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 547 - 600

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

Sarah Hunter, Head of UK Public Policy, Google; **Stephen Collins,** Head of EU Policy, Microsoft, for Hotmail; and **Emma Ascroft**, Director of Public Policy, Yahoo!

The Chairman: Welcome. Thank you very much for coming this morning. We are grateful to you. This is a completely private session and I believe that our officials have discussed with you that we will take a transcript and then would like to discuss that with you as we hope that there might be parts of it that we are able to publish. We will be honour-bound not to do anything that would embarrass you or cause you difficulty. We want you to talk frankly to us. If you talk frankly, we can use that information to come to more sensible conclusions than if you do not spill the beans to us. We will respect your view if something is so sensitive that you do not want it out. We would prefer to have that information and not publish it than not have it at all. Perhaps a very brief word on who you are—Sarah, first, please.

Sarah Hunter: My name is Sarah Hunter. I am head of UK public policy for Google in the UK. I believe that we are here primarily to talk about our e-mail services. Just as background, Gmail—the e-mail service that Google Inc provides—has I think 425 million users worldwide. If you want to ask questions about any of our other services I will do my best to answer them but if there is anything I cannot answer I am happy to come back to you with written evidence, having asked my colleagues at Google Inc.

Stephen Collins: Good morning. My name is Stephen Collins. I am responsible for corporate affairs for Europe, the Middle East and Africa for Microsoft. I will not make an opening statement. You will have plenty of questions for us and we want to address what you are interested in rather than tell you what we think you should be interested in.

Emma Ascroft: My name is Emma Ascroft. I am director of public policy for Yahoo! UK and Ireland. I am here today representing Yahoo!'s UK business, but in order to be responsive to the Committee's questions I will draw on the experience of Yahoo! Inc where that is relevant. I thank you for allowing us to do this session in private.

The Chairman: I understand that after we booked you for this session, the Home Office called you in for a friendly chat. Why, what was discussed and what was the tone of the conversation?

Stephen Collins: There was no formal consultation with Microsoft prior to this contact from the Home Office. It clearly contacted us having seen us being one of the companies giving evidence to the Committee. It was a video conference call with one of our lawyers. I was not in on the call. It was essentially to allow us to ask the Home Office questions about the draft Bill. I would say here that it struggled to answer most of those questions.

Q547 The Chairman: We will come back to ask you what it struggled to answer. Sarah.

Sarah Hunter: It offered us an opportunity to meet having seen that we were also a witness. We have not had a chance to set up that meeting, unfortunately. We have met it once since the Bill was published. Similar to Stephen's experience, that was for us to ask it questions about the Bill rather than the other way around.

Q548 The Chairman: So in your case, it may just have been a coincidence that you were called in after we asked you to give evidence?

Sarah Hunter: It may well have been. I would not want to guess.

Emma Ascroft: This is going to sound like a familiar story. We were invited after the Home Office heard that we had been invited to give evidence to this Committee.

Q549 The Chairman: You had had no contact before?

Emma Ascroft: We had had no contact before. We met the Home Office in March 2011 to discuss the Government's response to the 2009 consultation on the changing communications environment, which Yahoo! UK responded to. We asked for a meeting in September, at which point the Home Office said there was no progress to report. I went on maternity leave at that time and made it clear that there was a colleague standing in for me who would be able to come to any meetings about this, but there was no further contact. As

I said, the meeting we had with the Home Office was three weeks ago. Again, it was very much presented to us as our opportunity to ask the Home Office questions. It was not for the Home Office to consult us on any options.

Q550 The Chairman: Let us go back to Stephen. You asked certain questions to which you felt that you did not get answers. What were those questions?

Stephen Collins: The ones where we did not get really specific answers, such as, "Can you articulate what the missing 25% of data is?". It could not really articulate what the 100% would look like, so it was difficult to see how it would get the 100%. On conflict of law issues, what if obligations that the Home Office placed on Microsoft put us in a position of legal conflict with home state laws? For us, that is those of the US, Ireland and Luxembourg. It could not really answer that. What if other Governments want access to the UK citizens' data that we are storing for longer now? That is a legitimate question that had not been put to them before, apparently. There is a whole series of questions.

Q551 The Chairman: You are reading from a brief there, Stephen. Would it be possible for the Committee, in confidence, to have that list or your brief?

Stephen Collins: [REDACTED]

Q552 The Chairman: We would be grateful. Okay, let us start with the 25%. Are colleagues content that we should pursue this line of questioning at the moment? Sorry, Sarah and Emma, did you have similar concerns about questions and answers?

Emma Ascroft: Yes, we had broadly similar discussions. There is a proposal in the Bill to require providers to generate data types specifically and only for law enforcement. That is over and above what a provider would generate and retain for their commercial purposes. We specifically asked what additional data types might be necessary, and the Home Office had to take that question away. From our perspective, the data types available to UK law enforcement, which it is empowered to request from Yahoo! UK, have not changed very

much in the time that RIPA has been in place. We are not sure that there has been a loss of capability. That is why we asked what additional data types it might want us to generate. We are still waiting for a reply on that question.

Q553 The Chairman: By "additional data types", what specifically do you mean? What would be examples of additional data types?

