HOUSE OF LORDS

HOUSE OF COMMONS

ORAL EVIDENCE

TAKEN BEFORE THE

JOINT COMMITTEE ON THE DRAFT COMMUNICATIONS DATA BILL

DRAFT COMMUNICATIONS DATA BILL

TUESDAY 23 OCTOBER 2012

HENRY PORTER, DUNCAN CAMPBELL AND PAUL HERITAGE-REDPATH

KEIR STARMER QC

Evidence heard in Public Questions 750 - 839

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.

Oral Evidence

Taken before the Draft Communications Bill Committee

on Tuesday 23 October 2012

Members present:

Lord Blencathra (Chairman)
Lord Armstrong of Ilminster
Lord Faulks
Lord Jones
Lord Strasburger
Mr Nick Brown
Michael Ellis
Dr Julian Huppert
Stephen Mosley
Craig Whittaker
David Wright

Examination of Witnesses

Witnesses: **Henry Porter**, Columnist for *The Observer*, **Duncan Campbell**, IPTV, and **Paul Heritage-Redpath**, Product Manager and Solicitor, Entanet Opinion, examined.

Q750 The Chairman: Gentlemen, thank you so much for coming to give evidence before the Committee today. Clearly, the Bill we are considering has provoked a wide range of interest and some comment in the press, and we wanted to make sure, before we concluded our evidence-taking sessions, that we gave members of the press an opportunity to tell us about the Bill and their perceptions of it and their views on it. We are very grateful. Now, although we know who you are, it would be helpful, please, if you just introduced yourselves for the record.

Henry Porter: I am Henry Porter. I am a novelist. I work as a contributor for the *Observer* and I am London editor of the American magazine *Vanity Fair*.

Paul Heritage-Redpath: Good afternoon. My name is Paul Heritage-Redpath. I am a solicitor and a product manager for an internet service provider called Entanet.

Duncan Campbell: I am Duncan Campbell. I have been an investigative reporter for 35 years and I have also been an expert witness on communications for nearly as long. Over the last decade, I have extensively audited and tested communications and computer data in the criminal courts. In terms of my journalism, reports that I published in 1980 and evidence I provided to the European Court were part of the trigger for the judgment in *Malone v UK*, which led to the Interception of Communications Act. Much later on, I was the expert witness and instructed by your next witness, Keir Starmer, in the 2008 European Court case of *Liberty & other organisations v the United Kingdom*. I have made sure that a copy of that case is in the hands of the Committee because it specifically considered issues of filtering in the context of communications collection and analysis and found the UK's practices to be non-compliant.

The Chairman: Excellent. Thank you very much. Our Committee members will have a range of questions for you. Do not feel you all need to answer every single one unless you wish to, but again do not be constrained and hold back.

Q751 David Wright: A gentle opening to the bowling, if you like, to ease you in at the crease. The media coverage of this proposed legislation has been, I think you could say, unrelentingly negative. It has been described as the "snoopers' charter" by many. Do you think that is a fair analysis of what has been proposed, because we have certainly taken evidence where witnesses have said they felt that the media coverage relating to this Draft Bill has been inaccurate?

Henry Porter: I do think it is fair, because I think it is a very bad Bill and it threatens the very foundations of our liberal society, and if you come from where I come from, which is a profound belief in our democracy and the ways of a free society, you see this Bill as a very great menace to it. So, even if the coverage is unrelentingly against this Bill, I do not think it is necessarily unfair.

The second point I would make on this is that we have to hold Government to account. Now, the media often comes in for a lot of flak itself: the BBC today, newspaper journalism throughout this last summer and last year. But the fact is we still have this important job to do and it will make it a great deal more difficult to do this job if the communications of sources in Whitehall, in politics, or in big companies can be traced to journalists. So that is another reason, and perhaps the secondary reason, why the media is probably very against this Bill, but I would say that the first reason is that it is hostile to the sort of society that we have now.

Duncan Campbell: I found it difficult to hear the Home Office complaining of unfairness when what they are putting forward to Parliament and this Committee is something that has really been stewing around for at least 10 years, being pushed forward in various ways, and yet when the witnesses come here it seems that no one in the telcos knows what they plan to do or how they will implement it. I was also gravely concerned that Mr Farr in his evidence, and within almost his first interchange with Mr Ellis, completely misled the Committee about the situation with communications data. I put a note in to expound on this should it be necessary, but the statement that 30 years ago BT was collecting communications data, and the implication that they will now not be making that sort of information as available, is the exact opposite of the truth. So, he is extremely badly informed, and passing on poor information and misrepresenting the situation as it is seen now in terms of the amount of information that is available, which has been increasing. It has been increasing as devices become available and new forms of data, for example location and cell-site analysis, come into the system. So I see the Home Office as having mis-served itself very badly from the very title of the presentation of the Bill as remedying a gap. No, they are not. Perhaps proportionately there are things that could be done, areas that can be addressed, but they have left themselves wide open to this accusation of it being a snoopers' charter.

I would not quite endorse that title yet, because what they are creating, if Parliament were to give them the powers in this form, would really be a universal surveillance engine attached to the mass or all of the British internet. Now, what you do with it, and whether it does become a universal snooping engine, is withheld from us, because none of the orders, none of the codes of practice, none of the facilitating instructions, some of which may come to Parliament, some which may remain classified, are before us. So, again, given the degree of obscurity, the surveillance engine could be the snoopers' charter or it could be reined in.

I would just, finally, say that the important point of human rights, which seems to have been overlooked in the way the Bill was drafted, has been formed. It has been formulated for us by the European Court and really supports the apprehension that perhaps is seen as coming too stridently from some journalists. "The mere existence"—and I am quoting now from the judgment—"of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users," which

is Henry's point and I would absolutely and strongly endorse that for the special case of journalists seeking confidential sources and secure communications to them when those sources act and come in the public interest. The Court finally said the mere existence of legislation of this type is an interference with Article 8 rights irrespective of whether there were to be measures taken against an individual person. So that is a very powerful legislative Act, longstanding in the European jurisprudence, that really does go to help understand why epithets like "snoopers' charter" have had widespread currency.

Paul Heritage-Redpath: I would say that the newspaper coverage has been, if anything, relatively balanced on this issue, because this is something that strikes at the heart of human rights, and I do not think the Home Office have done themselves any favours in the way that they have presented or engaged with it. I think the newspaper coverage has been limited by the fact that it is quite difficult to articulate to the public what lies behind this Bill and I believe that is a deliberate intention.

As a communications provider, we have had no contact from the Home Office. As a member of the association of communication providers, we invited the Home Office to speak to all of us collectively. They spoke for half an hour and they told us absolutely nothing more than you would find in the Notes on the Bill on the grounds of national security. Now, this is something that strikes at the heart of how we operate as an industry, and I think the fact that they will not articulate it to us means that the press articulating that to the public is very difficult.

Q752 David Wright: So your view, as a panel of witnesses, would be that far more groundwork could have been done by the Home Office in terms of background detail. One of the things we have struggled with as a Committee, Mr Campbell, relates to your point, which is about understanding what lies beneath this legislation: what will come to Parliament at a later point?

Duncan Campbell: Yes. I can address it both as a journalist and I can address it from the bottom of the pile, if you like. What is it that my police colleagues would like to be bringing into court that they could get from communications data that they do not now get? There are relatively few things, given the richness of material from other sources, and if you take, for example, whether we can go to Skype, it has been laid out that there is a completely alternative route for going to Skype, so we do not need to worry about Skype in this context.

They have also eschewed looking at things that could be simply explained to Parliament and public. Way, way, back, 12 years ago, we were working on Chapter 2 of RIPA and soundings were taken, views were expressed, as to how you proportionately apply the surveillance of weblogs. Chapter 2 of RIPA does provide some powers, but it has never really been put into practice. Now, since the new provisions, excluding the additional filtering requirement, necessarily embrace all of that, that whole debate could have been laid out in the open. The Home Office could have briefed on it, they could have addressed the arguments that were put for both sides then, expressed a position, allowed Parliament to take its view and so on and so forth. So they have missed a lot of areas where, without needing to have recourse to national security considerations, they could have been open.

Q753 Lord Strasburger: I was going to ask you why you think the Home Office have got it so wrong.

Duncan Campbell: I think they have insulated themselves too much into a very small group that really only essentially talk to themselves and a few others, a few key engineers, and not sought to access even, perhaps, their own Ministers in getting an understanding of what might be required and what might be developed. They are operating in too small a world. I went myself to one of the Home Office briefings a couple of years ago when we

were looking at the previous Bill and asked them to try to explain some simple points, and they struggled. They did not seem to know their brief and they did not seem to be very enthusiastic about learning their brief. It was very disappointing.

