CORRECTED TRANSCRIPT OF ORAL EVIDENCE

HOUSE OF LORDS

HOUSE OF COMMONS

MINUTES OF EVIDENCE

TAKEN BEFORE THE

JOINT COMMITTEE ON THE DRAFT COMMUNICATIONS DATA BILL

DRAFT COMMUNICATIONS DATA BILL

THURSDAY 6 SEPTEMBER 2012

Evidence heard in Private

Questions 601 - 659

Members present:

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

Examination of Witnesses

Simon Milner, Director of Policy for UK & Ireland, Facebook**; Colin Crowell**, Head of Global Public Policy, Twitter; **Stephen Collins**, Head of EU Policy, ex-Skype/Microsoft**;** **Steven Murdoch**, Chief Research Officer, the Tor Project, and Senior Researcher, University of Cambridge

Q601 The Chairman: Welcome everyone. We are in private session with our visitors and we will now start record recording. A warm welcome to you and thank you very much for coming. This is a private session and the people in the room are the Members of the Committee, our officials, clerks and our Lords and Commons transcribers—and no one else. Perhaps I may identify people and make sure that no one has crept in you. Will those supporting Mr Murdoch put your hands up?

Steven Murdoch: There is no one with me.

The Chairman: Is anyone supporting Simon Milner? Simon, could you turn around and confirm that those two people are with you?

Simon Milner: Those people are with me, yes.

Q602 The Chairman: Stephen, your people again? And Colin Crowell? Good, that is excellent. We are all complete. Thank you very much for coming. Thank you to those who have given us written evidence. This is a private session. We will be making a transcript but we will not automatically publish it. We would like to show it to you and discuss it with you. If our clerks and you can discover anything that we feel is safe to put into the public domain, by agreement we would do so. But we do play fair—if we tell you it is private, it is private. I hope that will encourage you to speak frankly to us. We all want to have powers to deal with terrorism, paedophiles and drug dealers, and we as parliamentarians have to balance that against the privacy of the individual. If we are to get this Bill right, we need to get from you a frank analysis of its strengths and weaknesses. We prefer to get that in private, even if we cannot talk about it afterwards, than for you to sit there and not spill the beans on what you think is right and wrong. If you do spill the beans on things that you do not want public, we will not make it public, but ideally we want to hear it. For the record, could you briefly identify who you are?

Steven Murdoch: My name is Steven Murdoch. I am with the Tor Project and I am also a researcher at the University of Cambridge.

Simon Milner: I am Simon Milner. I am director of public policy for Facebook in the UK and Ireland.

Stephen Collins: Hello Committee, I am Stephen Collins and here again. This time, I am wearing the hat of Skype. Until six months ago, I was head of regulatory affairs and global law enforcement relationship management at Skype.

Colin Crowell: My name is Colin Crowell (@Colin_Crowell on Twitter). I am head of public policy for Twitter.

Q603 The Chairman: Excellent. Thank you. Perhaps we can begin. I understand that some or all of you, after we asked you to give evidence, may have been asked to go to the Home Office for a discussion. Is that right? What was the discussion about?

Simon Milner: On behalf of Facebook, I am happy to confirm that, yes, we were invited to a discussion at the Home Office. It was our second meeting with the department since the Bill was published. We asked questions about the Bill and provided some other perspectives that I going to share with you as part of this session today, in particular our concerns around some of the provisions in the Bill.

Q604 The Chairman: But you had dialogue with the Home Office before we asked you to give evidence to us?

Simon Milner: Yes, but only after the Bill was published. We had no dialogue with the Home Office before the Bill was published.

Q605 The Chairman: And you had no input? You did not write to them and give it?

Simon Milner: We were never asked and we never provided it.

***Steven Murdoch*:** The Tor Project has not had any communications with the Home Office about this. We have not been invited and we have not had talks with them.

Q606 The Chairman: Briefly, Stephen, you are at the same point as before.

Stephen Collins: Yes, exactly the same, so I shall not waste time by repeating it.

Q607 The Chairman: And Colin?

Colin Crowell: We had one conversation with the Home Office about two and a half weeks ago. So we, too, were contacted after the Bill had been published and had one phone conversation with them about it.

Q608 The Chairman: That contact would be after we asked you to come here and give evidence.

Colin Crowell: Correct.

Q609 The Chairman: I see. So some of you had discussions with the Home Office via either teleconference or face to face. What was it about? Were you raising questions?

Simon Milner: Yes. In our case, we were asking questions in particular about the data retention proposals and what the Home Office had in mind on what that might mean for Facebook. It explained that to us that the Home Office envisaged that there would be a retention order on Facebook to retain all communications data in respect of Facebook users in the UK for a year. That gave us grave cause for concern about such a blanket retention requirement being placed on us. We also talked about the access process, but we were particularly focused on the retention regime in that conversation.

