway you make, the more likely it is that, without some form of judicial oversight, in an individual case, if there is evidence that something has gone wrong, there will have been a violation. Now, that analysis becomes much more problematic because there is so little case law on surveillance, because of the simple fact that these cases do not come to light very often. They will often only come to light when there has been a problem, and Liberty will be very familiar with this, having recently represented a lady from Poole who only found out that she had been trailed by her local authority because another local authority employee let it slip.

Actually, the problem we see, looking at the case law, is the courts have been quite robust about the fact that the best safeguard you can put in place is judicial authorisation prior to a surveillance having taken place. They have stopped short of saying you have to have this in all cases.

There are surveillance circumstances where they have said that you do not need a judge but, in most of those cases, it has been the case that they have looked at the facts and

said, "Actually, all the other alternatives have been explored; it was a proportionate decision; there were numerous other safeguards in place to offset the fact that you did not have prior judicial authorisation, including the provision for robust retrospective scrutiny." We say that the provisions in RIPA, which are being replicated in this Bill, fall far, far short of those kinds of robust safeguards. I would be quite happy to take you through why we think the detail of the IPT and the Interception of Communications Commissioner structures are failing, but I know we are short on time.

Rachel Robinson: In relation to that specific second question, we think that the data collection provisions of this Bill are not and will not be—are very unlikely to be, in any event—compatible with Article 8. In fact, we think that the provision that exists at the moment is highly dubious on Article 8 grounds. That is before we even get to the RIPA parts of the Act.

Q239 Lord Strasburger: Chair, could we ask Ms Patrick to write to us with her views on that?

Angela Patrick: Yes, I will do that.

The Chairman: Yes, we are happy to have a paper on your view on the failings of the Interception of Communications Commissioner, how you think it should be toughened up and what teeth it should have. Before I ask Lord Armstrong to come in, you mentioned in your comments that you saw a sliding scale of intrusiveness. I would really like, and I think the Committee would like, to get a paper from Justice setting out what your idea of the sliding scale is, from, I presume, at one end a name and telephone number of the person through the middle-ranking bits—bank account, the tracking of information of where they have been every five minutes.

Angela Patrick: We have actually produced a very hefty piece of research on it, and I am quite happy to have copies sent to all of the Members, if you would like them.

The Chairman: Excellent. We would certainly like that, yes, please.

Q240 Lord Armstrong of Upminster: If one wanted to restrict the scope of this Bill, one could reduce the number of authorities that are entitled to exercise these powers or one could look at the purposes for which it could be made. I want to look at the second of those. There are 11 or 12 purposes in the Bill, taken out of RIPA, which are permitted purposes for the purposes of the Bill. They go well beyond national security, law enforcement and serious crime. Are you happy with that list of purposes or would you like to see it reduced?

Rachel Robinson: We have consistently expressed concern about this list of purposes, which largely mirrors that provided for in RIPA. We feel that it is very difficult to envisage a case that does not involve or fall within the serious crime category in which it would be justified to access communications data. Those other purposes listed, things like the economic interests of the UK, are incredibly broad and encompassing potentially. There is a real potential here to go beyond what is necessary and proportionate and to, in fact, attach to or apply in circumstances that do not involve criminal behaviour in any way. That has always been a real cause for concern under RIPA, under the current arrangements. Of course, now that what we have on the table are proposals that will dramatically increase the amount of communications data and the kind of communications data retained, provisions around access are thrown into sharp focus. They become even more of an issue.

Q241 Lord Armstrong of Upminster: I am not quite sure what I am getting from that. Do you want to restrict the purposes to serious crime, terrorism and national security?

Rachel Robinson: What I would say at this stage is that it is very difficult to think of a case that does not fall within those categories in which it would be proportionate to access highly sensitive personal information about an individual. What we would also say is the fact that the Home Secretary can amend by order the list of purposes and the fact that the purposes as they stand are so broad and ill-defined create problems of their own, which become more important when we think about the proposals on the table now.

Angela Patrick: I would just go back a step again. Unfortunately, like Rachel I would say the list of purposes does not affect how much data is kept, collected or retained. As a starting point, you keep everything. It does not matter if you are keeping it for the purposes of crime or the purposes of whatever; there is no qualification like that anywhere attached to Clause 1 of the Bill. Basically, it is me, you, the guy you saw on the bus this morning and the person you buy your paper from. Clause 1 enables the collection and the retention of data in connection with yours, mine, his, hers, your mother's, your daughter's and everybody's internet usage. That all gets kept. As to the first two qualifiers that I gave about safeguards in connection with collection, and retention and storage of information, albeit it is not in a government database—it will be stored in private company databases—the question is then: are there safeguards in place to ensure that that information is kept safely and not accessed for other reasons?

The second question I would simply ask is: is that justified, before we get to the question of state access? On state access, we have already said, in order to justify accessing information that is clearly engaging your right to privacy, the state must be able to justify it. We can say that for prevention and detection of crime or for national security etc. I entirely understand it. The further you get away from those core purposes, the more difficult it is going to be to justify. Now, I listened to the Home Office's and ACPO's evidence, which was very full. My understanding of the information you were being given from those parties is that they would not like to restrict the purposes, because the real belt and braces was that individuals were being asked to consider, even within those triggers, whether the use was necessary and proportionate. Now, necessary and proportionate are essential from a human rights perspective, but our real concern is, as is stands, there is nobody checking whether that administrative assessment of necessity and proportionality is right. There is no judge who is saying, "Have you got that right? I know that your understanding is that you really need to do this for a criminal investigation. Tick; that has got you in the trigger gateway. What is the necessity and proportionality?" Clearly they walked you through the training that they believe is adequate for that purpose to allow an individual senior officer to apply his mind to that balance but, at the minute, nobody is checking.

The Interception of Communications Commissioner has been reporting on these issues since 2005. Our research showed that, although the very small team of inspectors—there are only five—look through dip sampling each of these different bodies and how they look at communications data, not since 2004 has the commissioner's report identified any single violation of necessity or proportionality in the decision-making of any public authority. Okay, in his report last week he found one—one out of 500,000 every year since 2004. I am a little bit of a sceptic, but I am also a public lawyer who has acted both for Government and for claimants. In terms of administrative decision-making, no public body expects to get it right 100% of the time. We have said, as Justice, that those figures must suggest that the commissioner either does not see looking at necessity and proportionality as a core part of his role or, alternatively, they simply do not have the expertise or the resources to be able to apply that kind of balance. Of course, applying it retrospectively, in any event, would only get you so far, because the interference has already taken place. We say it is much better to have a prior judicial authorisation in most cases, making exceptions for emergencies, where

somebody who is used to applying their mind to those kinds of tricky balancing questions is asked to do it.

Q242 Lord Armstrong of Upminster: Can I just come back to the purposes? To take one extreme case, one of the purposes permitted was where somebody has died and you cannot find out about that. You want to obtain information about their next of kin or about other persons connected with them, or the reasons for their death. Would you say that the powers of this Act should not be used for that purpose?

Angela Patrick: We would say that possibly you might want to check his pockets first and do other things to check that it was actually necessary to do it. At the end of the day, it may be, if you have no other means of identifying somebody, you might be able to justify that use.

Lord Armstrong of Upminster: Even though there is no crime.

Angela Patrick: If you were targeting the individual who was deceased and you were trying to identify somebody who was connected to him to notify him of his death, you could arguably say that that very narrow purpose could be justified. Again, if you were only opening the doorway to looking at the information connected with a deceased person, you would have to be very careful in terms of the safeguards of how you look at the other information because, clearly, we do not communicate only with ourselves; his communication data will be connected with third parties and other people. If you are only simply using that gateway to identify somebody, they may not object to their data being processed for that purpose. It comes down to the degree to which you are using that trigger and the proportionality and necessity. Have you looked at alternative mechanisms? Do not just jump up and down and say, "Can I use the internet to find out who you are?" A simple check of the pockets or if he has a business card, so you can go and contact his employer, might work better first time.

The Chairman: We appreciate the detail of your answers, but we will need to encourage some brevity, as well.

Q243 Stephen Mosley: A very simple question, and I apologise, Lord Chairman, but I am not a lawyer: is there actually a definition of "necessary and proportionate"? Is it quantifiable or is it measurable at all?

Angela Patrick: Effectively, in human rights terms, what you are looking at is if there is a legitimate aim. In the context of Article 8, there may be other issues but we are looking at what the purpose is for which you are proposing to do this, so prevention of crime, etc. You would look at the severity of the weight for saying that there was a purpose and a reason to do it, and then you would look at whether it was a legitimate aim. Is there any alternative means of achieving this goal? Have you looked at the safeguards to make sure there is no alternative risk?

I am sure Rachel might want to say something else about this as well, but there is a clear set of frameworks that look to show that somebody has actually conducted the balance between the goal at hand and the impact on the individual, in order to look at whether or not they can achieve their purposes through other means. If they cannot, that puts weight on justifying the interference. How serious is the interference at hand—i.e. are we looking at monitoring somebody's behaviour for months on end? Is it going to impact on his communications for a long time, etc? There are a number of different exercises you go through.

Q244 The Chairman: Could I stop you there? Has Justice got a little paper on proportionality?

Angela Patrick: We can help the Committee with that.

The Chairman: We will happily see a couple-of-page document setting it out, if we may. Dr Huppert, and I will now open the floor to everybody to participate.

Q245 Dr Huppert: Thank you, Lord Chairman. Can I just declare an interest, again as a member of the advisory council of the Open Rights Group and as a former member of Liberty's national council? I got to ask a question in the last session with the two of you, and there was not time for you to answer it. The transcript does not even include the "yes" that you said. One of the assumptions that has been made throughout this Bill is that there is a clear distinction between communications data—the who, the where, the how and so forth—and content. One of the Home Office's principles is that these are clearly separable. Are you all confident that they are, in fact, completely separate and will always stay that way?

Nick Pickles: For the record, the question I answered yes to was not that question. My answer to this would be no to do an opposite. No, and you will hear technical experts say this but, to use the example of an offshore service provider, if I connect to that service, my ISP knows I have connected to a service—let us call it Yemeni Mail. If they want to know who I have e-mailed within that service, which is the proposal of the Bill, that is content of the communication between my computer and Yemeni Mail. The idea that there is some simple distinction, and that is before you get into encryption and architecture, is disingenuous and misleading.

Jim Killock: Again, I do not think there is. I think the Committee should think of the idea of separating communications and content data, as is proposed particularly in the black box element of this Bill, as applying a sieve. If you imagine you have a sieve, everything has to go through the sieve and then you have to catch some of the communications data in order to establish what that communications data is. This is necessarily a little bit fuzzy. You are expecting and hoping that the algorithms and the computers that you are using are going to do this absolutely cleanly.

Also, often sometimes a communications event may well imply or tell you what the communications content is. For instance, a URL will tell you the whole of the content. If a website is a single URL, a one-page website, then retaining the URL of that will tell you exactly what the content is. Other times, it will tell you merely broadly what the content is. Perhaps if I read the *Sunday Telegraph* every week that pretty much tells you the content that I am reading. Similarly, if I read the *Guardian* every week that tells you something different. It either implies about content or, sometimes, it can be the content. In any case, in terms of what the Bill intends to do in terms of retaining communications events, you have to sieve everything in order to find the communication event details.