Emma Ascroft: The Bill is clear on what sort of broad categories of data it wants—traffic data, communications data and so on. Within that, there are specific data types, for example who an e-mail has been sent to and from. That is the kind of thing we mean when we say a "type", and because we do not feel that the data types that law enforcement currently requests from us have changed significantly, we were trying to understand whether we would be asked to generate new types of data, as the Bill permits the Home Office to order us to do. It had to take that question away.

Sarah Hunter: I think our conversations were broadly along similar lines. The one thing I would add is that the intent behind the Bill of the officials we met seemed to be very narrow and reasonable. When we pointed out that the powers within the Bill were much broader than that, they could not quite address why there was such a gap. We concluded that we would have to go away and understand more about the detail before we could give them a view on whether we thought it was reasonable or not.

Q554 The Chairman: So you are all worried that the oral assurances are reasonable and sensible. Everyone in this room wants to crack down on terrorists, paedophiles and drug dealers, but you are worried that the definitions in the Bill would allow a much wider data collection?

Sarah Hunter: I think that is a fairly good summary of our position.

Emma Ascroft: We are concerned on two fronts. There is what the Home Office says that it wishes to do, but we are not entirely sure that it is necessary and proportionate. The Bill

itself is far broader and empowers the Home Office to do much more than what it has disclosed to this Committee. We have pointed that out to the Home Office, and pointed out the issue around extending jurisdiction and the likelihood that this would set a global precedent. The UK would be the first country to extend its jurisdiction and take a reserve power to require UK providers to retain data that they could not obtain directly. We believe that other countries would follow, including countries that would use legislation of this kind to limit free expression and infringe privacy rights of internet users. From our perspective that would create a bewildering patchwork of overlapping and potentially conflicting legislation. Companies like us would face impossible decisions about how to be consistent in how we protect our users and operate our businesses in the 57 markets around the world where we operate. The Home Office fully accepts that that is a possibility; it anticipates that other countries will follow suit and seems quite comfortable about being the first country to do that. What is less clear to us is that it accepts responsibility for the consequences of that, which is a concern for us.

Q555 The Chairman: So if you let Britain do this and you are based in the States, you are worried that China or, hypothetically, Syria might follow. But then surely you would not give access to them. If it went to the FBI, through mutual legal assistance, to try to get it that way, America would say, "No, clear off China". But you are worried that, although it may set a precedent, in reality it would be able to follow through and get the information.

Emma Ascroft: We are concerned that companies like us would be put in a position where we have to make difficult choices, when there are legal frameworks in place that specifically anticipate these issues around jurisdiction. Mutual legal assistance treaties, for example, specifically address the situation where data are required in evidence in one jurisdiction but fall under the jurisdiction of another country. They specifically acknowledge that that jurisdiction has limits, which is something that this Bill does not do. It does not place any

limits on this extension to UK jurisdiction. That is where we have concerns. The Bill seems to be proposing an entirely alternative framework when there is one already in place and one which we would have thought was a more logical starting point for a policy review to address the concerns that the Home Office has presented.

Q556 The Chairman: So from Yahoo!'s point of view, if the Bill were to be enacted in its current form you would still prefer to go through with a mutual legal assistance route than comply with the Bill.

Emma Ascroft: The mutual legal assistance treaty recognises that jurisdiction has limits. Regardless of what is written in this Bill, the UK jurisdiction has limits somewhere, and the mutual legal assistance treaty structure is designed specifically to address that issue. UK law enforcement uses that framework frequently, and there may be room to improve it, but for us it is a framework that gives us legal clarity and gives some order to this very complex international legal framework under which we have to operate. The concern with the Bill is that we are afraid that it will trigger and prompt other countries to make that legal environment even more complex when we are in a situation with overlapping and potentially conflicting laws that will put companies such as ours in a position where we have to make the decisions and arbitrate between the different legal systems. That is clearly what MLAT anticipates not happening; it aims to address that.

Q557 The Chairman: On this point of the route—whether to use mutual legal assistance treaties or implement the Bill—what is the opinion of Microsoft and Google?

Stephen Collins: The three companies are all set up legally and operationally in different ways. I can speak for Microsoft a little bit, having worked there previously. We address this matter in different ways. MLAT is not a big part of the process; we rely a lot on so-called voluntary compliance with RIPA as it stands at the moment, in accordance with US, Irish and Luxembourg law. The issue for us is that we have not been told by any of the agencies with

which we work that there is a problem; we work very hard to co-operate with legitimate investigations that UK law enforcement and other agencies conduct. We understand that there is a need, but at the same time we try to balance a user's right to privacy against those investigations. But it is an extremely co-operative professional relationship. It is perplexing to us, given the sudden appearance of this Bill with such broad ramifications, that no one will come and say to us that there is a problem, or that they do not have this or that data set, or that something needs to be for 120 days, not 90 days, and that that kind of thing is hampering their investigations. That is the perplexing part for us. One thing that struck me as I read the background brief from the Home Office to this draft Bill was that although it claims that there is an information gap I am not so sure that it is one—it is more a capability gap. There are multiple references to telephony in the background brief. My concern is rather that having got used to 20th-century technology and the data sets produced by it, using those very successfully in criminal investigations for evidential purposes—there has been a plethora of new data as mobile telephony has become a mass technology—they have become completely reliant on those data sets to pursue those investigations. However, on the 21st-century technologies, from companies such as ours and from others from which you will hear later today, we are not providing the same kind of services. A lot of the time they are not services at all; they could be semi-autonomous software applications. They generate different data sets. It is impossible to imagine attaching, for example, telephone numbers to a Facebook page or call data records to Skype video communications. It just does not work. So for me there is a danger that we are trying to address a capability gap when there is lack of capability of understanding among law enforcement agencies of 21st-century technologies and the data sets that are generated and how they can be accessed and used for investigations. It could well be that the data sets cannot be used in court as evidence currently, and maybe that is something that could be looked at. It could be that law

enforcement needs greater training from industry and third-party specialists. I do not know what the solution is to bridge that capability gap, but it is like using a sledgehammer to crack a nut to try to introduce primary legislation on the basis of a supposed information gap that really does not exist.