Paul Heritage-Redpath: Speaking as a member of the public, there was an extraordinary self-assurance about the presentation by the Home Office to us of a from-high-to-low basis: "We have decided this is in our best interests, and we are not going to tell you what it is; you will just have to believe us." That was really how the Home Office presentation, at a quite senior level, came across to us.

Q754 The Chairman: You said in your opening remarks, Mr Campbell, that there are areas that could be addressed. It would be helpful if you could elaborate on those for us, please.

Duncan Campbell: First of all, I referred to weblogs. Now, internet service providers do not routinely obtain a log of what happens when a user, any one of us, is using our browser. In fact, a very rich trail of information is generated, many entries per page, on your computer, and for a certain time it would also be held by the communications service provider. So a step that the Home Secretary could take is, by order, to have that data held. It would be huge; it would be difficult to process, but we all know what it is. It comes into the courts every day, because it is also found on suspects' and defendants' computers. So it is a kind of evidence that need attract no secrecy. The businesses do not want it because beyond, say, a few weeks to do an engineering study of whether your server is working, you absolutely do not want to store that kind of data. But there need be no secrecy about those kinds of records or how they might be filtered or how they might be used and, indeed, the previous debate on RIPA addressed that. I think Professor Anderson's evidence also covered some points about that and probably Professor Sommer's too.

Then there are those areas where the solutions cannot exist realistically. The Information Commissioner mentioned virtual private networks; I would agree with that. There is the problem of Tor. It is a problem from the point of view of UK law enforcement, but, although I did not put it in my CV, I go and work for the other side on occasions, in that respect, bringing the knowledge of what you can hide. I have done that quite specifically in support of the Syrian insurrection and people who are struggling to overthrow the Assad regime and, of course, they have high dependency on Tor, their lives are at risk and if this Government were to, by some method—and I think Tor would say it is impossible—make that not available to them, we would bring about a far greater deficit in human rights in other parts of the world.

You have things like Skype, which have set out a model that works if you address the mutual legal assistance treaty things, and I have seen products come into the courts from MLAT. It is effective; it is what you want; it is the communications data that is asked for. All of that is not being considered.

Q755 The Chairman: There are criticisms that MLAT is a bit slow.

Duncan Campbell: I have never seen MLAT work fast, but I think already comments have been made as to the way the Foreign Office could be encouraged to speed that up.

Q756 Lord Strasburger: You talk about the request filter. Is it the case, in your view, that the distributed database that this Bill foresees combined with the request filter is going to be any different from the centralised database that was proposed in previous legislation?

Duncan Campbell: It appears to be larger, notwithstanding that it is distributed. I say that because the centralised database would ingather the communication service providers'

records at the specified times and hold them nationally with, no doubt, automated access, and that is required to come into being by the first part of the Bill. So basically, you have the national database within the Bill anyway, save that it will be held, in this model, by the CSPs. You then layer onto that the DPI devices that will hang on the key points of the United Kingdom network and mine as yet unspecified classes of data, presumably into similar local databases, but they will, by their nature, have to be integrated nationally, and I think this was conceded by the Home Office witnesses. You are going to data match across things that you see in the content derived from different nodes on the internet with different companies in order to try to get a match to generate communications data. So, if that analysis is correct, this is the national database of the previous scheme plus the additional databases supporting the need to retrospectively look at, I would imagine, a year's data taken from whatever the filtering system turned out to be. So, a bigger database.

Paul Heritage-Redpath: If I may address the Committee on the request filter generally, I think one of the challenges in the discussion around this debate is that it goes to technical matters and there has been very little technical discussion. The web is, ultimately, ones and zeros, and they are aggregated up into chunks, and those chunks may or may not have some meaning. Now, from the point of view of the request filter, we can see that use of the web is continually increasing, so the database that we are talking about, even if you take a year's slice, is only ever going to get bigger. Wherever that database is housed, it will require space, cooling, power, maintenance and people, and even if the Home Office pay ISPs for those things, that affects how you run a business, because you have to allow for somewhere for that database to live. Also, the more people and the more data involved, the more risk there is of human nature going in and having a look. This would be an extraordinarily large database. Keeping it secure would be, in my view, almost completely impossible. It is easier from a technical perspective than a simple "who is able to access this data?" perspective. So, from that point of view, it is a huge, huge risk, and I speak as somebody who looks after data centres and looks after ISPs.

It is unfortunate that we all have to speculate, because we do not have clarity on what is intended. I think, as I and others have read on the idea of the filter, it is Google for a set of databases that have been collected about traffic, so it can make connections. Now, on a very small scale, something similar has been tried recently by the Motion Picture Association of America and the BPI. They looked at about 13,000—so a small sample—of requests where they thought traffic looked like people infringing copyright, and they used an automated filter to perform that exercise. In 16% the addresses of the infringers were ones that were inaccurate, either malformed or not the right people. That is a very small sample. Now, that is just sending letters about copyright infringement, so it is not going to ruin anybody's day too much, but if we scale that up to everybody's communications all the time and have that sort of error rate or even a very small error rate, then the risk to human liberties is significant.

I would ask the members of the Committee to think about when you do a Google search. Bearing in mind that Google have the best engineers on the planet working full-time on search, how often when you enter a search term do you get a single correct result? You get many results and sometimes they are right, but how often do you get a single correct result? So if the idea of the filter is to say "We have aggregated traffic from all sorts of providers and we are then going to run a filter," what are the odds of that filter being 100% accurate and, even if it were, what is the use to the Home Office when they go before a court and say, "I have evidence, but I cannot tell you where it has come from because all I have used is a filter. I do not know what the filter is filtering and I do not know if it has got it right." So, from that point of view, just as a commonsense view, I have real problems with the filter.

Henry Porter: I would just add that it would be lovely if we could start using plain language here. This is a search engine or a data miner. I am not, obviously, as technically

expert as these two, in fact, much, much less so, but I had to scurry around and ask people who do understand these things for an explanation as to what it is. What it is is a data miner, so let's call it a data miner, which makes very, very fast connections between numerous sources of information. The fact that it is not in one silo of information does not make the slightest bit of difference. It is giving to a small group of people access to a massive amount of power. When we talk about this filter, we are talking about computing power, and it is computing power that is increasing with an astonishing acceleration every year. Our ability to do things tomorrow that we could not do today is extraordinary. So this Bill, apart from anything else, should take into consideration the massive power that will be given to these people who are running this system under the communications data silo or whatever you like to call it. So I would just warn that this is not power of today, but power of tomorrow. Who is going to be in the Government? Who is going to be in charge in the Civil Service? These are the things that worry me, the non-technical expert.

Q757 Lord Strasburger: This is for Mr Campbell specifically. Back to the filter. We have had evidence querying whether the results from the filter will meet evidential standards. If you were working with defence counsel on a case that relied on filter results, how would you go about questioning the admissibility of evidence derived from the filter and the weight to be attached to it?

Duncan Campbell: Lord Strasburger, my expectation is that the courts would probably never get to see the kind of information passed out of the proposed request filter. I will explain why in a minute, but the obvious point that goes to is how useful this can really be for prosecutions. The evidence given specifically in *Liberty v the United Kingdom* was that we are not going to discuss filtering, it is too complicated, you will not understand it, it is all classified, and we are not going to reveal our methods. The main reason for doing that, I suspect, is that the driving problem—which they never quite admitted until they came here and said, "We are never going to get one in six communications"—is that they do not want people to figure out what it is that they cannot get, because, fairly obviously, the bad guys will navigate through that. So their clear position in *Liberty v the United Kingdom* was that they do not want to explain how filtering works and they are trying to protect not their strengths but their weaknesses.

If I was wrong on that—I could be—then the admissibility would depend on the way that the court would approach testing, for example, an assertion from the prosecution by its experts that our filters had shown that somebody calling themselves Santa Claus on a certain network was, in fact, an individual they could identify and had in the dock. They would have to be prepared to disclose, in that case, the details of their filtering processes, which communications service providers they were taking it from, how they were pulling down the data—that is the phrase they used in *Liberty v the United Kingdom*—and say how they make it a match.

Then it gets worse. Obviously, if one is instructed for the defendant who contests that match, it would be necessary to do an audit trail according to the recognised standards of computer evidence to see what the parts are that go to make up that match. It may be statistical. It may be quite complex, and defence counsel will expect and the judge will expect that the prosecution, before bringing that evidence, will consider whether there is alternative evidence that you would wish disclosed, or at least to consider you had to disclose, to protect the rights of the defendant to due process. These are the obligations under CPIA and the Attorney General's guidelines. The defence, through the court or otherwise, might, quite properly, wish searches to be done of a more extensive sort. We would put in our own filter requests and get yet more pieces. You can, I think, start to see that, were you to add to the existing complexity of computer data cases from which judges, quite reasonably, resile if

they have to instruct juries, you would have an immense porridge of bits and pieces gathered from around the network, and an algorithm written by one company for the Government might say, "Santa Claus, 87% probable to be Mr Hoskins," for example, and, on the other hand, an alternative analysis might say you have not got a case that you have identified this person.