Rachel Robinson: In addition to the points James made there, there is also a conceptual issue here. To what extent does it still make sense to talk about communications data being separable from content because it is less revealing? That is the premise upon which these proposals are based. When we are talking about things like web addresses, how is that less revealing than something traditionally recognised to be content? That is incredibly revealing information.

Angela Patrick: Let me just reiterate that. The traditional description of communications data is "envelope data", which can be misleading. Actually, in terms of modern electronic communications, there is an awful lot that can be found out in terms of disclosure of the simple information that surrounds a particular communications event—where you are, where the person that you were speaking to was, how long you were speaking to them for, how much data you might have sent them, if you send people their photographs and various other things, and again web addresses. Even the Information Commissioner expressed his concern that you can learn a lot about somebody from their web history. It is

something that you would have to be wary of, but Justice would defer to others on the actual technology. The problem is, with Clause 1 being quite so broad, we do not even have the Government's explanation of how the technology will work. We have to be slightly cautious in terms of our being able to assist you.

Q246 Dr Huppert: Do any of you have any faith in the assurances that are in the Bill and the Home Office commentary that this will not allow for any access of content?

Nick Pickles: I assume the Home Office had not read the Bill with regards to postcards, because the last time I received a postcard the content was written on the outside of it. The Bill expressly covers material and data written on the outside of items transmitted in the post, and that is content. There are various other situations where the Bill is drafted in a way where data relating to content could be caught. The basic premise is there.

Q247 Lord Armstrong of Ilminster: When I was young, you used to think that what you wrote on a postcard was fair game.

Nick Pickles: I would agree with that, but I would also say that it is still the content of a message. If we are trying to distinguish the content and the communications data in that example, the Bill would apply to both.

Jim Killock: A postcard being fair game for your relatives is a different thing from a postcard being fair game for the security services and for private companies to log on behalf of the Government for future investigations.

Lord Armstrong of Ilminster: If I sent a postcard that had sensitive security information on it, I think I should be fully entitled to be found out.

Q248 Dr Huppert: Do you want to just comment on whether you have faith in the assurances? You do not have to comment on every question.

Angela Patrick: I was just going to add a very brief point, which is that, although we have problems trying to assess how much faith we should have, because we do not know what the technology is that is going to be used and we have not had the Government's explanations, even on the existing rules in RIPA, look at the Interception Commissioner's report, albeit that he only identifies a few mistakes. Mistakes there are, not least local authorities completely misunderstanding the type of data that they are allowed to ask for. Local authorities are expressly barred, on the face of the statute, from seeking data for purposes other than the prevention and detection of crime, but are expressly authorising themselves to get that data until, just by chance, the Interception of Communications Commissioner may have audited it and said, "Actually, you have asked for it and it is ultra vires. You should never have asked for it." Mistakes happen.

Q249 Dr Huppert: Can I return briefly to the way that communications data works? It is split in the Bill into traffic data, use data and subscriber data. Subscriber data we have discussed as being roughly equivalent to a telephone look-up. Actually looking at the Bill, it says it is information other than traffic data or use data held or obtained by a person providing a service about those to whom the service is provided. Would your reading of the Bill therefore mean that, if it was my Facebook account, that would include any posts I had made, any pictures I had put up or any likes I had made? Would that count as information held about somebody to whom the service is provided or would that count as content?

Jim Killock: It is subscriber details. A lot of this is subscriber details, because your profile on a service is all the set fields that you have to fill in, in order to create or maintain an account. On Facebook that would certainly include your date of birth, marital status, sex and age and so on, but also, as you say, the likes that you had made, the particular interests that

you had identified—quite a considerable amount of information that would really be content, except that it has been attached to your profile and is, therefore, in the terms of the Act, subscriber details. There is an obvious case to just slim that down to a number of set details that may be described as subscriber data.

Q250 Dr Huppert: That is very helpful. I will just ask one last question, and then move on and let somebody else ask questions, which is about the effect internationally of this. It would be interesting to get some sort of perspective. I know some of you have addressed this in your previous comments. Joe Biden, the Vice President of the United States, said that, where countries pursue monitoring arrangements, that could lead to businesses moving abroad to avoid those arrangements. Are there other countries that have techniques like this, which use black boxes like as proposed? Do we think there would be harms locally to our industry for having that?

Rachel Robinson: Our understanding is that the only countries that use this kind of DPI technology on a national level are, in fact, China, Iran and Kazakhstan. I know this was the evidence given to the Committee last week. We have not undertaken detailed comparative research but, on the basis of what we have established so far, we understand that is the case. We also understand, in a number of other countries—Egypt, Pakistan and Tunisia—DPI software is used at a local level for monitoring and surveillance of the population.

I think we have to be very concerned about our position here. Whenever countries in Europe, as I said in my introduction, are challenging the constitutionality of current arrangements, and given that this Government committed to ending the retention of data unnecessarily, we have to think about the direction that these proposals are taking us in, and also bear in mind that the current arrangements are subject to challenge and reference has been made to the European Court of Justice. It is something to bear in mind.

Q251 The Chairman: Which other countries across Europe are challenging them?

Rachel Robinson: Our understanding is that Germany has found the provisions to be unconstitutional, the Czech Republic, Bulgaria—and I am afraid the other two escape my mind, at the moment.

Jim Killock: Romania and Cyprus.

Nick Pickles: Ireland is challenging the existing the data retention directive in the European Court of Justice.

Q252 Stephen Mosley: I am very interested in Clauses 14 to 16, which establish this filter. It has been described as a filter by the Home Office people whom we have spoken to. You can probably look at it the other way around; other people might describe it as a search engine to go out there, pool all this data together and send the results out. What are your personal views on this and do you think the filter protects or impinges on an individual's privacy?

Nick Pickles: To refer to the earlier point, the filters highlight this change. Rather than having small amounts of data held that we pursue with a named individual or a named device, the filters are the way of bringing lots of data together to produce a result like a search engine would do, without necessarily requiring that data. One technique currently used is geoboxing. You say, "Here is a box on a map. Tell me every device, from this data, that has been within this area." The filters are intentionally the enabling part of the database function. Whether it is a central database or lots of little databases is irrelevant; the output to the officer is the same. Those filtering provisions are so broadly worded and so poorly drafted that they could allow mining of all the data collected, without any requirement for personal information, which is the very definition of a fishing trip. The metaphor someone else used is this will be fishing in

the sea with a net made of string. We will catch some small fish but the sharks will still carry on.

Rachel Robinson: I absolutely agree with the points made there, and I would just add that we are incredibly concerned about the role that these filtering arrangements provide for the state at the very centre of these proposals. These filtering arrangements will essentially join up the system of databases to create an integrated system. They will take the atomised pieces of communications data and form them into an incredibly revealing, incredibly full and detailed whole. In some circumstances, this will be done in order to establish the validity of the requests in the first place, before you have even established that the request is a valid one. That is a real concern for us.

Jim Killock: This area does create a very large number of potential risks, because you can remove people's privacy through several steps if you can match up data. You can attach a number of different identities to one person, for instance their mobile phone, their normal phone, their work e-mail, their personal e-mail, their Facebook account and so on. Then you can build up from that a map of all of their communications, both in time and, to a certain degree, in space as well because you have the geolocation data.

Because you can do that mapping not only against one person but other people, you can potentially identify people like whistleblowers. You can identify journalistic sources, and perhaps people who are worried about their legal position and are trying to consult somebody for legal advice. In all of those sorts of cases, where somebody might be either technically or actually breaking the law but, nevertheless, is acting in the public interest, they are going to be extremely dissuaded from taking action. That can have severe impacts, not just for exposing potential corruption within government, the police or elsewhere; it can also damage journalists' relations and their ability to report, and client/lawyer relationships. That is one set of potential risks that come from connecting this data up. I know that the Home Office is saying they are not going to use this data in this sort of way, but that is pure intention. The data will allow you to do this. I cannot imagine how they are going to be able to justify to themselves not using capabilities they have spent several billion pounds on.

The other set of risks comes from the ability to hack, which partly comes from the fact that you have got a distributed database and there are multiple access points, and these access points are available across the internet. You might think that I am sitting here saying, "What do you mean 'hacking'? This surely is not going to happen. We are going to be able to keep this data very secure," but I think we outlined in one example last week a little bit about what happened with Vodafone in Greece, in 2004, when the data of the Greek Cabinet, senior police officers and so on got accessed through a government back door that had been installed in the equipment that Vodafone had. It was hacked by persons unknown, and they got fined something like €70 million because of this data breach. The data breach occurred because the Government had asked their equipment provider, Ericsson, I think, to install back doors that they might want to use in the future. The back doors were not enabled because Vodafone or the Greek Government did not pay for the back doors to be enabled, but they were there and so somebody used them and we still do not know who. Suspicion lies with the US Government, but that is not a given.

The other example, which was in 2010, I think, was that Google had been asked to provide government back doors so that people could make surveillance requests similar to the sorts of things that are being proposed here. A number of people were attacked from China. Somebody from China, presumably the Chinese Government but I do not think anyone has conclusive proof, gained access to that data and obtained some of the e-mail records of Chinese citizens. I think it is believed that that was done for political reasons. Again, this was a government-mandated back door installed; it was meant to be secure, and was accessed by people who have criminal or political intent, from a foreign jurisdiction, which you have very

little control over. This is a real risk that has been created. When we talk about where the proportionality and necessity is for collecting data, we have to recognise that, in collecting data and creating access powers, we are creating genuine real risks to every citizen, if we are collecting data about every citizen. That is why, traditionally, surveillance is targeted at individuals. That becomes much more important in this data-rich world.

Q253 Stephen Mosley: You have highlighted some problems with back doors. Surely the advantage with this Bill if you legislate for it, if you put this filter in place, is that within the filter you can have security, you can have audit, you can have logging and all these things in the filter, so there is no need for back doors. Surely we should be trying to make sure that this Bill legislates for it all and provides the framework so that it can all be done legally, above board, without the need for back doors.

Jim Killock: How does a filter work without accessing a number of databases and comparing that data? Without a single database, how do you do that without there being a number of databases, all of which have access?

Q254 Stephen Mosley: There is one other area within Clauses 14 to 16 that concerns me. It does not actually specify who will own, run or look after this filter. In fact, it gives explicit power to the Secretary of State to transfer the functions to other designated public authorities. Have you any thoughts on that?

Rachel Robinson: We have concerns about that. There is the obvious uncertainty, which is a problem in and of itself, but there is the potential that this creates for filtering arrangements to be run by, for example, an organisation more on the front line even than the Home Office. That has to be a real problem in terms of operational involvement and the ability to impartially operate a service so central to the system. That is one concern. In terms of co-opting other authorities, the Information Commissioner, etc., into the system, they are effectively and should be a check on the system. Co-opting them into the system in that way would not, we feel, be appropriate.

Nick Pickles: Far be it for us to cast aspersions on the Home Office's ability to manage things they have contracted out.

Michael Ellis: I would not have thought that was appropriate. It was a contract with LOCOG, rather than with the Government was it not?

The Chairman: Let us move on.

Nick Pickles: I accept the clarification. I think the point is absolutely right that where you allow these filters to sit is central to the way that the information will be accessed and how the filters can be used. I return to my earlier point: who is stopping these filters being used for unnamed searches—for situations where certain profile criteria may exist? The purpose of the filtering is to show me who meets these criteria, rather than show me what this individual or device has done. That is the role of the filters. If that is anywhere near the front line, you have a serious risk of conflict of interest and of abuse.