Q558 The Chairman: I do not want to lose the point about the information gap, but I also do not want to lose the point about the mutual legal assistance treaties now that we are on it. What you have just said is crucial, and members of the Committee will want to explore it and whether there is a capability or information gap. Could I just finish off, along with any other colleagues who wish to ask questions, on the mutual legal assistance treaty, and Sarah's view on it? If this Bill were to be enacted in its current form, how would you and your company feel about using that, or would you prefer still to use the mutual legal assistance treaty route for whatever reasons?

Sarah Hunter: At the moment, Google has a number of different ways to enable law enforcement to access user data. We have an emergency procedure, when there is an immediate risk to life, which is manned 24/7. Like Microsoft, we voluntarily comply with RIPA, to the extent that we can. For all other data requests we encourage Governments to use MLAT. We are supporters of the MLAT process. On Emma's points about conflicts of jurisdiction, they do exist, and MLAT is designed to try to resolve those conflicts. We have heard informally that the MLAT process can be slow. My colleagues at Google Inc tell me that if that is the case, it is not the company side of the process that makes it slow; we therefore assume that it is the government side of the process that slows it down. I echo what others have said—that if there is a problem with that process it would be very sensible for us to start by looking at speeding it up and making it more efficient. The jurisdictional challenges that the Bill will provide will not make the MLAT less used; I think it might make it more used.

Q559 Dr Huppert: I was going to ask about communication with the Home Office, but I will stick to MLAT. What proportion of requests that you get from the UK do you currently comply with?

Sarah Hunter: Google publishes a transparency report at www.google.com/transparencyreport. It breaks down how many user data requests Google Inc complies with across different countries. I think we complied with 68% in the last half year, so 32% we did not comply with.

Q560 Dr Huppert: How many of those involved MLAT requests?

Sarah Hunter: We do not break the figures down, but I suspect that that 32% would have been requests directly from the UK Government. We would then in some cases have pushed them to MLAT. I think that the US number of complied user data requests includes MLAT, and is a very high number; I think that we complied with something like 98% of US government requests, because MLAT comes through that. It makes our life a lot easier because Google Inc is a US company that is based in the US, and we have to comply with US law.

Q561 Dr Huppert: As I understand the Home Office's intention with the Bill, it is that companies such as yours will be given a choice: "Either comply with what we would like you to do, or we will at least threaten to do DPI on transiting data and extract your data as they pass through the network". Is that your understanding of the options, and how could MLAT fit into that as a third option? This Bill would empower the Home Secretary to say, "Look, you're not prepared to have your data sucked in by the filter, so we will just collect it as it transits".

Stephen Collins: On the particular point about DPI, I will not comment immediately. [REDACTED]

Q562 Baroness Cohen of Pimlico: The one thing that is obsessing the Committee is how much all this will cost. Therefore, when I listened to your description of the MLAT procedure, my first instinct is that it will be much cheaper to go via MLAT than to say to you guys, "Change your system so that we can suck off the data". Is that perception faintly right? Let us suppose that you decided to co-operate with the Home Office rather than insisting it went through MLAT, and altered your systems so that you could do that. Will that cost a lot of money? Under current legislation, the Home Office would of course remunerate you, but is it an expensive thing to do?

Emma Ascroft: Probably. As there is such a lack of detail in the Bill, it is difficult for us at this stage accurately to assess what the impact might be. That is one of the reasons why we are asking the Home Office for that detail. There is no doubt that if the Home Office asks us to generate data and retain them for longer, that will have an impact on our storage capacity and data-centre planning. The challenging part is not just the storage of the data but the retrieval. You can store much data, but you have to be able to search and retrieve them, and that computing power in technology that sits over the top of a data storage capability is the difficult and expensive part. We also expect that having more data would lead to more requests. That would have an impact on how we staff the team that responds to law enforcement requests. Therefore, speaking broadly, those are the categories of costs we would incur, but we cannot accurately assess the impacts until we have an idea of the requirements. However, as I say, the Home Office has not been able to tell us that; it will all come later in secondary legislation or in orders and notices. At the moment we do not have visibility of those, and neither would they be subject to further scrutiny. Therefore, this Committee cannot know what the full costs will be either, and we have to take it on trust.

Stephen Collins: On the MLAT point in Baroness Cohen's question, the real issue is that MLAT is very slow. It is a government to government activity, so the costs to us would not

be lower; we would merely receive the requests from a different court. That would be ideal for us, but we have to appreciate that law enforcement investigations sometimes have to move quickly, and MLAT processes can take months—multiple months—with some countries. We therefore need to keep in mind as well that if MLAT were to be investigated in order to be updated and improved with various individual second countries, it would require a big effort not just on the part of the UK but on the part of those other countries.