There is also the problem that, if you go back over the implementation of RIPA, they have not really stood up to evidential standards. Early on, we did have issues about whether the computer data—and it is computer data—that comes through in response to Chapter 2 requests—subscriber calling, bill data, cell-site data and so on—should be produced and handled to the same standard as the police handle normal computer seizures, which is generally extremely good. That was lost before the courts, but the proposition that was endorsed by a judge in an unreported judgment and that came to be adopted was that there should be a golden or certified copy of original data as it was obtained by the service provider and supplied to the police, and it would be retained in the custody of the communications service provider. Now, that was used as a phrase for standard practice, but was never understood, and for many years, although I think it has ceased now, the SPOCs would deal with this by sending back their email to the communications service provider, and the communications service provider's staff would send a statement back saying, "We recognise this as being the kind of data we use in our company," and think that was good enough. So we have already seen those kinds of problems in the way that the SPOCs worked in the first decade.

Q758 Lord Strasburger: That was quite a long answer to a short question. Could I just try to distil that back and see if I have understood you correctly? You seem to be saying that, because the authorities are unwilling to disclose the mechanism behind the filter, it is not possible to validate the effectiveness of the filter and it is not possible, therefore, to put the evidence that falls out of it before the court in any meaningful way. Is that right?

Duncan Campbell: I believe they would not produce it in the first place, because they would foresee the issue of technical difficulties.

Q759 The Chairman: So whatever other use the Security Service or the police could make of a filter, using it is as evidence in court is unlikely to be one of its main functions.

Duncan Campbell: On the basis of as much information as we have as to how it would work, which is, of course, little, that is my view.

Q760 Lord Faulks: I have just one thing; perhaps you can help me, Mr Campbell. We have a letter from the Director of Public Prosecutions suggesting that some of this evidence previously has been admissible as business records hearsay. In your capacity as an expert witness, are you familiar with this concept?

Duncan Campbell: Yes, and what he says is correct.

Q761 Michael Ellis: Of course, it is right, is it not, Mr Campbell, that very complicated evidence, including of a forensic nature, perhaps cell-site analysis, is already produced in court on a regular basis. It does not seem to hamstring the courts in producing relevant and admissible evidence of a modern type. They can handle it, can they not?

Duncan Campbell: The use of cell-site evidence has become increasingly established over the last 15 or 16 years. It has a degree of technical complexity to it. It is generally reduced to maps and put in a form that is helpful.

Q762 Michael Ellis: Yes, and so with cell-site analysis, which is the location of mobile telephones, usually the parties in court would stipulate or agree between themselves that the evidence has been obtained in a certain way and make an admission to that effect, so that the jury were not troubled with unnecessary complexities.

Duncan Campbell: Yes, the courts always admire a situation in which experts for the two parties seek to agree as much as possible and then precisely distil down that on which there is disagreement and on which the jury should deliberate.

Q763 Michael Ellis: That could happen in the instant case, could it not? It would not need to necessarily be explained to the jury in finite detail how everything happened. How scientists obtain DNA from a sample of blood would not necessarily have to be explained, but merely the bare fact that the scientists have come to the conclusion that the DNA within blood is that of the suspect.

Duncan Campbell: It is axiomatic that if the experts advising each side agree, then there is only a single joint statement to come before the court, which the judge would normally accept. I think I gave perhaps an over-detailed answer to Lord Strasburger, but in the area where the filter comes through—and I speak from a shared ignorance of what this filter will really be when it turns up and what the database will be that it applies to—you are going to ask the simple standard questions that you would ask representing anyone: where did this come from? What are the component parts? What is the means by which it is processed, and how do you reach the conclusion that you have told us you reach? If there is going to be a dispute—I am trying to foresee the kind of evidence that there might be—there will be a dispute as to how that could be reached and whether it was valid, and it would be massively complex.

Q764 Michael Ellis: If I can just take a step back, do you accept the premise that there has to be a legal means for interception of, in this case, data communications? Do you accept that to defeat the ends of terrorism, serious criminality, paedophilia and the like there has to be a means to do that?

Henry Porter: Yes, I do, but I believe in targeting the people that you propose to prosecute—the people you believe to be criminals. I do not believe that this entire nation should subject itself to a massive surveillance campaign by a few people who appear to be unscrutinised, their methods untransparent. But I certainly think that we should have these powers and we do have these powers.

Q765 Michael Ellis: Yes, and have had them for many years.

Henry Porter: Absolutely, no contest, and there are, what, half a million of the interceptions now per annum, roughly?

Q766 Michael Ellis: Of course, we should emphasise that this Bill does not deal with the interception, as such, of content. This is a different matter. This is not something that is seeking to read people's emails, which has been an aspect of the misreporting that I am sure you would all agree has taken place.

Henry Porter: Can I disagree with that?

Q767 Michael Ellis: You disagree with what?

Henry Porter: Yes, of course, the Bill lays out the difference between content and the data of the communication, but the fact of the matter is we all know in this room that the data surrounding a communication is as useful and can lead you to the content of that communication, and so the difference is very much a spurious one.

Paul Heritage-Redpath: If I could address the point, going back to DNA, ultimately with DNA you have a physical sample. You may disagree on how the analysis has been done, but you have something that is repeatable. With digital evidence, unless you have an audit trail of how it came to be all the way through, there is the possibility that somewhere along that way somebody may have tampered with it.

Q768 Michael Ellis: Yes, but Mr Heritage-Redpath, you need the audit trail as well with DNA or other forms of evidence. You need to be able to say that blood came from X person. You could not just magic up the sample and say it matches the defendant.

Paul Heritage-Redpath: Quite, but what I am saying is that in the case of all normal evidence, the police force, who have done a splendid job for many years, have targeted it in a particular case. What we are talking about here is something entirely different. We are talking about, let us say, on the face of the Bill for the moment, capturing data about all communications lest it might be necessary or helpful at some point over the next rolling 12 months. That is a different thing to a targeted investigation.

Q769 Michael Ellis: But you accept, do you, that there needs to be a legal means for police and law enforcement agencies to lawfully go about this type of activity? You accept that fundamental premise.

Paul Heritage-Redpath: I do, and I think the way the Home Office have sold this Bill is that everybody accepts the fundamental premise that we should have the means to combat criminals, but it is not then a stage to say, "Having accepted that, just sign this Bill off," because those are two different things.

Q770 Michael Ellis: Do you and your colleagues also accept, if you accept that premise, that the legal means have to keep up with modern and novel methods of communication? So, if it is lawful and has been for decades to intercept, for example, landline telephones, do you accept that modern methods of communication cannot be simply ignored, because criminals will use those modern methods of communication to defeat the aims of justice?

Duncan Campbell: There was a time, of course, when there was no law on interception of communications. We, the press—I and the press in large measure—pushed that into happening, and I do take pride in that.

Michael Ellis: Congratulations.

Duncan Campbell: Thank you. I hope it was sincerely meant.

Michael Ellis: It is. I try to say everything sincerely, Mr Campbell.

Duncan Campbell: I completely agree with what you say, of course. It is fit, proper and necessary that interception of communications and processing of communications data be available as part of the armoury to combat all the things you have mentioned. That is not my problem with this Bill. My problem is that it is not fit for purpose. It has not been thought through and it is not going to work. Leaving aside human rights, we are required to test issues like proportionality and necessity, and, in this forum, we are also required to test value for money and technical efficacy. Now, the witnesses who came here on the first day said to you, "We will spend all this money, and by 2018 one in six, 15%, of communications that we would like to get we will have no data about." Now, that is a huge amount of gap that is, on their own evidence, not going to be remedied. Where that data came from, we do not know—whatever survey assessment it is—but that simply raises the question of whether it is even achievable and, of course, it is not achievable to get everything. Our police forces and our security services are doing the best jobs they can. They are going to get it wrong sometimes. There are going to be some dark areas.

Q771 Michael Ellis: We cannot catch every burglar, can we?

Duncan Campbell: Right. So once you have accepted, as I accept, your premise, as I must, you must also, with respect, accept the other premise that there will always be the dark areas and that, therefore, the proper area for debate is fitness or proportionality, necessity—necessity given the other types of data that can be used in investigations—technical effectiveness—can it work—and cost efficiency. Then come all the human rights criteria—the fact that you do terrify people by creating powerful laws.