Q255 The Chairman: Mr Killock, you said, without getting into conspiracy theories here, that it may have been the United States Government that leaned on Google to build in back doors to the Greek system. In view of the fact that Google and Facebook are giant American corporations and they have to keep the American Government happy, and the British Government is hoping that Google and Facebook are going to co-operate to give us, the British Government, the information we want, how concerned are you that our friends in Homeland Security may lean on Google and Facebook to give them the information as well?

Jim Killock: Certainly that is a considerable worry, and there is a lot of co-operation there. We have to be a little bit careful here. This discussion is actually about police access.

Other sorts of access are not especially in the scope in this conversation. I am not saying they are not of interest to you—they should be of interest to you—but in terms of trying to understand quite what the dynamics are, I think we should be a little bit careful to say this is about police investigations, Special Branch and other parts of law enforcement, rather than the sort of surveillance and access that MI5 in this country would have. They have a different regime, which I am sure we would be delighted to discuss, but I think it is probably a little bit broader than the Committee wants to take on, at this point.

Q256 Baroness Cohen of Pimlico: I have two questions, one of which I think you have answered. I think everybody is telling me that communications service providers are not going to be able capture communications data reliably and store it safely. I will just check that there is no dissent there. One of the objections always made by anybody to inquiries, or what they would view as repressive sorts of inquiries, is that criminals, terrorists and bad guys could easily and cheaply avoid the production of communications data. Do you have evidence of this? Is this a point that you guys would make or am I putting words in your mouth?

Nick Pickles: The Home Office accepts that they will still have a capability gap of 15%, even if this project is 100% successful. I would ask any government department to produce a demonstration of an IT project that has been 100% successful. The real nightmare situation is not the data being lost, in reference to the first part. The nightmare situation is someone watching it. If you are not interfering with the data, but you are watching who is communicating with whom, when and where, that information is extremely commercially valuable in terms of espionage, but also in terms of simple stock market manipulation. The nightmare situation is someone watching, not stealing.

Q257 Craig Whittaker: Could I just interrupt there? With all due respect, if people were going to do that, do they not have the capability to do that now anyway? Is that not a bit of a red herring? If somebody is going to do it illegally, they will get on and do it.

Nick Pickles: To use the example of a commercial webmail provider, they have an incentive to keep this data secure, because that is their business model. They will say, "If our security is breached, our product is less attractive." A CSP does not have that incentive. A commercial service provider does not have the incentive to keep data about your e-mail use secure, because they do not want to hold it in the first place. If that security breach did happen, the CSP's first response is, "We do not want to hold this data and we are being forced to hold this data by a Bill." There is a serious question to ask about the motivation.

The attacks referred to previously were aimed at Gmail, and Gmail largely resisted those attacks. Can the same be said of an organisation that does not have a commercial motive to protect that data? Indeed, it could be someone working within that organisation. There is a risk there to that data, a serious risk, so you have the risk of abuse of access, not just loss. On the second point, I will defer to colleagues.

Jim Killock: Sorry, what was the second point?

Q258 Baroness Cohen of Pimlico: The other point I was asking about was the general statement: "You might as well not do all of this, because criminals and terrorists will get away from it anyhow."

Jim Killock: There are two areas we are thinking about here. One is commercial services, which is the vast majority of internet communications. Then there are personal-to-personal types of communications, which might well avoid some of those commercial services. Most of those communications from one person to another person on the internet are done entirely securely not using commercial providers. Most of that is done by

business. Most of that is things like virtual private networks, where businesses want privacy and they do not want their information shared with third parties, so they avoid that.

The amount of communication that is done by citizens in that sort of way, where there is no record kept by a company like Google or Facebook, I am pretty sure is vanishingly small. It may get bigger or it may not, but I think that is something you need to hear from the technologists that you are talking to. My sense of this is that most ordinary communications are conducted through large organisations because that is where the investment is. Google invests lots of money in getting people to use Google, and so does Facebook. People like the services they provide, so they use them. Therefore, records are kept because they have them for business purposes. Therefore, law enforcement can get access to them.

The idea that we are getting a decline really needs to be spelt out by Charles Farr and colleagues at the Home Office. I would just point out that the Home Office's own paper says, as I mentioned in my opening statement last week, that there is an assumed 1,000% increase in data going across networks. The Home Office accepts that. When they say to you, "We will only have 65% of the data rather than 75% of the data," what they are saying to you is, "In 10 years, we will have 650% growth if we have nothing, but we want 750% growth." Their statistics pretty much bear that out. We need to know what exactly that 100% growth they are not getting entails, and why it is that they might find it difficult to access that, given the huge commercial availability of communications networks.

Rachel Robinson: In addition to the very sophisticated potential methods that have been mooted here for potentially evading or getting around the proposals set out in the Bill, there are also methods of very little sophistication that could potentially be used to get around these proposals. For example, there is the use of a pay-as-you-go mobile phone with an anonymised SIM, so the possibilities for evasion range from those with very little sophistication to very sophisticated encryption and anonymisation techniques, hijacking the unsecured networks of others, etc. It is a wide range of problems.

Jim Killock: I might add that one of the rather better known techniques for avoiding government surveillance is Tor. Tor is largely paid for by the American security apparatus, or has been, largely because they want to enable Chinese dissidents to avoid surveillance from the Government there. It cuts both ways at all times.

Q259 Lord Strasburger: I have some questions about safeguards to prevent misuse of data. I think we may have strayed into these areas already, so we might be able to get through these quite quickly. There are concerns about the potential misuse of communications data. Do you consider that the draft Bill seeks to address these adequately and do you have any evidence of any abuse under the current RIPA safeguards?

Angela Patrick: I will start off, because I think I will be very brief, but the others can deal with the technical issues. Our starting point, to repeat what I said earlier, is not necessarily about abuse; it is about the expansion of retention and collection. As we know, when you expand the amount of information you keep, it becomes more difficult to manage. The likelihood that you are going to have mistakes—not misuse necessarily or abuse, which is a potential problem but not necessarily the major one—increases when you expand the potential for error. You have to look in great detail, if you are going to expand, and we do not know how, why or what. We are a bit concerned about what the actual expansion will involve, and we are very concerned that no justification has been provided so far.

When you are looking at that expansion, you have to look at what the safeguards will be and nobody has told us what they will be. Actually, it is incredibly difficult for us, as informed commentators, to try to help the Committee understand the risks, not only of misuse but of error. We have to simply look at the fact that these databases, as much as they will be automated and otherwise running on various programs, may themselves be fallible. They will

be designed and run by human beings to a certain degree. We all know that, when it comes to data, people do make mistakes, often very costly ones for those who have simply had their data stored. They may never have known that it had been stored, but now may have the concern that it is either in the ether or sent elsewhere, with no knowing who has it.

Q260 Lord Strasburger: With respect, we have heard all that before. If you could concentrate on the safeguards and whether you think they are adequate, that would help us.

Angela Patrick: The problem is we do not know what the safeguards will be, because we have not been told what the technology is going to be and we do not know how it is going to be stored, except that there is going to be some agreement between the Government and CSPs. We heard the point made earlier that it is okay because it is not a government database. It is private companies managing data that, as my colleague has said, they have no real commercial incentive to keep. Actually, the question is: do we trust the private sector to keep these databases secure? If we do, what is the detail, where is the trust and what are the safeguards that are imposing on them obligations to ensure that there are protocols in place not just to avoid misuse but to minimise error?

Q261 Lord Strasburger: Do you have any evidence of misuse under RIPA?

Angela Patrick: The best evidence we have is the Interception of Communications Commissioner's reports.

Lord Strasburger: Your best evidence is the lack of evidence.

Angela Patrick: There is a lack of evidence, but also look at the mistakes that were self-identified. There are not many of them; I think the figure is 900 across law enforcement agencies. They identify that they are fallible.

Jim Killock: I have one quite interesting piece of evidence. Obviously the public authorities now report most of the time. That is the evidence we get, but one of the complaints that has been made about the current access regime has been that Google does not comply with enough of these requests. I think they have been turning down something like 30% or 40% of the requests made to them. Why have they been declining 30% or 40% of the requests? Because they have been inadequately framed; they have not been signed off by officers. It is not because they think that they are entirely inappropriate and they will not deal with them; they just send them back as poorly formed. If that is the case, Google has given us the only real example of how these requests are statistically performing; we do not really have that as quantity from the Interception Commissioner's reports, because they just give numbers and do not tell us what the sample size is. If Google is correct in saying they have to return 30% or 40% because they are badly formed, we have some evidence that this is not working very well.

Rachel Robinson: In relation to the first part of this Bill and data collection, in terms of safeguards, all we really have are empty assurances or requirements that data needs to be kept securely, without more. That is a cause for concern. That stops us from scrutinising, potentially, the safeguards envisaged by the Government. In terms of access arrangements and other parts of the Bill, many of the safeguards proposed are process-related—formal requirements, for example, that the requisite individual would be named in a notice, etc. There is very little in the way of substantial safeguards there.

Nick Pickles: The very definition of abuse is sketchy, because the problem is that if, currently, an officer views acquiring data as necessary and proportionate, it is by definition not abuse. As we heard the other day, there are police officers who think it is necessary and proportionate to use this data for road traffic offences. Is that an abuse? No, because the process was followed and the criteria are satisfied. Is that a fit use for a surveillance infrastructure not used in a democratic state anywhere else in the world? I would say that is

not a fair use but, by definition, the officer said it was necessary so it cannot be abuse in the legal sense.

Q262 Lord Strasburger: Thank you. Some of you have suggested that the powers in the draft Bill might put off whistleblowers or endanger privileged communications, such as with lawyers. Do you think these are real risks, despite the permitted purposes and the authorisation regime? Are there additional safeguards that could be introduced to lessen these risks?

Nick Pickles: 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. Indeed, there is no recognition for privileged communications with MPs. I understand the Home Office has still to respond to concerns about the Wilson doctrine with regard to this legislation, which were clearly raised, given that a constituent contacting a Member of Parliament would have their e-mail recorded. There is a clear issue there. I would defer to colleagues on that for further points.

Jim Killock: We are speculating and we need to really understand and see precisely what the filtering arrangements in particular reveal. I would point to Ireland as an example of where this has occurred. The cases being brought by Digital Rights Ireland, I believe, involve individuals whose data was abused. There was a recent article in the *Guardian*—I will send the details of that to the Committee—where again there have been cases of journalists and police finding data incorrectly used and inducing some degree of a culture of fear among some of those groups. It is entirely possible, once the data is collected, for that sort of thing to arise. We have to firstly understand what the proposals really are. I do not feel those details have been explained to the Committee and us. Then we have to start to understand how the data that is being collected might actually be interrogated. We certainly see, in other countries, some indications of how it can go wrong.

Q263 Craig Whittaker: At one end of the scale, we obviously have the Government, police and security services saying they have a need. At the other end, we have you guys, who I think are saying the Bill is not fit for purpose. What would you suggest we do to make it fit for purpose?