Q610 The Chairman: And Mr Crowell?

Colin Crowell: Yes, our conversation with the Home Office was similar in that it largely focused on asking questions about the intent of aspects of the legislation as we read it. The legislation is largely enabling, with lots of the implementing regulations and orders to come. Subsequently, sir, we were curious as to how they saw it working in practice. We also had questions about the assertion of authority to a company such as Twitter, which is subject to

US laws, and the relationship that we might have with a communications carrier here in the UK and the acquisition of our users' data and the retention of that data here.

Q611 The Chairman: Mr Milner and Mr Crowell, you were concerned about retention for UK users. Where would those data be retained? Would it be in the US or in servers in UK?

Simon Milner: As regards the UK, it might be worth the Committee understanding our user base here. We have around 30 million active users in the UK and around half of them will log on to Facebook every single day. All our data are held in data centres in the US, and therefore I envisage that we were subject to an order that these data would be retained in a data centre in the US. That is what the Home Office envisages as well.

Q612 The Chairman: Do you have concerns about that or are you relaxed about it, irrespective of the cost?

Simon Milner: We are very concerned about it.

Q613 The Chairman: What would the concerns be?

Simon Milner: In respect of the cost benefit of such a measure, we would be asked to retain enormous amounts of data which we would ordinarily delete if the customers asked us to do so. For 30 million users, only a tiny fraction might be subject to a request as part of a law enforcement investigation, but the data set would be there and it would be known that it existed. Law enforcement agencies in other countries might also seek access to those data via the US courts. We think that that should be a real concern for the UK citizens and for Members of this Committee.

Q614 The Chairman: Mr Crowell, is that a similar concern?

Colin Crowell: Yes, it is similar. Our servers are also in the United States, and one of our concerns would be about a UK-based carrier ordered to collect Twitter data here in the sense that our user data would be retained by a UK carrier. That would therefore pose

problems to us in terms of our terms of service and privacy policies. If such an order were to come to a domestic carrier here, that would collect and warehouse our data. We would also have issues with respect to not knowing when an access request for such user information was served on the company that was UK based and collecting our data. Finally, it is not clear how the filtering regime that is outlined in the Bill would work in practice, even from a technological standpoint.

Q615 The Chairman: We will come to the technology in a moment, but let us just park it if we may. If I am tweeting a person in the States and you are asked by the British Government to store those data, presumably data on the person I am tweeting in the States would have to be stored as well, or at least part of it.

Q616 ***Colin Crowell***: Yes, if it is a direct communication back and forth between two users, we would store both.

Q617 The Chairman: The same would apply to Facebook, I presume

Colin Crowell: It is a real conundrum from a jurisdictional standpoint how we would deal with user data that might be related to non-UK citizens that might be part of a communication with a UK citizen. There is also the issue that it is not just as simple as solely dealing with the United States; often people are communicating with other people in various countries around the world.

Simon Milner: Further to Mr Crowell's point, we would strongly oppose any measure that required us to violate the law in another country. One thing that we would expect to result from a discussion around an order would be that we would want the UK Government to frame an order so that we were required to retain data only in respect of UK users, otherwise we might be violating the law in the US or, more likely, other European countries, given the data protection framework. So we would store data only in respect of UK users. If the Government sought to propose an order requiring us to maintain data about users in

other countries, we may well have to seek a solution which involved the courts. We would not want to do that; we think that that kind of conflict over jurisdiction does not help the primary purpose of this measure, and in terms of our good relationships with law enforcement we would not want to have that kind of conflict over jurisdiction. But it seems inevitable that that is likely to result from this measure.

Q618 The Chairman: So if I or any other British citizen sent a message to friends in Switzerland or the United States and it is contrary to Swiss or United States law to store it, you would have to develop a system whereby you stored only my half of the message?

Simon Milner: That is what we would envisage would be the only way to ensure that you could be able to comply with UK law, as we would of course want to do, and comply with the law in other countries. To give an example of what kind of data that might result, you might have a record that says that UK user A communicated with UK user B, and then with somebody else somewhere in a foreign country, but with no information about where that person was or what country they were in—only that there was a communication with somebody else via Facebook. We struggle to see how that will be useful for law enforcement.

Q619 The Chairman: I can immediately see the gaps, but if that is your view of what you would have to do legally it is worthwhile information to have. My final point on the international aspect is this. If 30 million British subjects are held on a server in the States, do I understand the Patriot Act and others correctly in thinking that American authorities, whether the NSA or the FBI, would then have the right to say that they wanted access to anything on an American computer?

Simon Milner: Well, we are subject to the US courts, and if we receive a valid and enforceable order requiring us to disclose data about a user we have to comply with that order. It is worth bearing in mind that UK users of Facebook have a contract with Facebook

Ireland and are protected under Irish data protection law, which is under the European data protection framework. We are subject to some very clear and robust rules around how we handle their data. It is not an issue that has arisen thus far, but you are right that, given where we hold our data, it could be an issue in future.