Q772 Michael Ellis: On the technical efficiency aspect and the other aspects that you mention, therefore, you do not think the Bill is strong enough.

Duncan Campbell: No. I do not think the Bill is capable of getting to 100%.

Q773 Michael Ellis: But nothing can get to 100%, can it, in all seriousness?

Duncan Campbell: Exactly. Exactly.

Q774 Michael Ellis: We cannot arrest 100% of burglars, even with fingerprint technology. We cannot do that, so we can do the best that we can do. Gentlemen, on this point, which is the necessary and proportionate aspect, the Bill envisages that any request for comms data would be necessary and proportionate. It is a safeguard written into the Bill and that would be verified by a senior officer. Now, we have, and have had for many years, aspects of our civil liberties that are affected by the opinion of senior officers. So, for example, within the 1984 Police and Criminal Evidence Act, a superintendant has the right to extend detention before anyone is charged in a police station. A chief inspector can oversee ID parades and the like. So there is a safeguard there that we are used to in the English criminal justice system. So do you not envisage that those safeguards can apply equally well here and, if not, why are you worried that they will not work here when they have worked for decades elsewhere?

Henry Porter: I hate this idea of self-authorising this sort of power to one individual. One individual may act in one way, another one may act inappropriately, but what I want to see is scrutiny. I want to see how this process happens, and I personally think it should be in the public domain—these authorisations should take place in public. After all, we are talking about a democracy that is a fragile democracy. If you look at what has happened over the last 10, 15 years, we had an ANPR system pushed through the country, cameras recording registration numbers everywhere, on every motorway and through every town centre. This happened without even Parliament granting the money. It happened because ACPO decided that it should. You have CCTV cameras being enabled very gradually with face recognition technology. You have CCTV cameras in schools, in cabs, in trains, in pubs, in restaurants. What I am saying is that this is part of a very, very serious move towards what could easily become the structure for a police state.

So let us just go back to the authorisation. The police are not perfect. They have misused ANPR information to track legitimate protestors. There have been occasions revealed during the Leveson Inquiry where police officers have accepted money to give journalists information, to say nothing of the misuse of the Police National Computer. I just do not think this power should be just given to the police, so I am not as happy or as content as you are about the way that might happen.

Q775 Michael Ellis: We need to move on. Forgive me. Are there any brief comments anybody else wants to make on that?

Duncan Campbell: In response to your question about senior officers signing on necessity and proportionality, that is necessary but it may not always be sufficient. I think, and some witnesses have put forward, that a much better scheme would be a multi-level surveillance authorisation, which, to some extent, already exists in terms of intrusive surveillance. That should be applied to the communications data schema, so that you have a signing off at higher levels or a warrant from sufficient authority, depending on the degree of intrusion involved. But these are the appropriate and necessary processes.

Just two minor points: although it was not required by law, the police sensibly adopted a scheme whereby assistant chief constables would be required to sign off on location data requests. They have dropped that now, but they saw the degree of intrusion necessary and they said, "A chief superintendant is not enough; we will go to ACPO rank."

The other point I would make is that the European Court has required that the procedures for examining, using and storing gathered communications material should be in a form that is open to public scrutiny and knowledge, and along with authority that is an important part of the process.

Q776 Mr Brown: I am quite interested in moving this on to the point about safeguards. As you have rightly pointed out to us, this is a framework Bill, and once the framework is agreed as primary legislation the flesh on the bones will come as secondary legislation. The opportunities for Parliament to say "no" or "pause" or "think again" are strictly limited, so it is important to us that we get this right. I am interested in what sort of safeguards we would insist are included. We have given some thought collectively amongst ourselves, Mr Campbell, to the point you referred to about a multi-layered authorisation scheme. It is there now, but would it be possible to extend that? In particular, I wonder if you could say to us what your thoughts are on the idea of a judicial element to the proposal. Should the magistrate's warrant that is proposed for local authorities be extended? Is it the right idea? Is the specialist authorising officer a better or a weaker safeguard than a magistrate who is independent but might not be as well informed or as experienced, or might be in awe of the police?

Duncan Campbell: They all get it right much of the time and wrong some of the time. I think a multi-level review of this whole area would be very sensible, and taken within that would be escalating ranks within the police force or security or intelligence services through to stepping outside to magistrates, district judges, judges, as might be appropriate to the degree of surveillance. The situation is that this business of content versus communications data is a shibboleth from the 1980s, when we had a plain old telephone service and clunky things called printometers, which could occasionally be attached to lines. Now, without going into the disparate technology of it, I think witnesses have told the Committee that the internet comes in layers, that the first layer is communication, but the content contains communications data about the next layer, and that content, in turn, contains communications. It all dissolves when you look at some of the very complex things that operate on the internet, and it would be quite appropriate just to review how distinct content and communications data really are, as part of an overarching review.

I know there has been a well tested argument about bringing intercept data into the courts. I have seen it. I have worked on it when it comes from overseas jurisdictions, and it is very hard to understand the degree of resistance, except a sort of primal fear of letting the adversaries know that we cannot do some things. So you could really quite usefully do an overarching surveillance scheme with officers of different ranks, judges of different authorities, and a surveillance commission that would act as the check and balance on whether the wide remits on all fronts had been followed.

Q777 The Chairman: That term "surveillance commission", you see that as a separate body and not a slightly enhanced role for the Interception of Communications Commissioner? Do you see him having any role in that?

Duncan Campbell: I think debates here and elsewhere have pointed to a need to really enlarge the scope and, indeed, independence of the Commissioner or whatever might be the successor body.

Q778 Mr Brown: I would like to elaborate on this. How far is a separate magistrate a safeguard and is there any further safeguard to be gained in restricting the number of authorities? The Bill only applies to the police, the security services and so on, although it is clearly shaped in such a way as to allow other authorities to be added in later and, indeed, there are hints as to which authorities, including local authorities, the Gambling Commission and so on, will be added in later. Do you think there is any safeguard to the public in restricting the authorities that should be added into the Bill?

Henry Porter: I certainly do, because if you look at the way RIPA was abused in the first half of the last decade, you had punt operators in Cambridge, a woman who applied to a school in Poole, Dorset, for her kid and was thought to live outside the catchment area, and I think you even had eel fishermen in Poole Harbour being subject to a major surveillance operation. So there is a predilection for abuse. We are not a naturally democratic country sometimes, and people will use these opportunities to use their power in an unpleasant way.

Q779 Mr Brown: A disproportionate way is what you are saying to us.

Henry Porter: Yes, I, indeed, was going to say that. So yes, I do think we should restrict as much as possible the number of authorities, and I think the maximum amount of transparency in the process that goes to authorisation is absolutely vital. One of the problems with this Bill is that it is not very specific. Duncan has been very eloquent in saying we do not really know what we are talking about, because it is non-specific in so many areas.

Paul Heritage-Redpath: Being in trade, I am required to make a business case for any investment that we do, and if I made a business case like this I would be sacked, because we have not been clear about what it is we are trying to achieve, how much it will cost or how to do it. The justification on the face of the Notes, as Michael put it, was, "This is all about catching criminals." Now, that narrows down what you are doing, but you get to the end of the Bill and it says, "Oh, and by the way, here is a list of X hundred authorities who might be interested." So in terms of proportionality, if it were just crime we would be having a much more targeted and productive discussion.

Henry Porter: Can I make one point about crime? Crime is on a steady downward trend. Whatever the economic circumstances of this country, steady, steady, steady, it goes down. For the last 20 years I think it is down 27%, the last 12 months 6%, and yet we are constantly being told by politicians that we have to guard ourselves against this terrifying society we live in. One of the main planks of this Bill is to fight crime, but let us just look at what is happening out there: we are a very law-abiding society and we are getting more law-abiding.

Q780 Mr Brown: What the public—our constituents as well as your readers—are worried about is that something they have done—on the internet or some communication, some bit of their private life they do not want their friends and neighbours to know about—is going to be discovered by a snooper and exposed in some way. How best could we safeguard against that? These are innocent people who are entitled to their privacy. How should we ensure they get it?

Henry Porter: Well, let us not have a vast database with large amounts of information in it. That is one way of guarding people's privacy. The second way is not to collect that information in the first place. I have a great problem with the argument that, because people give so much away about themselves on social network sites or to Tesco or to whoever, the Government and the state have a right, therefore, to take all that information and put it into a database. If you listen to Ross Anderson, the professor you had give evidence earlier this year, he would tell you that there is no way that you can have a database that is, at the same time, large, secure and functional. That means that, once your constituents' information is in a big database, it becomes much, much more vulnerable. So my answer is: do not have this Bill. It is very simple. Mr Ellis has made very good points about targeting criminals, but to collect this massive amount of information on people means that one day it will become vulnerable, maybe to a journalist at News International or a detective working for News International. This is the point: once you have these databases, they are a treasure chest.