Sarah Hunter: I will just add an element to what Emma said. No one should be under any illusion about how complex, expensive and hard it is to secure user data at scale. Protecting a terabyte of data is very different from protecting a petabyte. As Emma said, it is not just about storing it but about being able to search through it and retrieve it. Our company runs search, and in engineering terms it genuinely is rocket science. So the more you protect, the more you require a communication service provider to store, the more you have to be able to search through it. That is very difficult. At Google, we employ, I think, 250 engineers just to protect data overlaps. This is not something that should be taken lightly.

Q563 Craig Whittaker: You mentioned in your transparency report comparable figures of usage for the UK, France and Germany. France is 44%, Germany is 45% and the UK is 65%. Why is there such a difference in giving information? Following on from that, Brazil has similar amounts and is at 90%.

Sarah Hunter: I agree they vary quite widely, and I am impressed that you know all the figures better than I do.

Craig Whittaker: It is called Google.

Sarah Hunter: Yes. I have asked my colleagues at Google Inc whether there is any more information that we can give, and the reasons vary quite widely. Sometimes it is simply that the form was filled in wrongly. Sometimes it is that the SPOC does not know what data are

available. In those cases, the person at Google Inc who receives the RIPA request goes back to the law enforcement agency and says, "Can you narrow it?". Our Google Inc colleagues work with law enforcement agencies to ensure that they can comply wherever possible with them. I suspect that the reason why Brazil is slightly different might have something to do with the fact that we have different services there, in particularly Orkut, which is a social networking service that is very popular in Brazil. I can check and come back to you if you would like to know why Brazil is particularly different, but I think that it might to do with that service.

Q564 The Chairman: Could we move on to the point that Stephen made about the 25% gap? He did not know where it came from. Can you explain your comments on capability versus information? You said in evidence that there is a huge plethora of new information, and you were not sure why the security service and the police needed more information and that they were not dissecting properly the information you were already supplying. Can you elaborate a little on that?

Stephen Collins: Of course. It is not necessarily that we are not supplying but that information is out there and could well be publicly available. I think that there is a lack of understanding not so much on the security service/related agency side but more on the regular police side. There is a lack of understanding of the potential for the pursuit of criminals from data that exist on the internet already. Let us take a concrete example. In the circuit-switch world, when people picked up a telephone a copper wire relayed the call to one other individual call data records were generated from one end to another end point and the telephone company knew both end points. That was the primary means of remote communication. Then we had mobile, which did pretty much the same thing but allowed you to walk around while you were doing it. However, it is not the same thing as communicating via Facebook. It is not the same thing as being in a multi-party video

conference via Skype. These are different things; different data are generated. Different data may well be captured by Skype. They may be there but they might not be being asked for. I do not know unless we talk to the law enforcement agencies and the Home Office and they tell us what they think we are not currently supplying that they desperately need.

Q565 The Chairman: You have asked that question and they cannot elaborate on what it is they think they need or what they think is lacking?

Stephen Collins: They cannot elaborate on what the 25% is. Therefore, I cannot understand how they have worked out what the 100% is.

Q566 The Chairman: Emma and Sarah, do you have any comments or observations to make on that?

Sarah Hunter: We certainly did not have that figure of 25% shared with us. When we met the Home Office, it did not give us that number so we did not ask it about it.

Emma Ascroft: As I said earlier, we asked what the requirements of law enforcement are and, as the others have said, we have not necessarily had the operational feedback to say that we are missing stuff. That is why we asked the Home Office what additional data types it feels it is missing. The data types that are available to it now and that it has the powers to request are broadly the same as they were when RIPA first came into effect. We are therefore not sure that there is any loss of data with respect to Yahoo!.

Q567 Craig Whittaker: We are also struggling to understand the 25% figure. In your expert opinions, as a percentage of the data out there, what could it use that it cannot currently get hold of?

Emma Ascroft: We do not know what the figure is, but from our conversation with the Home Office it seems that one of its issues is the availability of data. Its concern is around the MLAT process and its lack of timeliness. By the time a request reaches a non-UK provider, the data are simply not there. This is why we all share an interest. It is in

everyone's interest to see the MLAT process work more efficiently. It makes sense to make more use of MLAT not only from a legal point of view but from a practical point of view. If it could be made more timely, effective and efficient, it would be in everyone's interest. Another tool that we think UK law enforcement could make use of is preservation orders for non-UK providers. In the US, for example, preservation orders are very widely used by US law enforcement. Where it has a particular target in mind, a US law enforcement agency can serve a preservation order on a communications provider and then preserve the data on a particular target so that they are not deleted in the time that it takes for the valid request to reach the provider. There are lots of ways in which UK law enforcement could work within existing structures to obtain data in a more timely way from non-UK providers. We just do not understand, because there has been no consultation, to what extent there has been a policy discussion in the Home Office exploring these very options. We just do not have visibility on that.

The Chairman: We had better get back on course.

Q568 Dr Huppert: I will look at the current law first, if I may. Is it clear what your legal obligations currently are, and would you welcome clarity in that? You talk about co-operating voluntarily, but does that expose you to legal risks if the US takes a different position?

Stephen Collins: [REDACTED]

Sarah Hunter: [REDACTED] We voluntarily comply with RIPA. My understanding from my colleagues at Google Inc is that that works fairly well. We have certainly had no complaints about the time it takes for us to respond to RIPA requests.