Q620 The Chairman: Is it fanciful that American security agencies could serve a legal notice on you, saying that they did not just want information on this dodgy character, Blencathra, but on all 30 million Brits so that we can do a trawl for other reasons.

Simon Milner: The approach of the US authorities has been much more around preservation than retention. You might get requests to preserve data about accounts of somebody of interest, who may well be suspected of illegal behaviour. So it would be completely out of character, given their approach to these issues, to take that kind of blanket action.

Q621 The Chairman: And Twitter is of the same view, roughly?

***Colin Crowell*:** Yes.

Q622 The Chairman: Can we move on to the third question?

Q623 Dr Huppert: Mr Murdoch has been a bit silent so far. Tor has a slightly different relationship to this. What would be the consequences of this Bill on your operations? Are there specific consequences that you would have directly?

***Steven Murdoch*:** In some sense that is difficult to say, because the Bill does not go into very much detail. The Tor Project or architecture is very different from these other systems. We do not process the communications of the users. People who use the Tor network download the software from us, but their communications go over servers that are operated by volunteers to which we do not have access. Because we have designed the system to have privacy from the start, we would not technically be able to hand over any communications data, regardless of whether we were ordered to do so. Whether we fall

under the legislation at all is an open question, and we have not had any guidance as to what they believe. If we did, we would have to substantially change the architecture of Tor, and basically rewrite it from scratch, before we could do anything useful to provide communications data. Long before that happened, our funders would pull out and the users would pull out and the project would effectively cease.

Q624 Dr Huppert: It is helpful to understand that. There is an issue about the gap that the Home Office says that it wants to close. How often do you get data requests at the moment that you are unable to satisfy or that take a very long time to satisfy? Do you have experience of the gap existing when you get requests that you cannot satisfy.

Stephen Collins: Maybe I can kick off for Skype. I have been very quiet because I did not want to repeat everything I said in the last session. In the early days of Skype, we had all sorts of fanciful requests; it took a lot of time and effort on our part to educate particularly the SPOCs, specifically in the UK. We have built up a very good relationship with various constabularies around the UK to make them understand what Skype is and what it is not—a telephony service. It is a peer-to-peer software. We tell them how it works and what data we can usefully provide to them on receipt if a valid request. These days we get very few requests that are technically inept, if that is what you are pushing at. There is a good understanding not so much among the regular police officers but among the SPOCs at least, and we have spent a lot of time and energy to try to educate them so that they do not waste their time, and ours.

Q625 Dr Huppert: It is not just technically inept requests that we are talking about. There are also cases where there is a technically ept request, if that is a term, which asks for data that you do not have, but which under this Bill you would have.

Stephen Collins: Still for Skype? The data that are generated we will make available, if it is in a useful and accessible form. We have made it quite clear what those data sets are to the law enforcement community in the UK.

Q626 Dr Huppert: So the Bill would not have an effect on the data that be obtained from Skype?

***Stephen Collins*:** The Bill would not apply to Skype.

Colin Crowell: We probably get fewer requests for user data than some of the other services, only because the nature of Twitter is that most of what happens there is already public anyway. Law enforcement oftentimes simply has to go to the web on its own and can obtain the relevant Tweets that they were looking for. We probably get fewer requests there. With respect to the gap and a request for greater data collection and retention, Twitter also tends to collect less user data than perhaps some of the other services. For example, we do not collect information from our users about gender, age, home street address or things of that nature. If there are personal data that we have no legitimate business reason to collect, we do not gratuitously collect it. The irony, in looking at this Bill, is that on most of the other panels that I tend to appear, the policy makers and elected officials are urging us to collect less data and engage in data minimisation, rather than to collect more. The provisions of the Bill that hold out the possibility that we may be compelled to collect data that we have no legitimate business reason to collect is also a concern for us. We would have to explain to our users why we were collecting it and for whom.

Steven Murdoch: Like Twitter, the data that we can disclose to law enforcement are public anyway, so most of our effort goes into training law enforcement as to what Tor is, what data are available and how it can make use of them.

Q627 Dr Huppert: So you do provide some data?

Steven Murdoch: The data that we provide are to confirm or deny that a particular request came through Tor. So we can say that a particular IP address was a Tor server at a particular point, and that can guide future investigation. We provide that information, and we also provide software to law enforcement or to anyone else that will allow them to find that information without contacting us.