Rachel Robinson: The answer is that we just do not think the case has been made for these types of proposals. When you are embarking on a human rights assessment of these proposals, you have to look at the revealing nature of the information, of course. Then you have to look at potential law enforcement gains. The idea or the suggestion that these proposals will lead seamlessly to gains in law enforcement is something that we would challenge. We are told that, in 95% of serious criminal investigations, communications data plays a role. We are not told, however, how many of those investigations lead to successful prosecutions and what kind of a role communications data played in those prosecutions. Was it central? Was it peripheral? Were there other techniques that could have been used in order to get the same point?

Q264 Craig Whittaker: In your opinion, then, nothing would make this fit for purpose.

Rachel Robinson: In our opinion, the data retention arrangements that we already have in place are very hard to reconcile with the protection of personal privacy. The blanket retention of data about individuals, as opposed to targeted surveillance, with which we have no problem, should not be a feature of a liberal society.

Craig Whittaker: In your view then, absolutely nothing can change in this Bill to make it fit for purpose.

Rachel Robinson: In our view, the basic provisions set out in this Bill—take away reference to access and scrutiny, which basically replicate current provisions—are to require communication service providers to retain data that they would never keep for their commercial purposes, as essentially an arm of the state for these purposes. We do not think that that can be justified.

Craig Whittaker: No, then there is nothing that can be done to make this Bill fit for purpose.

Rachel Robinson: Yes.

Q265 Craig Whittaker: What about the other witnesses?

Angela Patrick: We are concerned that, basically at Clause 1, we just have not seen the evidence, not least that we do not quite know what the scope of Clause 1 is. If the assumption is that, reading it as drafted, it creates a very large power to, as Ms Robinson said, collect pretty much any information that passes from anybody through a CSP, then that is a big ask. Actually, what you have to do as a Committee, and as an objective observer, is look at what this gets us. What does it gain? We have quite a wide gateway provision in RIPA already. What you are talking about is adjusting the ask to the evidence that it is needed. The problem we have is that we have not seen the evidence from the Home Office, other officials and data users for why this vast expansion is justified.

Q266 Craig Whittaker: What would you do then? What would you suggest?

Angela Patrick: If you were asking me to rewrite the Bill, I would drop the first part and read our report on RIPA. Do not expand the collection and retention of data; just up the existing safeguards in RIPA to perhaps make it fit for purpose in the first place.

The Chairman: That was very clear and concise, thank you.

Jim Killock: The problem we have here is that we do not have a clearly defined problem to give an answer to. What we have is a bald statistical statement that access to communications data is going to grow by 650% rather than 750% or, if you want to phrase it the way the Home Office does, it is going to decline from 75% to 65% access.

Q267 Craig Whittaker: Could I ask you, yes or no? What would you do, if anything, to make it fit for purpose? If you do not think it is fit for purpose, could you make it fit for purpose or do we just kick it out?

Jim Killock: Given that we do not really know the problem, it is an incredibly hard question to answer.

Craig Whittaker: With all due respect, you have a lot to say on this Bill to say that there is very little information in it.

Jim Killock: There are a lot of implications from what the schemes appear to entail—that is to say filtering, databases, connecting databases, extra powers to collect—but there is no indication of what precisely is being targeted and why. It seems to me there are two things going on. Firstly, the Home Office believes that, by connecting data up and being able to make queries against it, they will gain some very nice, extremely intrusive, revealing and important-for-them new powers, which they do not really wish to discuss with the public and tell us that it is about maintaining capability. That is one reason why they are doing it.

Secondly, there is some possibility, given that they are saying that there is this gap between what they might access and what they are currently going to access, that they are finding it difficult, in some circumstances, to get hold of communications data that exists. But when we ask what that communications data might be, we get told things like, "We do not really want to discuss that, because that will help people hide themselves." Without that information, trying to fix this Bill is very difficult. There is probably something in trying to

develop better relations with overseas companies, understanding how it is that they get data, whether the legal regimes are sufficient and whether police officers understand how to get that data from overseas companies. There is a bunch of questions like that.

Q268 Craig Whittaker: In your view then, it is not fixable.

Jim Killock: No.

Nick Pickles: The Bill is not fit for purpose and that was the view that I took. It was also the view that the current partisan Government took in 2009, when they opposed the same thing.

Craig Whittaker: What would you do to fix it or would you not fix it at all?

Nick Pickles: It requires the monitoring of every communication made by everybody in this country.

Craig Whittaker: Would you fix it or would you not fix it?

Nick Pickles: It is distinctly undemocratic, so I think it should be thrown out.

Craig Whittaker: You think this should be thrown out. Thank you.

The Chairman: We must be brief if we can. We are running rather late.

Q269 Michael Ellis: Just briefly, in fact there was a difference in the Labour proposals of 2009, was there not, Mr Pickles? That called for a central database whereas this does not. I would just correct that.

Nick Pickles: I would challenge that immediately. If you have a look at the 2009 consultation document issued by the Home Office, it states quite expressly the Government rejects a central database, and the Information Commissioner welcomed that in their response to the 2009 consultation.

Q270 Michael Ellis: As far as what the problem is, the mischief that this Bill is attempting to redress, all of you tended to say that you do not see what the problem is. Is it not obvious, and have you not now heard the accounts of others, that technology has moved on? Communications data has moved on. The authorities are saying they can no longer monitor in the same way that they used to be able to, when it was landlines and mobile telephones. There has been a degradation in their monitoring ability. They want to stop terrorists and criminals from committing offences. That is obviously the case of what they are trying to achieve, is it not?

Jim Killock: It needs to be really spelt out exactly what that means.

Michael Ellis: Hold on, Mr Killock. You have said that, but you also seem to want the authorities to tell you and your colleagues what it is that criminals do to avoid detection, so that anyone listening to this Committee who has bad faith in mind can use those tactics to avoid criminal detection.

Jim Killock: Under current data retention, we know exactly who retains data and what. We know precisely which ISPs are retaining logs and exactly what are in those logs. When it comes to the inaccessibility of data, we need a bit more than assertions. An assertion that goes around Parliament a lot is, "What about Skype?" That is quite an interesting one. Skype is peer-to-peer, so calls go from individual to individual. Presumably they do not produce data trails, but Skype is also an application owned by Microsoft. There are some centralised parts of their network and there are back doors built into it. I am afraid that, in order to understand what this apparent capabilities gap is, we are going to have to hear what types of communications are not being accessed in what circumstances.

Angela Patrick: I just want to add that we started our research that we did—and I will provide that to the Committee—on the basis that we thought there were problems with RIPA. Part of it was that technology had moved on. That is where we were in the 1970s; we were

saying, “Gosh, technology is racing ahead and the privacy laws are not keeping up.” The question is: technology is racing ahead but that also means that what you could be looking at are vastly greater powers to monitor individual activity by capturing data. For example, we used a very facetious example at the start—envelope data. It does come from “Let’s track who sent what letter to whom,” or how the telephone exchange knows who is speaking to somebody else. That is a very limited amount of information—who called whom when, who wrote to whom when, what their social communications are, how often they speak, etc., but technology has advanced in such a way, as we have explained, that we can tell where you were, how much information you sent to each other, how often you met and what your history on the internet was. It is a changing pattern, and we would not like advancing technology to be used to mean that we are depreciating the amount of data we can collect. It is simply that advancing technology is perhaps opening up avenues for surveillance. The question for parliamentarians must be: what avenues are appropriate, proportionate and necessary?

Q271 David Wright: Can I just turn briefly to the monetary costs and benefits of these proposals? You may have seen the previous evidence that we have taken, where Home Office officials have given us estimates of the net cost of the draft Bill. They are saying it will be £1.8 billion over the next 10 years. Do you think that is realistic? Secondly, what do you think about the net benefits figure that they have calculated of £4.4 billion? Again, do you think that is a realistic figure?

Nick Pickles: I might note firstly that I formerly worked for an IT contractor, at the time when the Public Administration Select Committee was producing its report into the rip-off culture in IT. I would urge the Committee to read that report if they are interested in how IT contracts are procured. The Minister could not even bring himself to say at the Dispatch Box that the £1.8 billion estimate was accurate. The Parliamentary Question from Duncan Hames MP asked about that; the Minister could not say so. We have also asked the Home Office to provide details of the breakdown, so both the cost and the benefits, and where they fall. We have been told we cannot have this because it affects commercial interests, security and law enforcement, which is surprising given that the majority of the benefit falls on HMRC. I cannot quite see how tax returns are either commercially sensitive or, indeed, security or law enforcement. I would merely refer to the Government’s own IT strategy, which says there is a presumption against IT projects over £100 million, because they do not work.

I would refer to the fact of whether there is a competitive market. No, because, as we have heard, suppliers do not know what they are supplying. Is Government an informed buyer in this situation? Again, I would refer to previous IT projects. Will this software be non-proprietary, so available and integrated? No, because, as we have previously heard, suppliers will only be told in certain instances what they are building. Finally, will it integrate with the existing legacy estate? As the Public Administration Select Committee looked at, the Government has no interest in understanding this because it will cost too much. In answer to the £1.8 billion of costs, I will eat any hat if it costs £1.8 billion, because it is simply not true; it will not happen and the idea that this will come in on budget is simply remarkable.

Q272 David Wright: Your view is it will be a lot more than that.

Nick Pickles: I think it will be a lot more by a factor of 10 at a minimum.

David Wright: How much risk will the private sector bear?

Nick Pickles: From past experience of government IT projects, very little. From every IT contract ever produced, and indeed if you look at the National Audit Office reports today into the Home Office’s management of the Border Agency, weak leadership and poor project management remain a hallmark of public sector procurement. I see no signs of that changing

anytime soon. This would make history as the first government IT project to come in on budget, on time.

David Wright: What you are saying to the Committee is that you estimate 10 times the cost that they are quoting.

Nick Pickles: When the first proposal was floated in 2009, estimates were actually £18 billion.

Q273 David Wright: Anybody else?

Jim Killock: I do not know that I can say exactly what the costs will be. You need to hear a lot more again from the Home Office. We need those breakdowns to understand precisely what the proposal entails and where the potential cost overruns might be, but the fact that Charles Farr, who proposed the interception modernisation programme under Labour, sat here and told us that black boxes were not a particularly big concern for this Bill tells us that he has put his ambitions, and the Home Office have put their ambitions, for large-scale data collection through black boxes on the backburner. Now, that may well be because money is a little bit tight right now. It may well be, especially given the fact that the Bill is an enabling Act that allows new collection duties to be imposed over time, either directly on service providers or through these collection procedures and black boxes—either route—that you could easily see new categories of information being included, new duties of retention being included and the Bill going up, purely because people say, "Here is another thing we want. Here is another thing we want." Over time, you end up with a scheme that looks remarkably similar to Labour's original proposals and the costs look remarkably similar, even though the promise originally was rather less ambitious. I think it is promising a lot to say that this is going to stay.

Rachel Robinson: The only thing that I would add to that very comprehensive answer is that, as technology develops, there is a great deal of technological opinion to the effect that the costs of adapting infrastructure to deal with new technological developments will be great, endless and constant. That is a real concern.

Q274 David Wright: What about the cost of the additional regulatory regime that was being proposed earlier? One of the things you were suggesting—I am changing tack a little here—is that you wanted greater oversight, for example through the judicial process. Have you got any estimates of any additional costs that would be incurred, if we had further judicial oversight, in terms of giving permission to search for data?