Duncan Campbell: If there is an obvious concern, indeed, in auditing SPOC data down the years, I have always had it in mind to watch for an extra one being slipped in to bung to a journalist. I have not found any, but it may be that Lord Leveson and the associated police inquiries will be leading to this in due course.

Mr Brown's point about the sensitivity of data and the risk it could leak would, in my view, flow largely from creating this database in advance or these databases that are required. Again, rather than the obscurantism of the Home Office approach, we can address this quite specifically in the case of weblogs. In my expert capacity, I have to sometimes look at weblogs that, when seized from computers, can sometimes go back years and years and, frankly, they terrify me. The intimacy with which you can see what somebody is doing, what somebody is thinking, you can infer when their attention has strayed from their partner to some other prospective sexual target—it is written there to be seen. Now, if that person is under that degree of surveillance, because their device has been seized by the police because of a suspicion, then you can at least see how that comes about, and the rest of the population can be reassured that is never going to come to pass unless officers do come through their door for whatever reason. If you move to what was envisaged under RIPA and which will be reconstructed here, then, at the very least, the big internet service providers are going to be asked to store that kind of data, although we have no clue as to the depth of knowledge, and that degree of intimacy. That means that, if anyone wants to go on a trawl, whether authorised or unauthorised, whether the purpose might be approved or not, they can trawl to see who has been accessing special clinics. They can trawl for who has been going to particular websites. They can trawl to draw up profiles and demographics just in the same way as Google does. Clearly, most or all of that would not be proportionate. How do you stop it? Do not do it in the first place. Stick to what you get on people's computers.

Q781 Dr Huppert: I am very much enjoying the comments you have made so far. It has been a great pleasure to listen to. Can I look at some of the issues to do with parliamentary scrutiny and what is envisaged within this Bill? You have all expressed concerns about the, I guess, skeletal nature of the Draft Bill, for example, clause 1, which, to paraphrase slightly, says the Secretary of State can, by order, do anything she likes. Do you think that is inappropriate, in that there will be a system where you have this primary legislation, there is then an order, which is essentially unfettered, and that provides then for notices, which nobody gets to see? Does that seem like an appropriate way to take things forward?

Henry Porter: It seems mad for a democracy to even be considering this behaviour. I am amazed we are in this room countenancing this legislation. We have all brought ourselves

to a point where we feel it is necessary to think in these terms, but step back and imagine what Wilkes would have said or any of the other great men who have been responsible for fighting for this democracy and the liberal, free society that we have. Imagine Wilkes listening to you now and saying, "Well, these notices will be shuffled past, nobody will take any notice of them." It is unimaginable that we are even considering this.

In the last Government, I used to go to Select Committees to watch one or two of the Bills being discussed. I was astonished that we were even thinking of this way. There was a thing called the Legislative and Regulatory Reform Act, or some mad scheme.

Lord Jones: The Abolition of Parliament Act.

Henry Porter: That was it. Sometimes—when you just said that—I think how can we countenance this? We must be thinking of our democracy in different terms from the ones I was brought up with. We have to sit on this Bill. I do not care what party anyone comes from. This Bill is dangerous. This Bill is really, really dangerous, and if we let it get through in its current vague terms and then things are just added on, and nobody pays any attention, we will not have a democracy.

Paul Heritage-Redpath: We are all responsible for public money, at the end of the day, as well. I was involved in the e-conveyancing scheme with the Land Registry. This was a scheme where industry was consulted and where the people who were involved were very clear about what they wanted to achieve. There were very tight, small, objectives. It was £11 million of public money and it never came to fruition. I do not know anybody in the industry who thinks this scheme can possibly work and, to use a layman's analogy, I think we talked about telephones before and in his last piece Duncan mentioned weblogs. To be very clear, Duncan meant, I think, just the record of the URL that somebody had gone to—not content, just communications data. Now, the way the internet works and the way ISPs work is we try to move information around as fast as possible. The last thing we want to do is look at it. To try to explain how difficult this would be, what we do is akin to a traffic policeman going, "This way, that way." The original scheme, the old scheme of the great centralised database, started off by saying: "That traffic policeman will say, 'Stop, each car; I am going to ask the address you are going to and jot it down.'" You can see that will not fly. So the new improved scheme is to say, "Well, okay, we will just channel all of the internet and keep it. While it is going past, we will just keep it for a year on a rolling basis." Again, it is just common sense: how is it possible to get the capacity to do that, even if you agree that is a good thing to do? It is just like trying to pick the M25 up and photocopy it as it is going past. You cannot do it.

Duncan Campbell: That is a concern with the filter. There is no detail, as ever. We start from ignorance, but it is, to my mind, inconceivable that the tasks anticipated for any filter could be done on data as it streams past. Therefore, what you are left with is the elephant in the room that surrounds this Bill, which is we must not call it a national database because that is what the last Government did. Therefore, database is avoided, but in fact database is essential.

I fear the Home Secretary has not been well served by her officials on this. One is not privy to what goes on, but the sense is, "Do not worry about this; it is all techie stuff you really do not need to know. Parliament does not need to bother its head. It is the big complex internet; we will sort it out." Even if it was not this very sensitive and important area of legislation, what you look at with any knowledge of large public sector IT projects is massive expenditure, billions of pounds, on a future that is untested and on technology that seems incapable of being specified and that has not been described to the people whose equipment it will attach to. Let aside all of our other worries, the total gap in the information about how this will work means that there must be a very high probability that this will become yet the latest public sector, massive, cost-overrun IT boondoggle.

The Chairman: We need to conclude. Move on to the last question, please.

Q782 Dr Huppert: The officials will have a chance to speak. They are coming back to this Committee, and it is certainly a frustration of mine that we have not seen the draft of the Order at all. The Home Office position, if I try to paraphrase it, for making it so broad is that there is a fast pace of technological change and they want to have a Bill that is future-proof. I think that is the position. Given that we do believe that there is a legitimate role for communications data, how would you structure something so that you could resolve this? Would you have a series of Bills with sunset clauses? Would you have legislation that was extremely precise and needed replacing on a regular basis? What do you think would be the most sensible and practical way of getting the benefits of communications data without the harms?

Henry Porter: First of all, I think if you are going to give this power to the police and the Security Service, you have to have a period when you say, "Is it working? Is the scrutiny working? What effect is it having on our society? Is it having a chill on our internet and web industries? Is it having a chill on journalism?" So definitely you need to review it. If this is going to go through, you definitely have to have a sunset clause or some moment when you say, "How has this affected us?" Let us not just let it drift into the future imagining that it is working all the time as we planned originally.

Duncan Campbell: I think this Bill is future-proof, but in the worst possible way. It is future-proof in the sense that the Home Secretary seeks to have the power to her and her successors, in the words of the Bill, to do anything they like once the universal surveillance engine is connected up to the entire national internet. So, for that reason, it is additionally terrifying.

The alternative would be to reset the mechanisms of surveillance and allow that there would need to be fluidity as new data sources came along. A surveillance commission, if that were to be recommended, with access to both human rights advocates and technical experts as well as senior judicial figures, could address that—and with as much transparency as possible, which is the opposite of where we are now. And it will not be Twitter that we will be talking about in six years' time, it will be something completely new that no one has thought of now. So I do not think you can put in place a good future-proof Bill, but you could put in a transparent, thoughtful, representative system of reviewing how you adapt access to intercept and communications data as the technology changes.

Q783 The Chairman: Mr Redpath, anything to add, finally?
Paul Heritage-Redpath: No, that is perfectly fine, thank you.

The Chairman: In that case, thank you very much. We have overrun our intended time. That is because of the interest all panel members had in hearing your point of view. You spoke with knowledge, authority and passion, and thank you very much for giving evidence today.

Examination of Witness

Witness: **Keir Starmer QC**, Director of Public Prosecutions, examined.

Q784 The Chairman: Welcome, Mr Starmer. I am sorry we have kept you waiting. I know you are on a tight schedule today and I am sure we are so grateful to have you here.

Keir Starmer: I do not think you have kept me waiting, so I am very grateful.

Q785 The Chairman: I am sure colleagues will also respect the tight schedule you are on and we will be as crisp as we possibly can. Now, although we know who you are, for the public record, sir, I would be grateful if you would just state who you are and what you do.

Keir Starmer: Yes. Keir Starmer, Director of Public Prosecutions.

Q786 Michael Ellis: Good afternoon, Mr Starmer. Just to start off this session with you, do you consider that this Draft Bill, which no doubt you have had an opportunity to study, in its present form would allow your organisation or the Crown Prosecution Service to present evidence in court, where it existed, that would enable prosecution functions to be carried out? In other words, would it work?