Emma Ascroft: [REDACTED]

Q569 Dr Huppert: Just to clarify something from slightly earlier, when Charles Farr gave public evidence to us for the first time, he said in response to Question 79: "Major CSPs understand the problem that we are trying to solve, understand the technology and the way in which we are proposing to solve it, agree that that technology is feasible and are looking for legislation to underpin collaboration in the future". I presume you would consider yourselves as major CSPs? Would you agree?

Emma Ascroft: No. When the Home Office talks about major CSPs, it might be referring to traditional fixed and mobile operators. Certainly in our meeting, the Home Office spoke very confidently about its ability to order fixed and mobile operators to capture and retain data about third-party services provided by non-UK providers and about the willingness of those providers to do that. It also spoke very confidently about the capability of the technology—that the technology was there. We have had no contact with those fixed and mobile operators, so we cannot comment on their willingness to do that or on the technology, but that is what we heard.

Stephen Collins: The only reason why I imagine a company would welcome this Bill would be if it already provides outside RIPA and wants some kind of legal security to reduce its exposure. I do not agree with the evidence provided.

Q570 Dr Huppert: You think there are companies that do that currently?

Stephen Collins: No, that is just speculation. That is the only reason I can think of for any company welcoming the provisions of this draft Bill.

Sarah Hunter: From the Google perspective, Charles Farr's characterisation of the conversation is not one that I recognise. Actually, in our meeting with the Home Office, we questioned some of the technical measures in the Bill, such as the request filter. I do not think that we agreed, shall I say, on its feasibility.

Q571 The Chairman: Could I go back to the international aspect and ask how your global organisations comply with the differing laws of different states? For example, what would you do if required by the UK to disclose data about a communication originating from, say, Germany, where the retention of data may be unlawful, or from Switzerland, which may have other secrecy laws? What would you do then?

Stephen Collins: If we received a valid RIPA request, we would expect the proper due diligence to have been done by the law enforcement agency concerned and the signing officer. If it was a court order issued by a judge, we would expect it to have determined that there was a sufficient nexus with the UK and we would comply with that request.

Q572 The Chairman: So if the SPOC has signed it off, even if it has come from Germany, Switzerland or Timbuktu you do not query where the originating e-mail or message came from?

Stephen Collins: Which SPOC?

The Chairman: You said that you would comply with it if it was a genuine RIPA request.

Stephen Collins: Yes.

Q573 The Chairman: However, the onus is therefore on the police officer or the security service to check that, wherever it has come from, it complies with UK law?

Stephen Collins: Correct, but it is not under UK law. If we are talking about RIPA and UK law, we will respond to a valid, properly authorised request. We will not analyse the content if it is properly authorised.

Q574 The Chairman: You will not look behind the communication to see whether it has come from, say, Germany or Switzerland?

Stephen Collins: As we action the request?

The Chairman: If the UK wanted you to disclose information on a e-mail or a communication that originated in Germany or Switzerland, where a different law may apply, you would not be concerned about that?

Stephen Collins: Again, the people who respond to the requests have a certain amount of expertise, but they are not international law experts. They would rely upon the assistant commissioner, chief inspector or whoever it was who signed off the request, and we would respond to that in good will, believing that the UK due process had taken place.

Q575 The Chairman: Is that the same for Google?

Sarah Hunter: I suspect that we might have a different approach. If we thought that there was a conflict of law, we would probably put it through MLAT. That is quite a good example of the challenges that operating our services throws at our colleagues who deal with them and why the MLAT process is so valuable. It is very hard to comment on a theoretical case without knowing a lot of the detail, but it is a good example because that is why MLAT exists.

Emma Ascroft: From our perspective, as I said earlier, we operate in a very complex global legal framework. There are many factors that determine which laws apply to a particular court request but, speaking generally, if a request came to us through RIPA and was served on our UK business and that data did not come under UK jurisdiction, we would ask the law enforcement agency to go through the MLAT process to the appropriate jurisdiction. [REDACTED] UK law enforcement knows well that if the data fall under US jurisdiction, they have to go through the MLAT process in order to obtain them.

Q576 The Chairman: What data would fall under US jurisdiction? Those of any customer on your server which is based in the States?

Emma Ascroft: As I said, many factors determine which jurisdiction applies. It is a bit difficult to talk hypothetically [REDACTED]

.

Sarah Hunter: It is worth pointing out though, from a Google Inc perspective, that we do not know the citizenship of our users. The only citizenship or geographical information we have is the location where they set up that e-mail address initially. Now, I may be on holiday in India when I set up a Gmail account in order to e-mail my family but I am a British citizen. These issues of citizenship are quite complex when you have a global service.

Q577 The Chairman: So what law might apply there? What jurisdiction would Google in those circumstances think was relevant?

Sarah Hunter: All of this is on a case-by-case basis; you have to look at the requests and the IP address. It is a complex judgment.

Q578 The Chairman: How relevant is the location of the server in deciding jurisdiction? Stephen, you say that you comply with British and Luxembourg—sorry, is it US and Luxembourg?

Stephen Collins: It is Irish and Luxembourg.

Q579 The Chairman: Is that because Ireland has the HQ and Luxembourg has the server?

Stephen Collins: No. Luxembourg has Skype headquartered there and Skype is now a subsidiary of Microsoft. The US has the headquarters, which is where the majority of data are stored, but for international services we also have a data centre in Ireland.