Angela Patrick: We have not extrapolated that. There is some data in connection to the extension of judicial oversight to local authority decisions under RIPA. I am sure that, if you wanted to ask for that information, the Home Office could compile it by extrapolating the costs that have been incurred by local authorities asking magistrates, as opposed to going through the traditional administrative route.

Jim Killock: One cheap point for the proposals that some of us have raised is the idea of notification. As you are hearing from the police and so on, there are going to be times when notification should not occur; somebody who has been investigated should not be notified because they are going to be under continuing investigation or are suspected in that sort of sense. Simply telling people that they have been investigated and their data has been supplied is not going to cost very much at all. That could provide a lot of evidence about abuses, if particular populations are being profiled, if particular individuals are being somewhat hounded or if the investigations were just simply inappropriate. That might be a very cheap means of proving transparency, if you like.

The Chairman: We need to move on, Mr Killock. It is an area of interest we wish to explore, but not right today. Anything else, Mr Wright?

David Wright: That is it. Thanks, Chair.

The Chairman: Thank you very much. I am sorry we have overrun horribly, but thank you all very much. We could have gone on much longer interrogating all of you and getting the excellent information from you, which we will chew over. Please send us, those of you whom we have demanded them from, the papers we have asked for. Thank you all very much for giving your evidence today. Could I ask you to move quite quickly, so we can get the next evidence people in? Sorry for being so rude, asking you to move quickly.

Examination of Witnesses

Professor Anthony Glees, Director, Centre for Security and Intelligence Studies, University of Buckingham, and **Dr Julian Richards**, Co-Director, Centre for Security and Intelligence Studies, University of Buckingham

Q275 The Chairman: Welcome, gentlemen. Sorry for keeping you waiting but, in nearly all our evidence sessions we seem to run a bit late. We find them fascinating and we interrogate at length. For the record, could you state who you are and your position?

Dr Richards: I am Dr Julian Richards. I am the Co-Director of the Centre for Security and Intelligence Studies at the University of Buckingham.

Professor Glees: I am Professor Anthony Glees, and I am Director of the Centre for Security and Intelligence Studies at the University of Buckingham.

Q276 Lord Strasburger: Professor Glees, you stated on the "Today" programme in April that one of the arguments for the proposals in the draft Bill is that it needs to be done because it can be done. Why does the ability to access communications data necessarily mean that public authorities should be able to access it?

Professor Glees: In a radio interview it is not easy to get an extended argument across. What I meant by that was this: if there is unregulated space, and there is, and if this unregulated space is used for criminal purposes, and it is being so used, and if it possible to mine such space to make it regulated and to apprehend criminals, then it should be done. That is a very straightforward issue; it is not 50 shades of grey. It is a black and white issue for me.

Q277 Lord Strasburger: What limits do you think need to be applied to state intrusion into people's private data? Are there, in your mind, no limits?

Professor Glees: There are limits, but what those limits are is a rather deep philosophical question. The other way of looking at this is to look at the sorts of regulations that exist—for example, the Acquisition and Disclosure of Communications Data Code of Practice in its 2007 version, which I have read with interest and care. That seems to me to be an excellent way of ensuring that the correct boundaries are kept. As I say, 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. As I say, in my view the correct way to look at it is to ask yourselves what the codes of conduct are—the ways in which practice is regulated. I think, in the documents that I have seen, it is extremely well regulated and that people should not be afraid of this.

As I say, at the end of the day, what this is about for me is the introduction of some kind of lawfulness into cyberspace. It is self-evident that something that is already being done should be done in areas where it can be done and needs to be done. That there is this public disquiet about this so-called "snoopers' charter" seems to me to be not an issue that has anything to do with the facts before people, but is rather about a more general and, indeed, disturbing lack of trust in politicians and the people charged with looking after our security—the Director General of MI5 and head of the Metropolitan Police. These people are not trusted when they say they need these things. I think that is very disturbing, but it is not a reflection on the things they say they need.

Q278 Lord Strasburger: Do I take it then that you have no problem with content being collected as well?

Professor Glees: As you know, this is not about what; it is about who, when and where. Of course, content is a legitimate source of information but, again, as you know, people who want to intercept communications—that is to say gain access to content—have to go a completely different route. I think that is right. I think privacy is important. I am aware of Article 8 and the other aspects of the European Convention on Human Rights. That convention is extremely important but, in the real world of today, it seems to me entirely unacceptable that, like those people who rail against CCTV, people feel that they should be allowed to conduct criminal activities on the internet—that somehow it is a free space and it is a part of civil liberties and human rights that they should be able to use that free space for all sorts of wicked things from terrorism through to paedophilia and money-laundering. You know all the categories as well as I do.

Q279 Lord Strasburger: You would not be happy for content to be collected.

Professor Glees: Content is not addressed in this Bill. Yes, I am happy for content to be collected where it meets the very stringent different regulations that are required if content is to be looked at, i.e. a Home Secretary's warrant. It has always been like that. We have had a secret service for more than 100 years in this country. It has always looked at these sorts of things. What has changed is everybody's desire that this activity be made lawful and be brought into the law. That is very important. We need secret services. We give them a job of work to be done, yet they need to do it lawfully and they need to be accountable for what they do. As long as these things are all in place, I am perfectly satisfied.

Q280 Dr Huppert: I am struggling to understand some of what you are saying. When you talk about this being a philosophical question about the limits of state intrusion, actually it is what this Committee has to essentially determine and advise the Government and Parliament on. It is not just a sheer question of philosophy. You have been talking quite a bit about regulation of the internet and making things lawful online. I hope you realise that this is also not about regulating the internet, which is a different issue, involving a whole range of other Bills. It is that question about state intervention.

You mentioned people who describe this as a "snoopers' charter" or who are concerned about CCTV. Can you explain to me how the argument that you made, either on the "Today" programme or just now to Lord Strasburger, would not apply to a proposition, say, to put a CCTV camera in every single room to monitor what happens, just in case it is useful? I think we would all agree that that would be quite useful in terms of reducing crime. I suspect, around this Committee and most of Parliament, most of us would agree that it was not the right thing to do. How does your argument differ from that?

Professor Glees: I am a professor of politics as well as somebody with a special interest in intelligence-led activity. I am sorry if I have confused you; that has not been my intention. As I say, I think the philosophy about what is private and public is a very difficult area. In Parliament, I do not have to talk about things that particular MPs may or may not have done on the internet to publicise their activities. When I came into this meeting on the train from Bicester North, I suddenly heard the voice of Boris Johnson booming at me.

Dr Huppert: You may have some issues about that, but that does not quite address the question.

Professor Glees: I will come to it; I just want to give you the context. The philosophical aspects of privacy are very important. Am I suggesting that there should be a Big Brother CCTV in every room? Of course not. In my view, the people who make this claim are living in cloud-cuckoo-land. If I may, I will just give you some statistics. In 2003, I wrote a book about the East German intelligence service, commonly known as the Stasi. If you have a look at a real surveillance society, which is what communist East Germany was, in

1989, the last year of the Stasi's existence, there was one Stasi member to every seven East German citizens. In Britain today, there is one MI5 officer to every 7,000 citizens.

Q281 Dr Huppert: Professor Glees, clearly your book should be on all of our summer reading lists, but I still have not understood your principled argument as to why you are saying: "There is wrongdoing happening online; we could collect information about it, hence we ought to." That is, as I understand it, the argument you are making, but the same thing does not apply when there is wrongdoing happening in rooms and we could collect CCTV information on it.

Professor Glees: The quick answer has to do with proportionality. Something does not become acceptable if it is done in private. A criminal act is a criminal act, whether it is done in somebody's sitting room or whether it is done in front of Parliament here.

Q282 Dr Huppert: Whereas you were arguing that it should be done because it can be done and could be useful, you now say that in fact it is about the proportionality. Your argument is not about whether it is possible to collect this information online, from postcards or anything else, but whether it is proportional or not. Is that your new position?

Professor Glees: Sorry; I will repeat myself. When being interviewed by John Humphrys, or whoever it was, at 8.10 in the morning, you do not have time to develop a sophisticated argument. What I tried to set up was the point that there is this space; there are these things going on in this space. They are criminal things. It is now possible to at least have a go at finding out more about the things that are going on in this space. If it is possible, as it is, and if bad things are happening in this space, as they are, then it should be done. Of course it is a question of proportionality. If you are asking whether I think that councils should spy on people who put out the wrong bin, no, of course not. That is an absurd argument. It is the consistent attitude of what I would call the civil liberties lobby to reduce this argument to the absurd. This is not a matter of 50 shades of grey; this is something that is being done with existing communications. I am told that, every day, on average, each person in the United Kingdom sends four text messages.

Q283 The Chairman: Are they on criminal behaviour or criminal matters?

Professor Glees: I do not think they are on criminal matters, but I am just trying to make the point that this is a new form of communication that is being used. Thirty million people communicate with each other every day on the internet.

The Chairman: And you would collect all of it from everybody, because, somewhere out there, there are some people doing bad criminal things.

Professor Glees: Not only would I not do it, but it would be impossible to do it. That is the point.

Q284 Lord Armstrong of Ilminster: Many of us would agree that it was acceptable to have public authorities access communications data in the interests of pursuing terrorism or counterterrorism and serious crime, but the list of purposes is not 50 shades of grey but 11 or 12 shades of grey. Do you think that it is right that all of these purposes should be permitted by this Act? I know it is taking over from RIPA, so it already exists, but the Government appears to have shown some signs of wondering about that, because on the face of the Bill they have reduced the number of agencies that can collect and given themselves power to extend it to other authorities, so that people have to make a case. There is also the question of the purposes and some of the purposes are non-serious crime. Would it be justified or proportionate to use these powers for the pursuit of bicycle theft, which is a crime? Other

purposes here are not criminal at all. Are you content with the list of purposes as it exists or would you like to change that?

Professor Glees: Well, Lord Armstrong, what I would say to that is what you have already said. These powers were in RIPA in 2000. By all means, one should always have a debate about what should and should not be looked at. I would say from my vantage point, on the one hand you have people like Sir Tim Berners-Lee, the father, as we all know, of the worldwide web, and adviser to the Government, who in April this year said allowing this sort of data-mining would lead to "the destruction of human rights". Then you have people like me, who say that a human right is also to be secure. A human right is also to be able to walk down your road without fear of being mugged, or for children to go into a park without being accosted by drug dealers. Forty years ago, there may have been a copper on every street corner and in every public park. That is not the way it is these days. If CCTV, for example, can prevent crime and criminal activity then, yes, I am absolutely for it. On the question of proportionality, yes, I understand that, but again I point this Committee to things, for example, that David Davis MP has said.

Q285 The Chairman: Lord Armstrong was asking, of the permitted purposes, would you concentrate just on serious organised crime, terrorism and protecting the economic welfare of the state? Would you dump the other items on safeguarding public health and allowing people's dead bodies to be found?

Professor Glees: I am happy with that.

The Chairman: Are you happy to dump the others?

Professor Glees: I am happy with it, but obviously the most important things are the things that come first—the things that involve serious organised crime, terrorism, paedophilia and matters like this.

Q286 The Chairman: Dr Richards, for Lord Armstrong's question**.**

Dr Richards: I actually do have concerns that the range of purposes for which these powers might be used is too great. I would personally restrict it to serious organised crime including terrorism, and possibly certain emergency situations where lives are threatened, such as kidnappings and so on. I personally feel that the complete list, in which there is provision for collecting taxes and so on, goes too far, in my book, because these are very intrusive capabilities and I am aware of privacy concern. Proportionality, for me, means that only the most serious of crimes are legitimate purposes for doing this.