Keir Starmer: Yes, I think it would. We use communications data at the moment routinely and it would allow us to continue to do so.

Q787 Michael Ellis: You probably were not present in the room, but we have heard other witnesses say that, in their view, it simply is technically not going to be something that would work; the courts would reject it. But you say that already communications data is in use and you do not envisage problems with admissibility or relevance of evidence.

Keir Starmer: Communications data is in use routinely. From a prosecution point of view, what it establishes in many cases is, if you like, the chronology of a crime, proof of association, links between individuals. Linked with other techniques it can establish presence at a particular place at a particular time and corroborate witnesses, etc. We use it routinely at the moment in a wide range of offences. Admissibility has not been a problem in the past. Usually the data is admissible, either as real evidence or as hearsay evidence under the various statutes and criminal procedure rules. I do not anticipate that is going to be a particular problem going forward.

Q788 Michael Ellis: Do you equate it, possibly, with another example that I used earlier, cell-site analysis of mobile telephone locations or DNA, in that you would not necessarily need to explain to a jury exactly how it is that scientists are able to extract DNA from a blood sample, but you would have to satisfy a jury that the blood sample was obtained legitimately, that its provenance was accurate and that a responsible scientific officer had performed his or her calculations correctly? Admissions can be made between the prosecution and defence to that effect, and are, in most cases, where DNA or other technical or forensic evidence is adduced.

Keir Starmer: I do not think explaining it to the jury is a particular difficulty, because once this is adduced, either as real evidence or business records, it is not very often in dispute. It is simply what it shows us that is relevant, and what we would very often do is use techniques to establish for the jury X was talking to Y at this particular time when, let us say, a consignment of drugs came in, and X, Y and Z were all talking together. We say they are the conspirators and, linked with cell-site analysis, we can probably say, "And they were standing in the following places when they were having the conversation." Presenting that to the jury is not particularly problematic, because the basic facts are agreed and it is what you can read into it that becomes the issue. Very rarely is it disputed that X was talking to Y or where they were. It is the explanation that is given for that behaviour that becomes the issue for the jury. So I am not saying that presentation is never an issue, but it is not usually an issue.

Q789 Michael Ellis: So this Bill deals with not the content of material but the provenance of it, where it has come from, where it is going to, the time, the date stamp, that sort of thing.

Keir Starmer: Yes.

Q790 Michael Ellis: Therefore, it can apply, to use another example, to obscene images, for example in a paedophilia case. Where that has been transmitted over the internet, one of the mischiefs that this Bill would seek to redress would be that it would be possible to ascertain internet addresses and date and time stamps and so on. Is that correct?

Keir Starmer: Any offence that we prosecute that involves the internet in any capacity usually requires us to produce communications data to show who it was that was accessing what part of the internet at any given time, and it can run through a range of offences. One example we have on a schedule here is a harassment case, establishing who it was that sent various messages at various times.

Q791 David Wright: The point here, though, is that much of that evidence at the moment, Mr Starmer, would be obtained by seizing a person's hardware—entering their property, taking their computer away, analysing what they have been doing with it. It would not be about tracing material that is going across the internet live, if you like. It is about seizing equipment.

Keir Starmer: It is a bit of both. A lot of it is seizing equipment, but not all of it. From our point of view, we are obviously concerned with the product and what we can establish from the product.

Q792 Michael Ellis: In a nutshell, Mr Starmer, would this Draft Bill, as envisaged, assist you and your agents and officers in the exercise of prosecutions of serious offences in this country?

Keir Starmer: Yes.

Q793 Lord Strasburger: I think we are starting to get confused on this Committee between the benefits that law enforcement agencies and prosecutors are getting from the existing legislation—RIPA—and what additional benefits they might derive from this Bill, if it were enacted. I am hearing from what you are saying that you are, at the moment, talking about the benefits you get from RIPA.

Keir Starmer: Yes. I am talking about that. That is what we have experience of and our concern is that we should maintain that coverage. I do not doubt or challenge that there is a privacy aspect here and there is a balancing exercise. I understand that, and Parliament has to think about that carefully. All I can say is from a prosecution point of view communications data is extremely useful in many prosecutions, for the obvious reason that it allows us to establish who spoke to who when, quite often where they might have been at the time and patterns of behaviour. If you are trying to prove a criminal case, that is extremely useful information.

Q794 Lord Strasburger: That is based on the existing legislation.

Keir Starmer: Yes.

Q795 Lord Strasburger: On the issue of admissibility of data, the question that we will be driving at shortly is how, under this Bill, evidence that is derived through the filtering process would stand up in court. But I think we are going to come back to that later on.

Keir Starmer: By all means.

Q796 Mr Brown: The public are frightened that data held on them by various Government agencies is accessible by corrupt public servants, and sold on to somebody with no right to have it, but who wants it for purposes of their own; the topical example is journalists but it does not have to be that. As I understand it, the offence committed by, say, a corrupt police officer in taking information from the Police National Computer to see whether someone had a criminal record or not is misconduct in public office. How easy is it to prosecute the offence of misconduct in public office and how frequently is it prosecuted?

Keir Starmer: Misconduct in public office is a common law offence with fairly straightforward elements. It has to be misconduct that reaches a certain threshold in order to render it criminal. That would be one offence that could be used. There would be others, I suspect: the Data Protection Act and Computer Misuse Act, possibly offences under RIPA itself. I am not sure we would have the figures under misconduct, and I am not sure they would tell the Committee very much if we were able to produce them, because, I suspect, that where there have been cases involving misuse of data, it is probably a number of different offences that we have considered in individual cases.

Q797 Mr Brown: Do you believe the present law and the practicalities of prosecuting it adequately protects the public from the commissioning of this offence?

Keir Starmer: I think the Computer Misuse Act was strengthened a number of years ago and, to my knowledge, it has not caused us any great difficulties. That is from my memory. I am very happy to come back if it would help the Committee on this, but so far as I am aware, we have not run into any particular problems. If someone has misused data, we have not found ourselves unable to prosecute for want of a relevant offence, so far as I can remember.

Q798 Mr Brown: Could you have a think about it and come back to the Committee?
Keir Starmer: Certainly.

Q799 Craig Whittaker: Just very quickly, I just seem to get to grips with what is going on in the various avenues of this Bill and then I get blown away. You said that you often use live data communications from the internet as well as historical stuff from hard drives and stuff; I think that is what you said earlier on. How many cases would you say do not come to prosecution because you do not have the ability to get to the stuff that is in this Bill?

Keir Starmer: I am afraid I cannot give you an answer to that question. I apologise. The reason is that if there is not the evidence, then it is unlikely the case would ever be presented to us. We are presented with cases that the police have investigated and, therefore, they present a file where they think there is enough evidence. Now, there may be cases where we would say it would have been jolly helpful to have had a bit more of this or a bit more of that, but we do not normally have a case where I would be able to say, "If you had had that, we would have been able to prosecute," and we do not record that. There may be some cases. I am not saying that would never happen, but we would not then record it as a case that, as it were, we could not take forward because there was a gap in this particular piece of legislation.

Q800 Craig Whittaker: Just very briefly, could I ask for a best-case guesstimate from you then as to how much extra information this Bill is going to give you that you physically do not have now under current legislation?

Keir Starmer: I think our primary concern is to ensure that we can continue to use the data that is currently available to us, and the concern is that it is retained and used in a

particular way at the moment. If that changes in the future—and I think the evidence on this has come from the Home Office rather than us—we want to maintain the capability that we have. From our point of view, it is a reasonably simple approach. The more people use communications and the internet to transact business and to commit crime, the more important it is for us to be able to use evidence to establish that they have done so, either when it is an offence that involves the internet itself, and we have some of those, or where it shows elements of agreement, conspiracy, for other offences. So that is our concern.

Q801 Michael Ellis: So, because you are prosecutors and lawyers, you would not necessarily know; it would be the police who would know that they cannot obtain evidence against a member of a gang, for example, because they cannot achieve that evidence. You would only know or your people would only know whether they can prosecute files that are laid before them by the police.

Keir Starmer: Broadly speaking. The police would put the file before us. Now, in big and complicated cases there is a conversation that goes on, and we encourage it, where the police may bring a file that has nearly enough evidence but not quite enough, and we might suggest lines of inquiry to them, but they would then carry that out. I can envisage in the course of that discussion it might come up that they would have liked to have got X but could not get it.

Q802 Michael Ellis: Yes, and further to my colleague Mr Brown's question about penalties for improper use, would the offence of perverting the course of public justice possibly apply in some cases if there was misuse in the obtaining of communications data? Could you see circumstances in which it might apply? That is an offence for which there is no limit to the amount of penalty, is there? Life sentences are applicable.