Simon Milner: We have a dedicated team in our headquarters in California and in Facebook Ireland that handles requests from law enforcement. The team in Dublin handles requests from the UK authorities for standard requests. In emergencies, our Californian team can also help with those requests. Based on the feedback that we have from UK law enforcement [REDACTED] they have indicated to us that they are very happy with the relationship and the turnaround times within which we provide data. I believe that they would be in a better position to identify specific cases, if any, in which they ask for communications data that we are unable to provide, either through that request process or through the MLAT process.

Dr Huppert: No one seems to be able to put their finger on it applying to them, which is one of the problems that we are having.

Q628 Baroness Cohen of Pimlico: The actual legislation on data might require a British-based CSP to store the data as opposed to you guys. The onus in default is on that CSP. I think you have answered the question whether it will indeed alter your relationships with everyone who finds themselves having to do this. If a third-party CSP was told that it had to pick up your data as they went across it, is this technically very easy for it? What difference does encryption make?

Simon Milner: I am happy to start on that. I think it is for them to advise you on the technical difficulties of collecting third-party data.

Baroness Cohen of Pimlico: Indeed.

Simon Milner: From our perspective, rather as Mr Crowell was saying, we are often asked to testify about data minimisation. As you can imagine, the security of our networks and the security of how we store and look after customer data are fundamental to our businesses. Therefore, when we are concerned that someone else might be trying to intercept our data, we will move heaven and earth to ensure the security of our network. It is a grave concern to us that it might well be part of the new framework that UK CSPs might be required to retain these data. One would expect there to be not only implications for relationships in the internet value chain but changes in behaviour by users. Facebook users already have the ability to encrypt their traffic, and we would expect many more UK users to choose to do so were that kind of measure to be introduced.

Steven Murdoch: We are also very concerned about the possibility of third parties intercepting data going to the Tor network. The design of Tor mitigates the potential harm from unauthorised interception or the abuse of intercepted information, but it does not eliminate it. We are also very concerned about other systems going over the internet which human rights workers make use of but that do not contain the protections that Tor has. Going back to Tor, it would be possible to intercept the data, but there are some technical challenges. One of our design requirements is that it should be hard to distinguish Tor traffic from other internet traffic. We need this to resist censorship in places such as Iran, Syria and China, so our traffic can look like web browsing or Skype. It can look like many different things, so it would be hard to pinpoint it.

Stephen Collins: [REDACTED]

Q629 The Chairman: [REDACTED]

Stephen Collins: [REDACTED]

Colin Crowell: It is fair to say that no company would want its user data collected and held by another company. We have to hold ourselves out to our users and to US regulators and

assert that we take steps to secure our user data and protect it from compromise. This might be a situation in which our user data are held by another company and we have no control over the security features that it brings to bear in storing that data. Secondly, there are the competitive issues and concerns that Mr Collins just raised. The technical aspects of achieving it are tricky, and one of the things that have been a characteristic of the internet marketplace, especially for a lot of the services that are web-based, such as the over-the-top services, is that they are in continual evolution. The features and services that we roll out will change from time to time from a technological standpoint, and there has often been this technological one-upmanship, with varying degrees of encryption and countermeasures for that, and so on and so forth. This would not be a static technology that is deployed once and then is there for use. It would involve measures on the outside coming in, and it would have to reflect how it could implement the filtering regime, as outlined in the Bill, to adequately tease out just the information that constitutes the communications data that might be relevant for an investigation as opposed to the other content and data that might be part and parcel of those packets. The final point I would make is that, to the extent that this is implemented in the UK, other countries might seek to do the same. So the paradox may be how British internet companies and British citizens might feel if a similar regime were instituted abroad.

Q630 Baroness Cohen of Pimlico: We are wondering what the implications would be of requiring a British-based CSP to store some of your data that go across it. Are you suggesting that your reaction would at the very least be to encrypt to protect your customers?

Colin Crowell: I do not know how we would ultimately decide to deal with a situation like that. We may have duties in other jurisdictions to protect data that may reflect on how we provide our service. The other aspect, which Mr Milner alluded to, is that our users also

have the ability to encrypt. So even if Twitter were not to do so, a user could encrypt on their own.

Q631 The Chairman: We assume that the order is given to the Vodafones, the BTs and the Everything Everywheres of this world to say that the data of yours that they intercept or that pass through their network have to be stored in the UK. Would you have a view on that? Would you want to see that in the Bill, or would you have concerns about how data from your network might be stored by a United Kingdom telecoms provider, shall we say, on their farm in India or outside the UK?

Simon Milner: From our point of view, that is a far lesser consideration than the fundamental issue of their being asked to store it at all. The location where they store it is less important than that.

Q632 The Chairman: So storing it in London is just as bad as storing it in Mumbai?

Simon Milner: Absolutely.

Stephen Collins: Before we consider that question, another question to ask is: how can we guarantee that the CSP has identified the right packets to be stored? Multiple providers, Skype included, use obfuscation techniques precisely to avoid being detected by deep packet inspection equipment. My question is a technical one: how would they guarantee that they would be storing the correct data under the order?