Q287 Baroness Cohen of Pimlico: Either Dr Richards, Professor Glees or both of you, under current legislation, a large number of public authorities have access to communications data likely to be replicated using order-making powers. Are you concerned by the length of the list of organisations? Should the powers be limited entirely to the police and security? There is a fairly long list of other organisations. If you or Dr Richards think that the sorts of things you can ask should be limited, do you think the sorts of organisations that can ask them should also be limited?

Dr Richards: The short answer for me is yes; I think the list is too long. I think the capability is absolutely necessary, in my view, for preventing serious crime, including terrorism and so on. I do think there is a red line that this list perhaps crosses, in my view.

Baroness Cohen of Pimlico: Would you limit the list to police and security/intelligence services?

Dr Richards: I think I probably would, yes.

Professor Glees: Could I just say that I do not agree with my good friend and colleague? I think that victims of crime have a right to be safeguarded as much as is possible.

It is very easy to say that fly-tipping, for example, is not a major thing, but if you live in a beautiful place, as my wife and I do, and it is defiled by people dropping their rubbish there with impunity, why should that be allowed? I am a zero-tolerance person. The argument that there are some things that are perfectly all right—you can beat your wife at home with all the doors locked so that nobody can hear the screaming, but you cannot do the same in the street—is anathema to me. I do not think lawmakers should be in the business of saying, to come back to David Davis, that the people who are going to be caught with this new legislation are stupid criminals. Criminals are criminals. Whether they are stupid or bright is of no concern to me.

Q288 Lord Armstrong of Ilminster: I share your views about fly-tipping, but is it appropriate for fly-tipping to use these powers to have access to communications data? I think that is the question that is in my mind. I would love to stop fly-tipping.

The Chairman: That was the question I was going to ask, but Lord Armstrong phrased it much better. We all want to take action against fly-tippers, but would you use the powers in this Bill to do so?

Professor Glees: You have to use the powers that you have.

The Chairman: Yes, but we are here to decide whether we should have these powers.

Professor Glees: Unlike my good friend and colleague Dr Richards, I am comfortable with them, but obviously, as always in life, you have to prioritise. There is a limited amount of people to do this. There is a limited amount of funds, and they should go to dealing with the most important issues first. There is no question in my mind about that.

The Chairman: It does not seem to have stopped some of the organisations in the 552 with access requests from finding the priority to do some of it.

Q289 Stephen Mosley: On those 552 organisations, there are only four listed on the face of the Bill. Do you think there should be more listed on the face of the Bill, or do you think that they should just come along afterwards through delegated legislation or something?

Professor Glees: Bearing in mind the public debate that has taken place, and bearing in mind that this is about the wellbeing of the public, the more that is set down and the more that is listed, the better. In a mature democracy, it is absolutely right to be having this sort of debate. Again, I pay my taxes, to the best of my knowledge, and I claim my expenses properly. If the use of communications data, which is currently not kept, would enable more people to stick by the law, I am in favour of it. This is the 21st century.

Q290 Michael Ellis: Gentlemen, can we come on to the issue of preventing inappropriate use of communications data? That is assuming, Professor, that you accept that there is a possible inappropriate use of such data. Would you accept from me that there is always a risk of misuse of power? We give constables the power to arrest people; there is always the possibility that that power will be abused. Here there is a risk of misuse. Would you say that it is proportionate to take certain risks in order to prevent crime and detect offenders? Would you say, therefore, that the terms of this Bill are proportionate? When coming to the issue of preventing the abuse, how would you propose to ensure that inappropriate use of communications is actually prevented?

Professor Glees: If I could deal with the second bit first—but I will come to the first bit—I think that the right way to prevent abuse is, first of all, to have proper regulation and a proper code of practice. As I said, I have read the Acquisition and Disclosure of Communications Data Code of Practice; I think it is a very good document and I am very happy with it. But there is another side, particularly where we are dealing with the secret world of intelligence. That is oversight and parliamentary oversight.

I am extremely concerned by what I regard as the failure of the Intelligence and Security Committee to play any role in this debate or, indeed, any serious role in any of the issues that have affected secret intelligence-led activity in Britain over the past few years. Our first port of call—by "our" I mean the public—should be to the Intelligence and Security Committee to find out whether the Intelligence and Security Committee and its Chairwoman are content with the appropriateness of proposed legislation. We are in a position, as I say, where we do not hear anything about that. That is why people like myself have to say the things that we do.

Q291 The Chairman: If I can elucidate slightly, I think you will hear, probably by 30 November, from the Intelligence and Security Committee, which will be conducting a parallel investigation to ours relating to the use of communications data for the Security Service.

Professor Glees: Forgive me if I say perhaps it has come 10 years too late, but better late than never. I know that it is proposed that the Intelligence and Security Committee be reformed. It is high time that it were reformed.

Michael Ellis: I think there is a White Paper about that.

Professor Glees: To go to your first point on the risk of people misusing the data, of course there is a risk. We saw it in the papers on Saturday: people can suffer because of wrong or unlawful behaviour.

Michael Ellis: You are referring to people who were wrongly arrested because of communications data errors.

Professor Glees: Yes, and that is wrong. Nobody in my position would seek, for one moment, to justify it. Just as the police will investigate people who are then found to be perfectly innocent, and that is not an argument for saying police should only investigate people who they know are guilty, so too, when it comes to communications data, we should not let the abuse of this in a very small number of cases indicate that this is not a worthwhile activity.

Q292 Michael Ellis: Briefly, Dr Richards.

Dr Richards: There are two things here and they are very important. One is the question of the capability that you have in place to extract the data. The second is the question of the process that you have in place for using that data. Sometimes, in a lot of the debates around this subject, the second aspect is forgotten or missed by some of the critics. There are some very rigorous procedures in place for accessing and using this data in a properly authorised way. Already there are procedures in place under RIPA that ensure, in my view, that, although there were always risks of misuse of this data or using it inappropriately, those risks are greatly minimised.

Michael Ellis: You would take the risk in order to resolve the mischief that the Bill is seeking to control.

Dr Richards: If you have in place a rigorous and appropriate process, then yes.

Q293 Michael Ellis: Finally from me on that point: do you think the penalties that are available are appropriate for those who would or could fail to comply with the requirements of the Bill? For example, for offences that might include the Computer Misuse Act, misconduct in a public office and the Data Protection Act, do you think those penalties are appropriate?

Dr Richards: Yes, I do, and I do not particularly see any need to change them. Those things are in place for a good purpose.

Michael Ellis: Do you agree, Professor Glees?

Professor Glees: Yes, I agree.

Q294 Mr Brown: May I just follow that up? You are both academics. You have made a study of this area. One of the great constraints on people taking part in wrongdoing is that they will be caught and punished. Are you able to say anything to us about people who take information from the police computer and sell it for commercial gain, or public servants who look up people's social security or medical records and sell them for gain? Do you know how frequently this is done and how often it is prosecuted?

Professor Glees: No, it is not something I have done research into.

Dr Richards: No. Again, I return to what I said just now: there will always be risks that this can happen in a system. You have to put in place procedures and processes, firstly, to minimise the risk of it happening in the first place and, secondly, to monitor what is going on and to have the appropriate penalties afterwards, if that does happen. I have some personal experience of working in an intelligence situation where we used to make these sorts of requests for these sorts of data, previous to my academic experience.

Q295 Mr Brown: Do you accept that a principal fear in the minds of our constituents is that information about them will be improperly accessed, improperly used and may be improperly sold to somebody else? The biggest safeguard against that is that somebody who does such a thing will be caught and punished.

Dr Richards: I accept that people will have those concerns and I understand those concerns. Again, all you can do is try to reassure people that the appropriate procedures are in place to minimise that risk greatly and that people are held to account afterwards, if it goes wrong.

Mr Brown: You both believe that they are.

Dr Richards: I believe so, yes.

Professor Glees: You are talking about very serious offences. They are already serious offences. I would simply make the point to your constituents that their interests are better safeguarded in regulating this part of the cyber domain as far as possible. By "regulating", I mean allowing it to be examined for the purposes of fighting crime. They are better served than by letting it be a kind of Wild West, where there is no lawfulness. People are far more likely to steal data from you or send you fraudulent e-mails if they think that they will not be traced. If they will be traced, they will not do it.

Mr Brown: I certainly agree on that point: that to make the law more effective, you have to capture people who break it and bring them to justice.

Q296 Lord Strasburger: We are talking here about safeguards against misuse. You both seem to be perfectly content with the safeguards that exist in RIPA. We have heard, in this Committee, of one known case of a prosecution, over several years, where there have been 0.5 million applications for data a year. Let us say that, out of 5 million applications for data, there has been one case of misuse identified. There are only two possible explanations in my mind, although you might be able to come up with another one. Either the safeguards are as immaculate and watertight as you seem to believe or the abuses are not being detected. Which do you think it is?

Professor Glees: For me, this comes back to the first point, which is trusting the people we charge to look after this area.

Lord Strasburger: Excuse me, but are the safeguards not there to check whether we are right to trust them?

Professor Glees: The statistic you have quoted, and I have not done the research into it, could be taken both ways. It could be taken to mean that there is a very small risk, or it

could be taken to mean there is a massive cover-up and the public do not understand. I am inclined to believe that the people who do this—the head of the Met, the Director General of MI5 and the head of SOCA—do it with the right intentions.

In my experience, if I may say so, and in my work, if there has been a problem about intelligence-led activity in the United Kingdom, it has not been that it has been too interventionist; it has been that it has not been sufficiently interventionist. Things have not been found that should have been found. If you accept that and you accept that, in a lawful mature democracy such as ours, you have to place trust in the people charged with directing these matters, that statistic that you quoted to me bespeaks good news, not bad news.

Lord Strasburger: I am very happy to trust these people, but I am going to check to make sure that I am right to trust them.

Professor Glees: Of course there should be accountability. This is oversight.

Q297 David Wright: On that very point, clearly within the Bill it is not the head of the Met who is making a decision about what data is gathered. It is actually much further down the chain than that. Do you think that there is a need for more judicial oversight within the process? We have heard evidence already that requests for data inquiries really ought to be signed off, at least by a magistrate. Do you agree with that?

Dr Richards: No, I do not, for two reasons. Firstly, if the process is followed correctly, then, even though the authorisation is given within the public body itself, it should all be logged and recorded. Those logs should be available to the Interception of Communications Commissioner for auditing afterwards.

Q298 David Wright: Dr Richards, let me just break in there. What happens if you get an organisation with a canteen culture, where somebody goes along to one of their friends down the corridor and says, "I need some data on this particular individual or about this particular device and, I tell you what: don't put it down under that level of request; stick it down under this box here, so that it does not show up on any monitoring report, so there is no data"? It comes back to this point about people abusing the system. It is far more difficult to do that if you have to present evidence before a magistrate, is it not?

Dr Richards: My experience is that, firstly, that sort of culture just does not exist in these bodies.

David Wright: What, nowhere? It does not exist in any organisation?