Q580 The Chairman: So what problems do you face in dealing with requests under RIPA because you have jurisdiction in Ireland and Luxembourg? Do you have to ensure that any RIPA request complies with Luxembourg and Irish law?

Stephen Collins: [REDACTED]

Q581 The Chairman: With Yahoo! and Google, is it similar or do you have servers in other countries as well?

Sarah Hunter: Our data centres are spread across the world. It is worth taking a step back to remind ourselves that Google Inc moves the data of its users between these data centres at a fairly rapid pace. You do not want to have one data centre holding all the data, because if it powers down overnight or it fails then it is very annoying to have lost all of your e-mail content. We spread the data across the data centres globally, so in those circumstances for Google Inc the US law is the primary decider for us.

Q582 The Chairman: Okay, so you all have servers spread across different countries. Taking up your earlier viewpoint, suppose that those countries say, "Britain is doing this; the UK is passing this new RIPA law. We want to do likewise", then Luxembourg says, "Right, we want access to all of that as well", and Ireland says the same—and with your server in India, the Indian Government hypothetically say the same. Do you see that as a risk and how would you handle that if it is a risk or possibility?

Emma Ascroft: Yes, it is a risk. This is a scenario that we discussed with the Home Office. We believe it is a very real scenario and, frankly, so does the Home Office. We believe that if the UK extends its jurisdiction in this way and takes the reserve power to require UK providers to capture and retain the data, if it is not available by extending jurisdiction, other countries will follow suit—and that will include countries that could use laws like this to limit free expression and infringe the privacy of internet users. As I said before, it would create a bewilderingly complex patchwork of overlapping and potentially conflicting laws, and put companies like ours in a very difficult position where we have to make difficult decisions about how to be consistent in our approach to law enforcement and protecting our users.

Q583 The Chairman: Any other comments on that before we move on? No—you agree.

Q584 Lord Jones: I heard, and liked, your reference to the user's right to privacy. That was in one of your earlier remarks. As a group of witnesses here, how often do you dig in

over looking after the rights of the user? I heard the word "citizenship", too, from one of you. How important is that to you and how far down does that commitment go in terms of your employees around the world?

Stephen Collins: From a Microsoft perspective—I am sure it is very similar for my colleagues—we would not have a successful business without the trust and confidence of our users. That is a kind of base assumption for building a successful business, particularly where there is an awful lot of competition in the marketplace and users can change to competing services at a couple of clicks of a button, so we have a robust privacy policy which we follow and implement rigorously. We have strict controls in place within our law enforcement response team—our global criminal compliance team, as it is known—in the US and, for Skype, a law enforcement relationship management team. They are trained to look at a request, check that it is properly authorised and undertake due diligence so that we can maintain this. It is a difficult balance, but we try to maintain the balance between co-operating with law enforcement and respecting the fundamental privacy rights of our users.

Q585 Lord Jones: Do you have many bust-ups? I mean: have you had distinguished cases on this?

Stephen Collins: With law enforcement?

Lord Jones: Yes.

Stephen Collins: [REDACTED]

The Chairman: Mr Wright, briefly, then we will move on.

Q586 David Wright: On the basis of that, what would be your market positioning reaction to this legislation in terms of the global market? Do you think that organisations such as yours, or even start-ups, will take specific decisions about UK law and about the way that they operate?

Sarah Hunter: Our position is probably very different to that of a British start-up which generally will not have a lawyer on its staff, for example, when starting up. We all have a number of lawyers. We are used to processing data requests and we are comfortable with that sort of relationship with law enforcement—and, as Lord Jones suggested, pushing back and being robust where necessary. For a British start-up, this Bill might put huge and unwieldy obligations upon them, such that it would put you off starting up a business. If you felt that you had to not only retain user data but potentially ask for extra data that you would not necessarily want to ask for, and then have it available to law enforcement, that is a significant cost. I think it would be very harmful to the competition within our sector.

Q587 David Wright: Miss Ascroft, you sort of said that your business was segmented in terms of its UK and US parts. Is there a threat that companies would start to say, "Well, we'll close down the UK element of the business, focus all of our activity within US jurisdiction and segment our business structure differently"?

Emma Ascroft: Given our company structure, Yahoo!'s UK business would be subject to this law, however it would be passed by Parliament—

David Wright: Yes, that is what I am trying to say.

Emma Ascroft: So, yes, that part of our business would be captured. In terms of our other businesses around the world, it is the situation I described earlier in that we would expect other countries to follow suit and to pass very similar legislation. The Home Office anticipates that that is exactly what will happen and we will be in a very difficult position because our policy globally, as Stephen said, is that we are a company that is built on consumers' trust and confidence, and in order to honour that commitment we aim to be consistent in how we engage law enforcement around the world. The consequences of this Bill would make it difficult for us to be consistent around the world, and we would then be put in a situation where we have to make very difficult decisions about how we engage law

enforcement and how we protect our users. It is very hard to overstate the consequences of this Bill internationally for companies like ours. It really could be quite devastating on our businesses.

Q588 The Chairman: Google has pulled out of China, a mega market, because of various political reasons. Is there a possibility that if your American customers say, "Google, Yahoo!, Microsoft—you are co-operating with the British Government on this Bill so we're not going to play with you any more. Close down your operations in Britain or we ain't going to use you, or we'll use the Blencathra.com search engine instead, because you're working with a Government who we don't like"? How realistic is that threat, or is it fanciful?