Q633 The Chairman: [REDACTED]

Stephen Collins: [REDACTED]

The Chairman: I read a brief yesterday suggesting that DPI technology lagged a few months or years behind the innovations in technology for providing new services.

Stephen Collins: It is an arms race.

Q634 The Chairman: Is that correct, and what are the problems that it encompasses?

Stephen Collins: Is that from a Skype perspective?

The Chairman: Or just from an industry perspective.

Stephen Collins: I do not want to speak on behalf of my colleagues, who may take a different view. From our perspective, we have a dedicated team involved in this obfuscation constantly in order to protect the integrity of the communications. At the same time, DPI equipment manufacturers have guys on the other side trying to work out what we are doing. That will continue. The point about it from the perspective of this draft Bill is that it costs money to maintain DPI equipment. We do not just buy once; there is a constant need to pay to have it updated in order for it to perform. That is the key here—it is very expensive.

Q635 The Chairman: But if people are to comply with the Bill, you as service providers cannot introduce a new service and then wait a few months or a couple of years for the DPI technology to catch up. Would you be under an obligation not to launch your new service until there was the DPI to analyse, record, check or store it?

Simon Milner: If I might say so, one of the issues that this raises is how these orders are going to be determined. From our conversation with the Home Office, the clear sense was that it expected them to be negotiated; the Home Office would not simply write them and turn up on day one after Royal Assent with the order written. To some extent, there is a degree of comfort in that in that it recognises that it is going to have to take account of some very different services and situations. The Home Office also indicated that it saw imposing these requirements on the CSPs very much as a last resort. To our mind, that again is recognition that the Home Office has not really thought this through very well if it is a key part of the legislation but it is telling us about it only after the Bill has been published. It makes us feel rather worried that there is a sense of, "Don't worry, we'll sort this all out in the end once the Bill is passed". By then, though, parliamentary scrutiny is finished, and from our perspective that is not a good place to be. We would much rather be having those conversations well before any draft legislation is published.

Q636 Lord Strasburger: I am still in search of this elusive 25%. If representatives from the Home Office were here today—and we asked them—they might say that telephony was not all on landlines or even on mobile phones but is now over the internet, and they might point at Skype or Tor as developments that have reduced their capability to capture and retain information. Would it be true to say that, in the case of Skype and Tor, even after the Bill is passed the Home Office will be no further forward, because you do not hold in your organisations the information that it would need to make any sense of those communications? In the case of Skype, it is peer-to-peer encryption and you do not hold the keys, so you cannot help the Home Office. Am I right in saying that?

Stephen Collins: That is correct. That is a content issue, but Skype does not operate like a telephony service. Those data are not generated, and we would have to make incredible architectural changes—rewrite code—in order artificially to generate some kind of telephony-like data.

Q637 The Chairman: If you were ordered to do it?

Stephen Collins: I guess there would be a question whether a Luxembourg software provider could be ordered or compelled under the terms of a UK Act that applied to communications service providers, which Skype clearly is not when you read the definitions. So there is both a definitional piece and a jurisdictional piece that I would say exclude Skype from the RIPA terms.

Steven Murdoch: Tor is a US-based organisation, so if the Bill could be applied to the Tor Project—because the reason for the Tor Project existing is to protect the safety of users—we would be in an even more difficult position than Skype in implementation. We would almost certainly fight this in the US courts, and if it came to the point where we could not operate in the UK, we would sooner not operate in the UK rather than basically destroy the project.

Q638 Lord Strasburger: I understood you earlier to say that you do not possess the information that would enable the police or the security services to unscramble what has passed through your servers. You just do not possess it.

Steven Murdoch: Yes.

Lord Strasburger: So whatever legal obligations are placed on you, you just cannot give it.

Steven Murdoch: Yes, and under the current design we do not have access to those data. We would have to build something different from the beginning before we could be in a position to collect any of them.

Q639 The Chairman: Did the US State Department encourage Tor to be set up, or does it back it?

Steven Murdoch: The Tor Project was originally founded by the US Navy Research Laboratory. Most of its funding now comes from Governments and most of that comes, one way or another, from the US Government.

Q640 The Chairman: So the United States Government might have a view if the British Government wanted Tor to spill the beans?

Steven Murdoch: Yes. From speaking to the funders, it seems that they do not want anyone, including themselves, to have access to communications data because they are so sensitive for the safety of the users and there is no safe way to store them.

Q641 Lord Strasburger: Lord Chairman, I understood the witness to say that TorR does not possess the keys or the ability to unlock this information. It would have to completely change its architecture. Is that right?

Steven Murdoch: That is correct.