Dr Richards: I do not think it does. Secondly, if you have designed the system correctly, every request you make of an IT system is logged. Records are kept of what data you have pulled, when you pulled it and why you have pulled it, if it is designed correctly. I believe that you can design a system that can appropriately audit and monitor these things, if you design it correctly. The second point I wanted to make is that there is an operational imperative here. We heard the sorts of numbers of requests that need to be made to pull this data every year to support intelligence operations.

Q299 David Wright: Hang on. The scale for intelligence organisations is a separate point. We are not talking about the number of requests we have got. There is a lot of dispute about what those requests are for. One would imagine that, if there was some element of oversight from a magistrate, it would actually reduce the number of trivial requests for data, if I can use that phrase advisedly.

Dr Richards: It probably would, but I still think the scale of requests that the police and the intelligence agencies would be needing to make every day would be such that, for there to be judicial sign-off on every single request, the whole thing would grind to a halt operationally.

Q300 Mr Brown: Can I just ask it the opposite way around? Do you think that the magistracy is a sufficient safeguard and a necessary one just for the local government requests?

Dr Richards: Yes, although, as I said earlier, I am not entirely comfortable that local government should be using this data anyway.

Q301 David Wright: What we are saying is that a local authority has to go to a magistrate but that other organisations do not.

Dr Richards: I guess we are saying that, yes.

David Wright: And you support that.

Dr Richards: The implication from your question is that then you have a willy-nilly unregulated, unmonitored regime. That is certainly not the case. Procedures are in place to log and monitor. If the Interception of Communications Commissioner's office is doing their job correctly, they have access to the details of every single request that is made and have the right to audit that at all times. There should not be provision for willy-nilly searching of data.

Q302 David Wright: Do you think there is the capacity in that organisation to deal with that?

Dr Richards: There needs to be. There should be. It should be built into the system.

David Wright: "Needs" and "should be" are different things. Whether it is is a different matter.

Dr Richards: I would take that as a necessity for this regime to be properly administered.

David Wright: Is it able to do that now, do you believe? On the basis of what is in this proposed Bill, would it have the capacity to deal with that now?

Dr Richards: Yes, it does.

Professor Glees: I think it probably does, yes.

Q303 Stephen Mosley: Clause 1 of the Bill gives the Home Secretary the power to specify what data is held, who holds it and what equipment they use, but it does not actually give any more detail of how they will do it or what they will actually ask for. Do you think it should be more specific there?

Professor Glees: In dealing with that question, it allows me to add my ha'p'orth to the answer that Dr Richards has given to the previous question, which is that I think that we need more oversight. There is no doubt in my mind about that. If members of the Intelligence and Security Committee should in future consist also of senior lawyers, I would be delighted—senior academics too, as far as I am concerned. The way this Committee is organised at the moment—that it lies in the hands of the Prime Minister to decide who should be members of it, any Prime Minister—I think is wrong. We all know that the police computer is, from time to time, abused by police officers. We know that. It has nothing to do with this new legislation; that is the way it is at the moment. That is wrong.

Q304 The Chairman: Professor Glees, sorry to interrupt you, but can I just clarify something with you? You said you need more oversight, and then you talk about the Intelligence and Security Committee. Less than 2% of the requests of the 0.5 million requests relate to the Security Service, so we are looking at 98% of these requests relating to ACPO and the police. Do you think there should be more oversight there, which would be the responsibility of the other Committee?

Professor Glees: I think that, as far as the acquisition and disclosure of communications data is concerned, yes, there should be more oversight. Generally, there should be more oversight over data-mining and formal interception. Who does it? As I say, we all know there is reform in the air; we do not quite know who is going to do it. That is part and parcel, as is accountability. At the end of the day, I think we have to trust the people we charge with doing this and there have to be very severe penalties when that trust is abused. It is my understanding—I have not done a study of this but it is my understanding—that where police officers misuse the police computer, they are subject to very serious penalties.

Q305 Stephen Mosley: From that, in terms of this Bill, you think it should have a bit more detail—yes or no?

Professor Glees: Yes, more detail, absolutely.

Q306 Stephen Mosley: Dr Richards, one of the concerns we have heard about is in terms of black boxes. Is there any evidence to suggest that black boxes would be needed and do you have any concerns about introducing these into the mix?

Dr Richards: There are two elements to this issue. One is a technical element, and I will confess straightaway that I am not a technical expert on telecoms networks. The other is a risk and security issue. On the technical issue, my limited understanding is that, because the telecoms network is becoming so dynamic, diverse and complicated, the way this data could have been collected before, when you had particular pipes that everything went down and you could put a tap on to them, is no longer technically feasible. Stuff is flying around all over the network in a very dynamic way. I believe there are technical reasons why a more dispersed system of collecting this data is necessary but, as I say, I am not a technical expert and you would need to speak to other people about that.

In terms of risk, clearly any situation where you push sensitive equipment—and this is obviously sensitive equipment handling sensitive data—and disperse that greatly out of secure locations and into the telecoms network, yes clearly the risk goes up that something will be compromised, hacked into or there will be privacy issues. We have to weigh the balance of the technical need to do this in a particular way and the need to protect it as far as possible.

Q307 Stephen Mosley: One of the other new innovations within this Bill is the filter. What are your views on the creation of a filter? Effectively, to me it sounds like a search engine, which effectively will mine all the data that is out there and almost make it into one virtual database. Is that your opinion and do you see any risks with that?

Dr Richards: To the front end, to the analyst who is pulling the data, yes; in a way it will look and feel the same. By using this filter mechanism, it will look and feel the same as if there was a great big database behind the scenes that you could dip into to pull the particular information that you want. However, for operational reasons, it does not seem to make any sense. These intelligence questions that are being asked of the system about people's communication behaviours and patterns are quite complicated questions that require several different pieces of information to be pulled together and analysed, in a fused way. It does not seem to make sense to make that as difficult as possible, by saying you have to get this bit from over here, then you have to get this bit from over there, then you have to get that bit from over there. That just reduces our intelligence capability to the benefit of the terrorists and the criminals that we are going after. I think it is null issue in a way. If you are collecting the data, then how you query it, to a certain degree, to me does not pose any more risks than anything else.

Q308 Stephen Mosley: I can see some advantages to using a single filter to do these searches because, as you said, it provides one place for security, for auditing purposes and for logging purposes. Would you think that that would be an advantage?

Dr Richards: Operationally, it would be a massive advantage. Yes, that is what you need to do at the end of the day; you need to combine lots of different pieces of data together to give you an intelligence picture of what you are looking at.

Stephen Mosley: It might be an advantage to channel all the inquiries through the filter. I think, looking at the Bill, it is saying that they will do the inquiries normally, but only more complicated ones would be put through the filter. Do you think there would be an advantage to having only one access point effectively, which would be the filter?

Dr Richards: There probably would be, for all the operational reasons that we have discussed.

Q309 Stephen Mosley: Lastly, the Bill gives the power to the Secretary of State to transfer the ownership, the maintenance and the running of this filter to a third party. What are your thoughts on that?

Dr Richards: Again, it may be a technical question. I will refer back to some of the comments I made earlier. As long as you have the appropriate authorisation process and monitoring regime to ensure that everything is being done in a legally compliant way, so that you can monitor and audit logs to make sure that people are using the system appropriately, then I do not necessarily see a problem with that. It may be that the Secretary of State's office is not the best place, technically or logistically, to be able to run this system anyway. As long as you have the sufficient safeguards in place, I do not necessarily see that this is a problem.

Q310 The Chairman: Dr Richards, the Home Office has called it a filter, giving the impression it is narrowing down the information sought. I think Mr Mosley has called it a search engine, giving the opposite impression. Whose description is the more accurate, in your view—a filter or a search engine?

Dr Richards: My understanding of it is that "filter" is a slightly inaccurate word for this, because you are filtering lots of different pieces of information out of the system and putting them together.

The Chairman: Mr Mosley is right: it is more of a search engine, in your view.

Dr Richards: That is my understanding of it, yes. That is actually a more accurate description.

The Chairman: You agree as well, Professor Glees.

Professor Glees: I do, yes. I am not technical at all, but it is my understanding that a filter does exactly as Mr Mosley says.

Q311 Dr Huppert: You have both looked at approaches to communications data collection in other countries. There are a variety of different approaches. Are there any around the world that use the approaches proposed within this Bill?

Professor Glees: My understanding is that the Australian Government is closest to the United Kingdom in terms of this particular Bill. The country that I know most about, apart from the United Kingdom, is the Federal Republic of Germany. There, the German Chancellor is on record as having said, in her view, Germany needs similar legislation.

Dr Huppert: As I understand it, Germany currently does not have any aspect of the data retention directive, so they are somewhere behind and trying to catch up to where we were years ago.

Professor Glees: For historical reasons, not just because of the Nazi past but also because of the Stasi past, this is a very much more difficult issue in the Federal Republic than it is in the United Kingdom, where we look back with pride on our long history of democracy.

Q312 Dr Huppert: Indeed we do. Germany is way behind and would like to catch up to where we are now. You say Australia is sort of roughly where we are but trying to move a bit forward. Are there any countries around the world that currently collect communications data, or try to collect communications data, in the way envisaged in this Bill?

Professor Glees: To the best of my knowledge—I suppose the moment I say this someone is going to disprove it—there is no proper research into this. The distinction that would be made would be between the 27 member states of the European Union and the states of the European Economic Area, which share a common understanding of this problem, and then countries outside there. Obviously in a place like North Korea you would expect that they would take a very different attitude. That is why I come back to saying this is about lawfulness in a mature liberal democracy.

Q313 Dr Huppert: I suspect North Korea would say similar things about lawfulness. Do you agree, for example, with Joe Biden, the Vice President of the United States? He argued that, where you have monitoring arrangements like this, which impose some technological drag through back compatibility and various other areas, they might lead to businesses moving elsewhere in order to avoid them. As long as there is a difference in different countries as to what you have to do, there is an incentive not to be covered. Do you think there is a risk that companies may choose not to be in the UK, to do less activity in the UK, to store data overseas or something like that?

Dr Richards: I personally do not think there is a big risk there, for two reasons. One is that the telecoms network is a global network. It is very dynamic; it is very transnational, not just technically but in terms of its management as well. Whether you locate in one country or another kind of becomes less significant technically. Also, there are other reasons why, as a telecoms company, you might want to locate in the UK. There are particular fears about this interception capability, particularly given that it is supposed to be Europe-wide, and I know that lots of other EU countries are way behind in implementing this.

Dr Huppert: Sorry, Dr Richards, but this legislation is not EU-wide. The data retention directive is EU-wide.

Dr Richards: The directive that underpins it, theoretically, will eventually appear in other parts of Europe, if countries implement it appropriately. I do not know; I think that any fears that telecoms companies might have over this impacting on their business would be mitigated by the other economic reasons for whether or not you would want to locate in the UK.

Q314 Dr Huppert: Just so I understand, you are saying the system is incredibly dynamic and so telecoms companies could easily move, but they will not choose to do so, so does it not weaken our benefits? If you are saying there are economic benefits to being here, does it not at least weaken them?

Dr Richards: What I am saying is I do not think you do sufficiently, because there are other reasons for why you would locate in one or other country that greatly outweigh that issue.

Dr Huppert: You weaken them but not enough. I think I understand that.