Sarah Hunter: All our Gmail users are subject to US law, so our structures being different makes a difference in that respect. Our operations here are not the people providing Gmail services.

Stephen Collins: From the Microsoft perspective, we would not paint that sort of doomsday scenario. None of our services is provided from the UK currently. What large multinational corporations would look at, as they do already, are the compliance obligations for when they seek to invest in a country. It is a competitive environment; it is not just a question of whether or not you invest in the UK, but of where one invests. That is the crucial piece. To come back to start-ups, I share Sarah's view. I do not want to exaggerate too much but there is a whole host of reasons, when one is involved in a start-up, for siting a company in a particular country. One of those that is taken very seriously is the regulatory burden. There are also the questions of access to venture capital, the amount of red tape and the qualifications of the staff but, when you are a two, three, five or 10-man band, this is an important consideration. You simply cannot tie up capital in unnecessary regulatory compliance when you can go to another market—although there are tax issues as well, of course—and not pay those regulatory compliance costs.

Emma Ascroft: Can I add another point? This might be a good time to talk a bit about our commitment to openness and user trust, and how that manifests itself in how the companies work together. We are all committed to protecting our users' rights and privacy; together, Google, Microsoft and Yahoo! are founder members of the global network initiative, a global organisation that brings together internet companies, civil society groups, academics and investors specifically to develop a collaborative approach to protect and advance free expression. This organisation has developed principles and implementation guidelines that guide responsible company action in engaging law enforcement in response to valid requests for data disclosure. Those principles for all the companies concerned are a factor in guiding our investment and engagement in individual markets around the world. That affects not just markets around the world where there may be issues around human rights and free expression but also mature markets such as the UK. That is another factor that determines how we engage with law enforcement in different markets. You have heard separately from the GNI; it has given you written evidence, which will give you an idea of the kind of issues that companies like us face and how we work with human rights organisations to think very carefully about the impact of legislation and the way in which law enforcement operates on our commitments to user rights and openness.

The Chairman: We have covered a lot of ground. Baroness Cohen, could we jump to your Question 8, please?

Q589 Baroness Cohen of Pimlico: I think that Question 7 has been answered; we know that we are not very happy about being required to pass your data over.

If the legislation as envisaged went through so that a British-registered CSP was required to store your data in a way that it does not now, do you know what technical difficulties that would present for them?

Sarah Hunter: From Google's perspective, all of the Gmail traffic is encrypted by default and we are pretty confident about the quality of that encryption. It could be stored, but whether it could be read is another matter.

Stephen Collins: From the Microsoft perspective, all Skype traffic is encrypted, and increasingly encryption is being rolled out to enhance user privacy and security across the so-called Microsoft Live ID services, which include Hotmail. We would be in a similar position to Google, so presumably the data stream could be captured but there is nothing intelligible there.

Emma Ascroft: [REDACTED] We also raised questions about how the data would be secured and disclosed. We understand from the Home Office that, were an order to be served to a UK provider to capture and retain relating to a non-UK part of Yahoo!'s business, Yahoo! would not necessarily be told that in order had been served so we would not necessarily know that these data were being captured. We are also not entirely clear what the oversight mechanism would be within the oversight framework that is anticipated in the Bill—who would make sure that those third parties were capturing and retaining data in the right way, were not using them for other purposes, were storing them separately from their data and so on. That assumes that the data could even be extracted in the first place.

Q590 The Chairman: So you have said to the Home Office, "OK, you can tell Vodafone, BT and Everything Everywhere to capture these data but they are all encrypted, and neither they nor you can read them"—what did the Home Office say to that?

Emma Ascroft: We did not ask that question directly, but I believe that the Home Office has said to this Committee that it would not serve an order if the data could not be reliably extracted.

Q591 The Chairman: I just want to explore this point. You have told the Home Office, "Yes, you could store this material but it can't be extracted". What was the reason it gave for still wanting you to store it or getting others to store it?

Stephen Collins: But it was not for us to do the storage. The question is about the UK CSPs, the underlying network providers and access providers.

Emma Ascroft: The Home Office described this as a backstop power. I believe that it said to this Committee that it does not anticipate having to use it.

Q592 Stephen Mosley: [REDACTED

Emma Ascroft: [REDACTED]

Q593 Lord Strasburger: What level of confidence do you have in your encryption, and how would you respond to a request either for the encryption key or for you to decrypt it on behalf of a public authority in this country?

Stephen Collins: For Microsoft it varies from service to service. I think that we will be talking about Skype in the next session, so I will elaborate on it there. Very briefly, there are no keys held by Skype to decrypt communications; they are discrete peer-to-peer communications where a private key pair is randomly generated by the software of the two end users. Skype take no part in that communication, so even if we wanted to we could not decrypt Skype-to-Skype communications. With SSL encryption, for example, I would have to get back to the Committee on that regarding the precise methodology. I suspect that that would be possible but not easy. If you wish I will come back to you on the decryptability of SSL from originating providers, if that is helpful.

Q594 The Chairman: Have you had any discussions with the Home Office on potential legal liability costs that you might incur? This may be too hypothetical, but I can imagine that if we incorrectly ask for information from an American citizen, thinking that they are British or whatever, or someone with dual nationality, and that turned out to be wrong, we could

have a multi-million pound lawsuit in the American courts and then joint action ones against you from another few hundred upset Americans, and massive legal costs. Have your lawyers have a look at this? Is there any concern that this may produce a new legal liability?