Q642 Craig Whittaker: Most of my questions have been answered, but can I come back to you, Stephen? You said a couple of times that Skype would not come under this legislation. If the traffic was going across UK communications service providers, surely it

would—and whether or not that is captured by you or by those CSPs, you are going to get caught up in this anyway.

Stephen Collins: We will not be caught up; if that were the route that the Government decided to take, it would be the CSPs. Skype would have no involvement. There is nothing that Skype could do about that from a legal perspective, but it would be for the CSPs, with their DPI equipment, to seek to capture those encrypted data.

Q643 Craig Whittaker: [REDACTED]

Stephen Collins: [REDACTED]

Q644 Craig Whittaker: [REDACTED]

Stephen Collins: [REDACTED]

Q645 Craig Whittaker: [REDACTED]

Stephen Collins: [REDACTED]

Q646 Lord Strasburger: And what information are you able to provide?

Stephen Collins: [REDACTED] It is essentially subscriber information at the time of registration, which includes a variety of non-verifiable information: an e-mail address and an IP address at the time of registration. Then we have some communications data and call data records for some of the ancillary services such as SkypeOut, which allows you to call from Skype to a regular telephony service. Those CDRs, as they are known, are available, and there are one or two other things such as that concerning instant messaging.

Q647 Lord Strasburger: But Skype to Skype is entirely subscriber data?

Stephen Collins: Yes, because there is no service involved there. It is a self-provided service, and if you and I are communicating on Skype, our Skype clients and our computers are talking directly; they are not routing through Skype. All Skype has enabled us to do is to get into the peer-to-peer network. Once we are in, there is a distributed directory, which we do not control, inside the network on so-called super nodes. I do not want to get too

deeply into this, but we can find each other without Skype's help and then our software sets up a call between us. Skype has no involvement. That is where the private key exchange of encryption keys takes place. They are randomly generated by the software and then discarded when the session that we have ends, so if we spoke the next day it would be a different encryption key, randomly generated by those two. Skype cannot see that and has no involvement in that process.

Q648 Craig Whittaker: I have a final question, as I want to go back to this 25% figure that the Government have said is a gap. Is that a genuine "We don't know what 25% is", or is that just because the law enforcements do not ask any additional questions of you, because they already know what they can legally ask anyway? Does that make sense? Can you envisage what a proportion of the 25% is at all, or is it just because we ask you only what we ask because that is all we can legally ask you?

Stephen Collins: It could be, for example in the case of Skype, that they do not get full call data records for Skype to Skype communications. That may be it—I do not know—but how can that be missing when it never existed? It does not exist. It is not a telephony service.

Q649 Baroness Cohen of Pimlico: It seems to me that, at least on behalf of all the over-the-top services, the power for UK CSPs to collect your stuff as it goes over them is actually not useful. Would that be fair? So one then asks oneself, "Why is it in the Bill?". Is there any evidence you can see to suggest that it is a negotiating position for the Home Office to say to you, "Look, we'll claw it off by DPI", even if you really know that they cannot? I am asking you only to speculate about why the Home Office should want this power, because it is not obvious from the answers to your questions.

Simon Milner: I think you have had the Home Office here to provide evidence on understanding quite what the thinking is behind that. As you say, it may be part of their

negotiating armoury when it comes to discussing an order with a company such as ourselves, or others at this table.

Baroness Cohen of Pimlico: It is, in short, ad terrorem.

Simon Milner: Your Latin is better than mine.

Q650 Lord Strasburger: I know that we are stuck on this one issue but it is very important. Can I ask the question the other way around? If this Bill were enacted, how would the access to data of the public authorities that request data be improved, as far as you can see, if at all?

Stephen Collins: From a Skype perspective, I do not think it would be improved.

Simon Milner: From a Facebook perspective, in situations where a user has asked us to delete data and we are under an obligation to delete their data, if we are now required to retain their data, then in theory, of course, in respect of the odd individual user some data might be available that is not currently available. However, that would come at a very expensive cost in terms of the engineering effort that would be required by us to retain data that we currently delete—and which all our systems are set up to delete—for tens of millions of users, possibly just for the odd one or two requests that cannot currently be fulfilled to be fulfilled. Hence the sense that this is absolutely a sledgehammer to crack a nut. Yet the nut may not even exist, and we are not really quite sure how small it is if it does.

Colin Crowell: As I mentioned before, most of what occurs on Twitter is already public anyway and, typically, law enforcement simply has to go to the web and search for it. Where they are looking for particular non-public information or subscriber data, we do not get many of those requests, but it is Twitter's policy to preserve evidence as soon as we are informed formally by British law enforcement. If they have a particular suspect or account that they would like the non-public information from to build a case here in a non-emergency context, we preserve that evidence while the legal process runs its course to

convey it. Part of this is also taking two steps back and going back to the question of what the problem is that is being posed here. What is the problem that we are trying to solve? Going back to the question about the 25% gap, it does not seem to apply to Twitter because of course there is more information about what people are tweeting that never existed in the telephony world before, so there is more information there. Voluminous amounts of data on users from myriad companies could be collected through deep packet inspection technology. Again, that is what is being proposed to gain access to the few accounts where they may subsequently seek to build a criminal case.