Professor Glees: I think there is an ethical dimension here that should not be forgotten. That Mr Biden may have made these comments as an American does not impress me. We have seen a big company like Amazon, for example, managing to avoid paying tax

anywhere in the world, as far as one can tell. This again is a consequence of the lack of regulation of the cyber domain. I would argue strongly, looking maybe at the banking crisis and various other things going on, that the idea that unregulated space leads to economic success is extremely dangerous.

Q315 Dr Huppert: Again, Professor Glees, we are not talking about regulation; we are talking about data collection, which is very much not the same as regulation.

Professor Glees: To me, regulation means the imposition of legal norms and laws. That leads to regulation.

Dr Huppert: Professor Glees, the laws still apply; the question is about how you collect the information, which is not the same as regulation. A room that does not have a CCTV camera in it is still subject to the same laws as one that does. It is still regulated in the same way; it is just a question of what tools you have to go out and collect the information.

Professor Glees: It is a good philosophical argument but, as I say, the American pressure, which is that somehow, of all forms of communication, the internet should not be subject to lawfulness, I would say, is not something that should be seen as being of great economic advantage, except to the particular companies that are able to exploit it. We have seen where that ends.

Q316 Dr Huppert: We will hear what a number of the companies have to say about this later. Do you think there is a risk that, when you collect data into any sort of database, whether it is a central one or a number of other ones, you create a honey pot—that there is an incentive now for people to try to attack that data to get hold of it? Do you accept that as a risk—that you are generating a new source of crime?

Dr Richards: In terms of cyber-crime you mean?

Dr Huppert: Yes.

Dr Richards: Potentially, yes, but it is a risk you have to consider against the benefits that you get from accessing the data. Again, going back to that technical point earlier about whether, if it is implemented in quite a dispersed way, you disperse that risk, if it was all sitting in a lovely nice database in Cheltenham or wherever it may be, in some ways that risk would be higher.

Dr Huppert: There is a fascinating tension between one very secure location and a number of potentially less secure locations, and I think I understand the argument.

Professor Glees: The starting point is that the crime is out there. The crime is not made by the fact that this is data that can be mined. That does not make the crime; the crime is there. Mining the data might diminish the crime.

Q317 Baroness Cohen of Pimlico: Can I start with Dr Richards? People always suggest to us that, whatever regime is put in place, criminals and terrorists will evade it with the utmost ease. Since your background has to do with terrorists, do you think that is right and, if so, is there any evidence that shows they can evade this? That is what I am after.

Dr Richards: Yes, criminals and terrorists are very well aware that they are being monitored. They are the masters at trying to evade such monitoring, as far as they possibly can. That has happened throughout history. The suggestion that criminals and terrorists could easily outwit these sorts of mechanisms is greatly exaggerated, in my view. The only way to really avoid being monitored by the authorities is not to use any electronic communications at all. That is the only way you can be sure of doing it.

Baroness Cohen of Pimlico: Back to the carrier pigeon.

Dr Richards: Absolutely. Yes, there are ways. One of the things about the internet is you can appear on it very anonymously, but people have to communicate; they have to use the

services that are there, otherwise nobody knows who is talking to whom. I would say there is a limit. Yes, they will make it as difficult as possible, but they will not make it impossible to be tracked, in my experience.

Q318 David Wright: We have heard quite a bit of evidence from the Home Office team about monetary costs and benefits from these proposals. I would welcome your thoughts on them. We have heard estimates that the cost of the draft Bill will be £1.8 billion over the next 10 years and there would be £4.4 billion of net benefits. What do you think of those costs and benefits?

Professor Glees: I am not able to comment, I am afraid, on that aspect of it. All I would say is that estimates of costs and benefits are always going to be matters of speculation. That is all I would say; I have no expertise.

Q319 David Wright: Dr Richards, have you got any experience on this?

Dr Richards: I would broadly say the same. From a technological point of view, the proposals that flow out of this Bill are technologically very complex. To be able to do this physically entails some cutting-edge technology, which probably will cost a large amount of money, probably in the order of billions rather than millions. Whether it is £1.8 billion I just could not say; I just do not know.

Q320 David Wright: We have heard suggestions this afternoon that it would be up to 10 times more than that.

Dr Richards: I just could not comment on that. If we are talking £18 billion, that seems an extraordinarily high figure to me, but I just do not know what it would entail. In terms of the benefits, again I am extremely suspicious of any official figures on this. I think it is impossible to put a figure on how much you save the country by winding up criminal enterprises, capturing terrorists and so on. We see all sorts of figures bandied about. The National Security Strategy said that the annual cost to the UK from crime is £1 trillion. Where that figure comes from and how they have calculated it I just do not know. Particularly when we are looking at cyber-crimes, given that we do not know how much cyber-crime is actually going on, how you can put a figure on it I do not know. This is a very fraught area and, in my view, anyone who gives you an accurate figure is dubious.

Q321 David Wright: You are not aware of any academic modelling that has been done outside of the Home Office or other government departments on the benefits of this type of activity, more broadly.

Dr Richards: I am not aware of that, no. In fact, the only academic debate I am aware of is the fact that you really cannot trust any official figures on this.

Professor Glees: I think one policy aspect of cost is that any Government needs to be cautious about private industry trying to sell it software, at huge expense, that claims to do the filtering that we have talked about. In our own work, we are aware of the pressures on Government from what used to be called the military/industrial complex—the big companies that are very busy wanting to sell stuff. In respect of that, without trying to put an inappropriate plug in for our own work at the university, there are some things that the state has to do. The provision of security is one of the things the state has to do. The people who need to do this sort of work should be properly employees of the state and trained to do that. I do not think this is the sort of technical work that should be farmed out, because that would be a huge cost and a huge expense. To the best of my knowledge, both our Security Service and the Government Communications Centre and busy trying to recruit the young talent that they think can do this sort of work at the moment, and I think that is the right way to approach it.

Q322 The Chairman: Professor Glees, could I take you back to the point you have just made on being suspicious of suppliers willing to supply the sophisticated kit? As I understand it, one cannot go to PC World and get a range of this. There will be a monopoly supplier doing a specially designed bit of special kit. We all have experience of Ministry of Defence contracts that go to two, three or five times the cost, and then the generals always want to add an extra button just before the thing is delivered, putting the cost up again. Have you a view, therefore, on a monopoly supplier of this equipment? Are you suspicious of the cost estimates?

Professor Glees: Yes.

Dr Richards: Yes. As I said earlier, you are absolutely right that this is an extraordinarily complex technology that you cannot buy off the shelf. There are cost implications in that and cost risks for the Government.

Q323 David Wright: I am not a technical expert, but presumably this piece of kit will have to interrogate different private sector databases, which may be constructed in different ways. It will have to be adaptable to a number of private sector organisations' structured databases.

Lord Strasburger: Which are changing all the time.

Dr Richards: My limited understanding is that, yes, there is a huge array of different types of data, which is the problem, but the data rates are the problem. The amount of data flowing through the network is extraordinarily high and right at the upper limits of current computing technology. Those are the sorts of issues that you have got here.

Q324 Stephen Mosley: Has any assessment been made of how much data will be collected over the period of one year?

Dr Richards: Not that I am aware of. I would imagine, within the appropriate parts of government, within GCHQ and so on, they would have some sort of estimate of this. Whether that is disclosable, I just do not know. I have not seen anything publicly.

Professor Glees: Of course, we know the figure for last year, which I think was 550,000 requests to examine data.

Stephen Mosley: That was not the question; it was how much data is being stored over this process.

Dr Richards: I would think that would be known. The telecoms companies themselves know how much data is flowing over their networks, but I do not know. It is a lot.

Q325 The Chairman: Dr Richards, would you be aware of which countries in the world would be capable of making these black boxes and this sophisticated kit?

Dr Richards: Some of this gets into quite sensitive technologies, which I am not qualified to comment on. There would be a small number of countries that could do that.

The Chairman: Do we have the capability in the UK, do you think?

Dr Richards: I believe so, yes.

Q326 Mr Brown: Do you believe that, eventually, there will be an overarching European Union regulatory regime in this area? Do you believe the approach that the last Labour Government and the current coalition Government are taking, because they are broadly similar, would be compatible with what is emerging from the European Union?

Professor Glees: It is my understanding that the answer to that is yes. It is a critical area of co-operation with our European partners. Of course, if we were to leave the European Union, as some people say, that is something you could throw out of the window, but at the

moment we do seem to be, all of us, talking the same kind of language, subject to the same kinds of directives and underpinned by the same convention on human rights. That is good, in my view.

Q327 The Chairman: Unless any colleague has got any other question, could I conclude with this one? I think, Professor Glees, you said, "Of course, subscriber data is only who, what, where," but as I seem to be learning, it is not actually just who, what, where; it is who, what, where, when, the details of your bank account, every single thing you may put on your private Facebook account, your home address—everything under the sun could technically be subscriber data. Is that correct?

Professor Glees: I am afraid, if I said that, I misspoke. What I thought I said was that what this is about is "who, when and where", but not "what".

The Chairman: Sorry; my apologies. Yes, you did say that.

Professor Glees: I know people in the civil liberties lobby say, if you are looking at "who", you are looking at "where" and you are looking at "when", you are bound to also see "what", but again I have trust in the people we charge to do this. They say that it is not about "what".

Q328 The Chairman: I accept that. Let us forget about the "what". I misspoke there, if I said "what". What I was trying to get at is that subscriber data, as I understand it, is not just who, what, where. It is not just the person's name and their telephone number; it is a huge range of material, including your bank account number, including all of the information that you have to give to Vodafone, Virgin, Facebook or Twitter when you sign up. That is subscriber data.

Professor Glees: Yes, absolutely. Again, we know that that kind of data not only exists but is most massively exploited, not by any government agency or council or authority, but by the people who sell things to you on the internet. It is a fact of life.

The Chairman: For business purposes. That is a different question. Can we be clear then that, when we say, "Subscriber data is only who, what, where," it is not technically just who, what, where? It is who, what, where and an awful lot of other stuff.

Professor Glees: My concerns are related to this proposed Bill, and there it is very clearly stated that this is not about "what". One can believe or not believe it as one chooses. I choose to believe it.

Q329 Lord Armstrong of Ilminster: I think I got from the previous session objections from the civil liberties people that the "what" included so many things that it was tantamount to content. Of course, it is the "what" that gives the authorities the clues that they want to pursue their criminal investigations. Have you any thoughts about the point that the Chairman makes about the extensive subscriber data and the borderline between that and content?

Professor Glees: Where the civil liberties lobby, if I could describe them thus again, come at this from is the idea of a snoopers' charter and a surveillance state. For them, the starting point is that there is this great bank of data that will be mined arbitrarily, and that will affect each and every individual. If you come at this from the point of view of the Government and the agencies, this is about particular searches for people who may be involved in serious crime, or may be threatening suicide or risk of life. You all know the categories. There it is about finding about with whom they have communicated, when they have communicated and where those communications have taken place.

Lord Armstrong of Ilminster: Which tells you something about what they are talking about—or may do.

Professor Glees: The “what” will trigger the specific investigation, but what is being mined is not the content, generally. It is not a surveillance-state operation; it is a targeted operation.

The Chairman: Unless you have any other comments there, Dr Richards, thank you once again, gentlemen. We have grossly exceeded our time with you as well. I am sorry for keeping you back so late, but thank you very much for again an excellent evidence session, which we will chew over carefully. Thank you very much.