Keir Starmer: It might apply. It is not entirely straightforward. I certainly can conceive of some cases that might fall into the category of perverting the course of justice. I am not sure it would be the starting point in most of these cases, but it might be available.

Q803 Michael Ellis: Finally from me, would you say that there has been misinformation about this Bill in the media? You may not be able to answer the question. I do not know how closely you have been following it in the press, but would you say there has been misunderstanding or misinformation about it?

Keir Starmer: I am not sure I am in a position to comment on that. I have been following it, probably not as closely as everybody else, but I have been following, just at the moment, quite a lot of things going on in the media. So I think I am not particularly well placed to give a sensible answer to the Committee on that, I am afraid.

Q804 The Chairman: Mr Starmer, could you help me out here? I have heard you say probably a couple of times today what you are basically interested in is who spoke to who, when and maybe where they were with the tracking information. That seems to me to be fairly basic stuff, and I do not think any of our witnesses, including those, possibly, in the last panel, who were quite critical of the Bill, objected to that basic stuff being used by the police or accessed—who spoke to who, what, where and when. But the criticism of the Bill is that clause 1 seems to include a huge range of additional material, and logging on to internet addresses and so on, which could give a lot more information than who, what, where and when. Is it your view that you need all this extra stuff, or do you basically want to ensure that, whatever Bill we have in the future, you are getting the basic data you seem to be using at the moment—who, what, where and when?

Keir Starmer: First and foremost, we want no reduction in the data that is currently available to us. If it is right that those producing the data may not need to do so or retain it in the future in the way they have done in the past, and that is going to impact on our ability to get that data, then that is a concern. There are some offences where what we need and what we have had access to in the past has gone beyond that. We had one case called Dark Market, which was about, as the name suggests, a covert market where you could trade in stolen goods, cloned cards, etc. To prove that case we needed to have a lot more information about who was doing what on a particular website. So there is a category of offence—website-based offences—where we need to go beyond that, but our first concern is to ensure there is no diminution in the sort of evidence that is currently available to us and is used for pretty obvious reasons when you consider what it can show.

Q805 Lord Jones: What is your experience of the extent to which internet communications data is currently adduced as evidence? Is this evidence relatively easy to explain to a jury? Do you have some views you can give us again? Juries, I think, generally are not very expert.

Keir Starmer: I was alerted to the fact that there would be questions about volume and numbers. I am afraid that we do not track, on our own databases, the cases where we have used particular types of evidence; therefore I am not able to give an answer. We have given in our written evidence some examples of the types of cases. Communications data itself is used routinely. So far as internet communications data is concerned, I am not aware of any case where it has been overly difficult to present it to the jury. Presentation is not a particular problem for us, because once we have it in admissible form, frankly, most of the time the fact of it is admitted, and therefore it is simply for the prosecution and the defence to explain, as best they can, what they read into the information.

Q806 Lord Jones: Juries are a very British thing. Are you able, just for our benefit, to try and get into the minds of the many juries that sit throughout the nation every day?

Keir Starmer: No, I am not. I am no better equipped to answer that than anyone else is under the current regime. What we do though, just perhaps to give this some context, is where big cases fail I will very often have a case review panel, and walk through with the team—sometimes our team, very often our team and the police—the decision-making and ask ourselves why we think it failed and what we would do differently. As far as I can remember, I have not come across a problem where we thought it was because of the presentation of internet data communications that we have hit a problem. However, by its very nature, that is a selective exercise.

Q807 Lord Jones: Generally speaking, do you retain faith in the jury system?

Keir Starmer: Yes.

Q808 Dr Huppert: Mr Starmer, first, can I just ask when were you consulted on this Bill? When did you see what it said, and have a chance to talk to the Home Office about what implications it would have for your work?

Keir Starmer: Some months ago. I do not know the precise date, but I am more than happy to share with the Committee the dates on which we were asked to provide comments.

Q809 Dr Huppert: I think that would be very helpful to have a look at. Can I then ask about the admissibility of some of this, and the evidential integrity? I was struck by my colleague Mr Ellis's comparison with DNA. My PhD was exactly on DNA and I am sure that you will be well aware of work by Frumkin and others that shows that DNA data can be

faked, and this is why your predecessor decided not to take evidence that was entirely based on DNA. Presumably there are times when the accuracy of DNA evidence is questioned.

Keir Starmer: Yes.

Q810 Dr Huppert: So one would expect the same concerns with communications data, particularly if it gets more complex.

Keir Starmer: Yes.

Q811 Dr Huppert: Currently, we have relatively simple situations where most of the communications data that comes has been requested through a SPOC from a CSP presenting their own data, which they can be reasonably sure is accurate because it is their data they are passing on. This Bill envisages that a communications service provider in the UK would be using equipment that they were potentially supplied by the Home Office to collect data as it transits through the network, that belongs to somebody else, is laid out in a way that they are not familiar with and is potentially encrypted in some way.

Keir Starmer: Yes.

Q812 Dr Huppert: Do you think that would raise questions in a court and that somebody would be able to ask, "Who can assure me that this is the data that was sent in the correct format?"

Keir Starmer: It might do, but I think the rules on real evidence and hearsay evidence have moved on quite considerably in recent years, and it has not presented us with a problem so far. That is not to say it will not, or there will not be challenges just around the corner; of course there will be. Historically, though, we have not run into those challenges and the courts have been a bit more robust about real evidence and hearsay evidence than they were in the past.

Q813 Dr Huppert: Who would be able to present the evidence?

Keir Starmer: With real evidence it presents itself. With hearsay evidence the rule now is that it can be produced pretty much as a business document without a witness having to adduce it. That is how it is done very often, and recently the Criminal Procedure Rules Committee has changed the rules to enable that to happen a lot more easily. So, as it were, the old approach for many years, where you would have to have a human witness who would faithfully sign a statement saying that this is how it was all recorded has been, to a large extent, substituted with a record that proves itself. Nobody knows what the challenge is going to be around the corner, but I can say that at the moment there is rarely challenge to that record.

Q814 Dr Huppert: But what I am suggesting is that that is because the record is currently a far simpler document. If I can move you even beyond that aspect of the Bill towards filtering, that means you would have a system where there is purely a black box, where no individual or organisation could be sure at all that there had not been something that had gone wrong, nobody would see the transitory data, and you would have the outcome of a search that could not be verified. So whether or not you have a person presenting it, no police officer—nobody—could be sure that it was correct.

Keir Starmer: We would have to work through the practical problems. I take the point that you are making. No doubt there will be challenges, and obviously, from our point of view, we would want to be sure that in any given case we could comply with our disclosure obligations and therefore we would need to have a level of assurance about how that process worked, because we do have those obligations.

Q815 Dr Huppert: Did the Home Office talk to you about how this might work from an evidential basis? Did they engage with you to make sure that what they produced was something that you could use, or are you now retrospectively having to try to work out how to cope with their phraseology?

Keir Starmer: The communications in detail they have had have been with my policy and strategy team and, with your permission, I will check with them what and when, so that I can present you with a full answer on that.

Q816 David Wright: Can I just press that a little further? So you have not had a briefing with the Home Office about how this filter arrangement would work.

Keir Starmer: Personally, no.

Q817 David Wright: How can you make a statement at the start of your evidence, then, to say you believe this Bill will deliver its objectives?

Keir Starmer: Because I have read the Bill and I understand how it is supposed to work, and I have read a good deal of surrounding material and briefings, and I have talked to my team in detail about it.

Q818 David Wright: Okay, and you believe that, even having not seen the detail on how the filtering arrangement would work and the way it would produce material and the kind of documentation it would produce, that would still be suitable.

Keir Starmer: I have looked at the draft, I have looked at the briefings, and I have looked at the background material. I have looked at the experience we have at the moment. There may be practical difficulties. There will, of course, be challenges, but I do not believe, on the basis of what I have read and discussed, that there would be difficulties in using this information in the future. If it is right that the capability under the current regimes will go down, that is something that concerns me.

Q819 Lord Faulks: Just picking up on that, Mr Starmer, I think it is fair to say what you are really saying is that there might be some challenges because of the width of the filter; the existing rules about business-records hearsay and the like might not initially cover it. At the moment, I do not think there is much issue usually with the admissibility of these records. There might be some initial challenge, but you would expect it to settle down in due course.

Keir Starmer: Yes. Of course there will be challenges. I would be surprised if there were not, but I have faith that these will be workable provisions.

Q820 Lord Faulks: The obligation of disclosure can be rather onerous. There is going to be a considerable amount of additional material. Do you envisage difficulties with, potentially, a sizeable amount of material that you might be asked or obliged to disclose, consistent with the Attorney-General's guidelines?