Steven Murdoch: In the case of Tor, it would not make a significant difference. In the case of some other internet services, it could give access for the law enforcement agencies to more useful information. But criminals already have the capability to prevent law enforcement making useful use of communications data. Criminals have shown the capability, but human rights workers do not have the same capabilities that criminals have, so they will be put at risk by deep packet inspection and similar things that this Bill could introduce.

Simon Milner: Could I suggest that this could make this worse?

Q651 Lord Strasburger: Can we just stop? Sorry, but the Bill does not introduce deep packet inspection. The Bill introduces the wholesale retention of everyone's data for a period of 12 months. Deep packet inspection is a red herring as far as that is concerned. My question is: what does the wholesale retention of communications data over a period of 12 months do to enhance law enforcement and all the other agencies who want to get this? The message I am getting from the whole panel is that apart from, perhaps, some Facebook accounts that might have been deleted over that 12 months, there is nothing.

Simon Milner: In fact, it could make things worse by redirecting resources in an inefficient way. In the context of how we currently work with law enforcement, you have heard from all of us that we already have some very effective arrangements for dealing with law

enforcement and for providing information to lawful requests on a timely basis. Those are improving all the time and we have dedicated resources for doing so. Were this Bill to come in, one would expect that there could be quite an extended period in which some of those resources are being used to negotiate over a very difficult kind of order, with lots of resources focused on how much this is going to cost and on the engineering involved in it. [REDACTED]

Q652 The Chairman: Lord Faulks will want to come in on costs in a moment. First, just to finalise that point, how worried are you that if relations get soured, it will go back to the lawyers who will say, "Okay, give the Brits just what the American law requires and that is it"? Is that a real risk?

Simon Milner: I hesitate to say what would definitely happen. We are at an interesting stage in this process. It will be interesting to see how the Government react to this Committee's recommendations. We very much hope that will not happen, but it is certainly a scenario that one could imagine playing out if the Bill were to stay as it is and if the Home Office's approach to it is as blanket as it has suggested to us.

Q653 Lord Faulks: You have answered quite a lot of the points that I wanted to raise anyway. Very briefly, I detect that one of the real problems for all your organisations is the uncertainty and quite what it will mean in commercial and cost terms if the Bill becomes law. Have you made some estimate in your own minds as to what the costs will be? Bearing in mind that you can of course recoup those sums from the Government, have you any general comments beyond those that you have already made in that respect?

Stephen Collins: It is very hard to estimate what the costs will be when we do not know what we would be expected precisely to do under the secondary legislation on the code of practice. That is very difficult. We know how much it costs to retain data. We could calculate on that basis. What would not be in the cost-reimbursable piece are all sorts of

other things that have not been considered by the Home Office. Those would include things such as additional hardware databases for segmentation of the data from UK users—even if we could identity them, which I am not sure we could—into separate databases. A part of the draft Bill talks about the level of security required. It is almost an absolute that the data must be securely stored—not "reasonably securely" but "securely": 100%. That creates an awful lot more cost as well. We will need redundant systems, so everything would have to be duplicated and put into two locations. We have ongoing personnel costs to manage all these new sites and databases and to respond to requests. There is a whole host of other costs that are not considered at this stage by the Home Office. It appears that it has just looked at the cost of data storage. That is just the tip of the iceberg in cost terms.

Q654 Lord Faulks: So you do not think that its estimates are realistic?

Stephen Collins: I think they are really unrealistic—and the costs will increase. Even if we gave you a figure now, I would be willing to bet money that in 10 years' time that cost will have multiplied grotesquely.

Simon Milner: I very much support what Mr Collins said. In the same way as we do not understand how the Government have worked out their numbers, I cannot give you a number because we simply find it very difficult to understand what is actually being required of us. We expect that this would be a very significant engineering project. The comparison I would make is with the new requirements around deletion we had from our regulators—both the FTC in the US and the Office of the Data Protection Commissioner in Ireland. That has been a very significant project for us, with extensive resources deployed. That is for all our users, and this is for a subset of our users in a very specific way, just for the UK authorities. It is not the kind of project that we have ever done before, so it would be a major undertaking just to set it up. Then there would substantial ongoing costs to ensure that we continued to comply not just with this law but with all the other laws in the

penumbra of this. We have to ensure that we do not breach those laws because of what we are doing very specifically for the UK Government.