Stephen Collins: To be honest, this situation exists already, although maybe it would be exaggerated by the Bill. We are operating in good faith with the UK authorities, but we have no obligation to do so. We are doing this because we think it is the right thing to do. If that good faith is abused, we would have to think much more carefully about that co-operation.

The Chairman: If they are going to collect a lot more information, there is a bigger risk.

Stephen Collins: That is quite likely.

Q595 Lord Strasburger: Lord Chairman, could I ask my encryption question of the other two panellists?

The Chairman: Of course. I am sorry.

Sarah Hunter: From a Google Inc perspective, we are very confident about the security of our encryption. If a valid RIPA request comes in or UK law enforcement goes through the MLAT, receives a court order and in turn gets Gmail user data, we will obviously provide that data decrypted. If it was to use a third-party provider to gather the encrypted data, I think it very unlikely that Google Inc would provide anyone outside Google Inc with that key. That is simply because, as everyone said earlier, security is our most important asset. Our relationship with our users is predicated on trust. Without that, we have no business.

Emma Ascroft: I would say the same thing. If a valid RIPA request comes in, it comes with an obligation to provide the data in the clear. We would decrypt them. The encryption question is rather a red herring because the UK law enforcement agency can obtain the data direct from us using international legal channels such as the MLAT. If it came to us through those channels, we would disclose those data in the clear. If those channels work properly, this backstop power is unnecessary.

Q596 Lord Strasburger: You would provide that information decrypted?

Emma Ascroft: Yes, it is written into RIPA. Your obligation to disclose is to do so in the clear.

Q597 Craig Whittaker: I have two very quick questions. The first is on the encrypted stuff. Your data are captured by CSPs. How do you know whether that is context or content storing, which I believe is illegal anyway? Secondly—you may not be able to answer this question—how many countries subscribe to MLAT? Is there a possibility that, for example, Baghdad is not part of that process?

Stephen Collins: MLATs are bilateral agreements, generally. Not all countries are signatories with all other countries. I do not know what the list is for the UK; it is reasonably but not fully comprehensive. There will be multiple countries that are not MLAT signatories with the UK. On the point about content versus communications data, it is a very hard thing to do. Even when one can see the content and the communications data, there are disagreements among experts as to what constitutes content and what constitutes communications data. The best example is website URLs—the addresses for websites—where it is quite clear that you can identify where a user is going. The usual example is AlcoholicsAnonymous.org.uk/help: if you go to that 40 times a day, that is a good indicator of your behaviour. It is not really about your traffic or communications data.

Q598 The Chairman: If you go on to it 40 times a day, there is not much time for drinking. I was not diminishing your point, and we have heard that point before. We are coming to the end of our session. Is there anything else that you want to impart to us? Are there any other areas, from what you have read about this, that you think we should be focusing on if we are to make sense of it?

Stephen Collins: Can I ask the Committee really to think about this notion of the past and trying to capture in aspic something that was beautiful 10 years ago—and trying to get back

there. It is in the background brief. The Home Office states, "The Government is introducing legislation to ensure that communications data will continue to be available in the future as it has been in the past". Another part says, "CEOP is already experiencing significant problems because of the difficulty of obtaining the same level of subscriber information for internet communications as is currently available for traditional telephony". There is the problem. The key point is that our services cannot be made to look like telephony. We need better educated and trained police men and women.

Q599 The Chairman: Thank you. Anything to add to that, Emma?

Emma Ascroft: This is a global problem. The UK is not the only country looking at the challenges of a changing communications environment, the globalisation of communications and the changes in how users use those communications services. There were hearings on Capitol Hill last year where the FBI and Homeland Security said similar things. A consultation published in Australia in July is looking at exactly the same issues. It is a global problem that needs a global solution. The UK is the first country to have proposed draft legislation. It has done so relatively quickly without a great deal of consultation with the stakeholders who would be affected. Contrast that with the Australian process, where there is a consultation document out for public consultation now, a Cabinet committee has been convened to developed a terms of reference document that will also be subject to public consultation next year, and both Houses of Parliament are expected to do their own inquiries—and that is before draft legislation is published. The UK has gone out way ahead of the pack and the world is watching. If the UK passes this legislation, others will follow. We do not believe that that is the world that we want to create here. A more proportionate and less radical approach could be taken. We would welcome a sensible policy discussion on that. My second point would be that we must remember that MLATs are, by definition, a government to government process. The processes are defined by government and resourced by

government. If they are not working effectively and efficiently and are not timely enough for the law enforcement agencies that they are intended to help, it is for the Governments involved to review those procedures and how they resource them to make them fit for purpose in this internet age. We do not know whether that has been part of the Home Office's discussions. That is something the Committee should invite the Home Office to comment on.

Q600 The Chairman: That is very helpful. We thank the three of you, and your supporting teams, for being frank with us today. We will have a complete transcript made and officials will discuss that with you. We are not going to suddenly publish that. If you—not just Stephen but the three of you—supply us with the questions you asked the Home Office and to which you would like answers, maybe we can also ask the Home Office those same questions. We have an idea what some of them might be, particularly on cost and so on, but we would love to know the questions that you want answered. We will have a go. Thank you very much for coming today and good luck in future.

Sarah Hunter: Thank you.

Emma Ascroft: Thank you very much.