Keir Starmer: I think we will have to carefully consider how we approach the disclosure exercise if this regime becomes law, and we will have to be careful to ensure that we are taking what steps we need to take to comply with our obligations, and that we are completely clear with the courts as to what we have seen and what we have asked for and what we possess. That can be achieved. We have achieved it across a number of different fields where there were obvious problems.

Q821 Lord Faulks: I appreciate the context in which you tend to see cases, but you have also told us that you will review cases afterwards. Have you been aware of this

so-called data gap in the course of your work—the data gap that will potentially be filled by the obligation on CSPs to preserve data that they do not need for business purposes?

Keir Starmer: No, I do not think I can say I have seen that gap, but I am clear that the data that has been provided to us has been extremely useful and if it is right that what is now retained may not need to be retained in the future and thus what is available will reduce, that is of concern to me.

Q822 Lord Faulks: Do you have much experience of the mutual legal assistance treaty process? We have heard it tends to be rather a slow process, but can you help us more than that?

Keir Starmer: It is useful, but it is a slow process. It is usually reserved for obtaining evidence after the commission of an offence where that evidence already exists in another jurisdiction. I think the difficulty here would be, first, ensuring evidence existed, because it had been preserved in some way, because no mutual legal assistance treaty helps if it has not been preserved; secondly, it is a rather slow process, usually measured in weeks or months and therefore, to my mind, it would not work well in this particular field.

Q823 Lord Faulks: There is one other point I would like to ask you about, if I may. We have heard from the Information Commissioner, who gave evidence to this Committee, about a tendency for police forces routinely to extract personal data from, for example, mobile phones of suspects and then retain that data even though that person is subsequently not charged. This may be a bit of an unfair question to field, but can you tell us, first of all, whether that is legal or not, under PACE or any other provision?

Keir Starmer: I am not sure, off the top of my head. I do not know. I can certainly work up an answer for the Committee, but it is not a straightforward question and it is not one that I have considered before. I am sure, if I have a shot at it, I will regret it in about half an hour when somebody gently points something out to me.

Lord Faulks: I apologise for asking.

Keir Starmer: On the other hand, I am more than happy, if it would be helpful to the Committee, to give a considered view in writing in a pithy way.

Q824 Mr Brown: That would help the Committee. You can see why we are interested in it.

Keir Starmer: I do, but I equally can see the trap that I am obviously about to walk into if I attempt it on my feet.

Q825 Mr Brown: I do understand that. Do you know if it is extensively done?

Keir Starmer: I do not know, but I do not think anything can be read into that one way or the other. I do not think I necessarily would know. I have not personally come across it, but then I see a limited number of our cases and I would not necessarily be privy to that if it happened. I have not come across it, but I really do not think anything could be read into that one way or the other.

Q826 The Chairman: If you could reflect upon the issue and let the Committee have a note that would be very helpful.

Keir Starmer: Of course.

Q827 Lord Armstrong of Ilminster: The Home Office are depending fairly crucially on the distinction between communications data and communications content, and content is dealt with not under this sort of Bill but under completely different arrangements.

But the point has been made to us in the course of evidence that that is a very blurred distinction, because what you can get now about data shades into content. If you know who has been speaking to who, when and where, and the frequency of conversations, you can get a long way towards content. Is this something that has concerned you or affected you?

Keir Starmer: I do understand why that point is made. A classic example here for us would be a case where we are able to say that a consignment of drugs came into port X at a particular time, and we think that three people were involved in the exercise. We look at the communications traffic between them and we establish that, by coincidence or, we would say, because they are conspirators, they were in contact throughout the passage of the drugs and when the drugs arrived they were in a lot of contact all of the time, and then it dropped off. Whilst we do not know the content of the conversations, we are often asking the jury to infer that they must have been talking about the consignment of drugs that have just been brought into the country. Now, that does not the give the jury content, it does not allow us to rely on the content, but we are sometimes saying to the jury, "The only inference you can draw here is that at that time, as they were both—as we can tell using cell-site analysis—right there in the dock as the drugs came in, they were talking about the consignment of drugs." That is a classic example of when we use that.

Q828 Lord Armstrong of Ilminster: I think you are really saying that that distinction retains validity for the purposes of this Bill.

Keir Starmer: The distinction does retain validity. Nothing here encroaches on content, but realistically and frankly speaking, we are, on occasion, inviting the jury to infer that A was talking to B about the crime that we are trying to prove.

Q829 Lord Armstrong of Ilminster: But there is a difference between inferring something from a series of events and listening or reading the content of the communication.

Keir Starmer: Absolutely, and a classic defence in that case would be, "No, I am the godfather of his child and we were discussing what I should get for its next present".

Q830 Michael Ellis: Mr Starmer, just moving on a bit to the public authorities and who should access communications data, the Draft Bill limits those bodies that will have a right to use the powers provided to access communications data and all the other bodies will have to make a case to the Home Office as to why they should be included. Is that right?

Keir Starmer: I think that is right, yes.

Q831 Michael Ellis: So I was looking at the written evidence provided by the Crown Prosecution Service. Now, the Department for Work and Pensions is a Department that the CPS seems to wish to continue to have access to comms data, and this is clearly because of the work prosecuting benefit fraud.

Keir Starmer: Yes.

Q832 Michael Ellis: So how important is comms data to the work in the prosecution of benefit fraud for the DWP? Do you know?

Keir Starmer: Just by way of background, if I may, the DWP obviously investigate and prosecute benefit fraud. In March of this year, the prosecution function of the DWP was transferred to myself and to the CPS, so we now, within our team, prosecute DWP fraud.

Q833 Michael Ellis: So prior to that there was a separate prosecuting entity.

Keir Starmer: Exactly, and one of the areas in which we have all rationalised our business is that we now prosecute for some Departments where we did not before, so we now

house and prosecute on behalf of DWP, and that is why it is in our evidence, because it now becomes material for us.

The case here is pretty much the same. There is nothing particularly special about benefit fraud. It is fraud. It happens to be fraud against public funds as opposed to fraud against private funds.

Q834 Michael Ellis: Yes, but we want to stop it though, do we not?

Keir Starmer: We want to stop it and we want to prosecute it; the techniques and the evidence that you use for fraud on public funds is pretty much the same as you use on other funds, and our only concern was that, that being the case and it being the case that DWP currently access the data, again we did not want to use that capability because it would affect the prosecutions we now bring.

Q835 Michael Ellis: Would it be your submission that the Department for Work and Pensions and thus the Crown Prosecution Service should have access to comms data in order to prosecute benefit fraud?

Keir Starmer: All we are doing is gently pointing out that this needs to be covered in one way or another. I do not think it is really for me to say how that needs to happen; but one way or the other, those charged with this Bill, as it were, should know that the DWP currently has access through statutory provision to this data and uses it; and if, by whatever means, when the Bill is passed, they did not have that capability it would fundamentally affect the way in which we could prosecute their cases.

Q836 Michael Ellis: So you would not want a limit placed on that body for that purpose.

Keir Starmer: No. The only caveat is that, without studying again the detail of the Bill, I could not say for sure that it could not be achieved by some other means, but by whatever means there needs to be access to that data.

Q837 Michael Ellis: Do you oppose the repeal of Section 109, subsection (2)(a) of the Social Security Administration Act 1992?

Keir Starmer: It rather depends with what it is replaced. If the result is that there would be no provision for gaining access to communications data in fraud on the public purse, then, yes, I would be very concerned. If there is some sensible provision in its place, then no.

The Chairman: I think everyone in this room is happy to see benefit fraudsters prosecuted; it is just a matter of whether we need all the provisions in clause 1 in order to do it.

Q838 Lord Armstrong of Ilminster: The list of authorities that have access to these data under RIPA is very long—10 or 11 or 12 kinds of authorities—and includes not only local authorities but the Coastguard and other authorities. Do you feel, though, that the use that those authorities make of the powers of access are really much more limited than in the case of the police and the security services? Would you like to see that list reduced? Do you think it is justifiable to use these intrusive powers for these other purposes?

Keir Starmer: I am sorry. I am not sure I am in a position to answer that, because I do not know the use that they put them to or how extensively they use the powers they currently have. I am sorry; there is just a gap there in my own knowledge. I have not had any dealings myself with those bodies in this respect.

Q839 Lord Armstrong of Ilminster: You do not prosecute in all these cases, I take it.

Keir Starmer: No, and, to be honest, I really do not know how often they access it and what use they make of it and, therefore, I am not equipped to answer the question. I do apologise.

The Chairman: Thank you very much, Mr Starmer, for coming along today. I hope we have not detained you too much on your busy schedule. Thank you very much.

Keir Starmer: Thank you. I will follow up on those issues.