Colin Crowell: I would agree as well that it is impossible for us to predict the costs overall or the costs for Twitter because we do not know the extent of this or how sweeping the requests would be on us. The other points that Mr Collins and Mr Milner made are absolutely true: the volume of traffic over time is continuing to increase on the internet. We know this first-hand. Twitter is six and a half years old. It took three years and two months to go from the very first Tweet to the billionth Tweet. We now serve a billion Tweets every two and a half days. The volume over time will increase, so I do not know what the collection of that volume of data and the ability of people to sift through it adequately would cost, and I do not know how they would make the filtering aspects work.

Q655 The Chairman: Could I ask each of you to consider sending us a note on all cost aspects, not relating to your individual companies—we do not want that detail—but the items that could incur cost. Mr Collins has run through some of those, as has Mr Milner. We will not publish that but we will ask it from others as well. It would be helpful to the Committee to have from you and others who have given evidence your views on the things that might cost. We can collect that, make it anonymous and send it to the Home Office to say, "Look, these are the costs that various companies think they might incur if they were to do this". I would be very grateful if you could do that. I do not think we are asking you to breach any confidences there.

Simon Milner: So you want the cost headings.

The Chairman: Yes. Do not try to put your own figures to them. Just say, "If we were to do this, these are the cost headings we would incur". That might be training, extra lawyers, storage, data farms and the whole shooting match. Any other questions from colleagues?

Q656 Stephen Mosley: Trying to be positive about the Bill, with Facebook and Twitter, it looks as though people would have to store their data. If the Bill goes through and it happens, is there anything that you would suggest could be done to make it easier on you and on the British Government to make the system work?

Simon Milner: I am afraid not. As I have said, we can see only great complexity and extensive cost for minimal benefit. I would always want to be helpful but I am afraid I struggle to see how you can make this Bill more palatable.

Steven Murdoch: I agree. There is nothing that can really be done from our perspective. Either it would not apply to Tor or be used for Tor, in which case it does not make a difference either positively or negatively, or, if it applied to third parties for collecting Tor data, then we would have to have some way of preserving the safety of our users, and that would probably involve the users who choose to send data over the Tor network bypassing the UK. That would not affect users of the Tor network who were based in the UK.

Colin Crowell: I would just go back to a point I made earlier: it is Twitter's policy to preserve evidence once we are informed by law enforcement that they are seeking it. Regardless of what our data retention policies might be for various types of non-public data that we may have, once we are informed by law enforcement that they want information for a particular account for a case that they are building, it is our policy to preserve that evidence until they go through the legal process to obtain it. Again, finding some technological means to capture all of our data, including on users who will never commit any crime, to deal with the very few instances when law enforcement look for our non-public data to be conveyed to them as part of an investigation seems to us like overkill.

Simon Milner: To reiterate, that does not mean we think that there are no ways of improving the processes between ourselves and law enforcement. If you want to spend £2 billion of public money, though, why not use it to improve the intergovernmental MLAT

process, which is a very important part of this whole regime? You could spend a fraction of that money on significantly improving that process and really help law enforcement.

Q657 The Chairman: It has also been suggested to us that our police officers or security officers in the agencies should be better trained to ask for the right information, as the existing regime has all the information there but we ain't asking for it correctly. Do you agree with that?

Simon Milner: Absolutely. Indeed, that is why we spend time educating police officers on the process for seeking data from Facebook. We have published guidelines and an online mechanism for them to ask for data, based on them being authorised to do so. My colleagues recently spent some time in Glasgow meeting a large number of UK police officers and informing them about the process in place to submit a request for data from Facebook.

Q658 The Chairman: And was the end result that they were amazed that that ability was there?

Simon Milner: Some of them were used to it. It is like many things, though: it is having someone there putting a face to Facebook, who can help them to understand how to use the system. Actually, the UK is very good and has a good system. Most agencies know how to use our system and have well trained officers for that purpose. The UK is ahead of the pack in this area.

Q659 The Chairman: Is it the panel's view—I do not want to put words in your mouths—that part of this 25% gap, whatever it might be, might be closed with better training and more sophisticated techniques in the police and security services?

Stephen Collins: If only half the £1.8 billion was spent on training, that would be money well spent.

The Chairman: Thank you very much, gentlemen, and your supporting teams behind you, for coming here today. This has been very, very helpful. I am not just saying that; it has helped us. It has given us information that some of us may have suspected before but you have spelt it out for us. As I say, we will have a transcript that we will share with you, and we will discuss with you whether we would be able to use any of it, in an anonymised version or otherwise, in our published evidence. However, we are not going to expose you, having made a commitment that we will keep this confidential. If we could use some of it with your agreement, though, that would be helpful; if we suddenly come to conclusion X based on what you have said, it is helpful if we can publish some of the evidence to justify that. Please also supply the information on the discussions that you have had with the Home Office—the gaps and the worries that you have, the questions that would like us to ask—and any of the training that you could do. Thank you once again.