HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 027 • 2nd SESSION • 41st PARLIAMENT

EVIDENCE

Thursday, June 5, 2014

Chair

Mr. Pat Martin

Standing Committee on Access to Information, Privacy and Ethics

Thursday, June 5, 2014

● (1110)

[*English*]

The Chair (Mr. Pat Martin (Winnipeg Centre, NDP)): Good morning, ladies and gentlemen. We'll convene our meeting.

We apologize to our witnesses that we're late due to unavoidable circumstances.

Welcome to the Standing Committee on Access to Information, Privacy and Ethics. We're here today to continue our study on the growing problem of identity theft and its economic impact.

We are very pleased today to welcome representatives from Rogers Communications Inc., Mr. Kenneth Engelhart, senior vice-president of regulatory and chief privacy officer, and Mr. Aaron Storr, director of law enforcement support.

From Google, we are pleased to see again and to welcome back Mr. Colin McKay, head, public policy and government relations.

To both witnesses today, we have to apologize. We understand that the bells may ring again within about 25 minutes. What we're going to ask you to do is to enter your presentations into testimony. If there is any time at all, we'll divide it up evenly between the three parties, if that's agreeable. It may amount to one or two questions per party, and then we'll have to go when the bells begin to ring.

Having said that, I understand there is one matter of committee business to deal with before we invite the witnesses to speak.

Mr. Calandra.

Mr. Paul Calandra (Oak Ridges—Markham, CPC): Briefly, I seek unanimous consent to call Mary Dawson before the committee next Tuesday for 90 minutes and perhaps have committee business afterwards.

The Chair: Does Mr. Calandra have the unanimous consent of the committee?

Mr. Ravignat.

Mr. Mathieu Ravignat (Pontiac, NDP): He does, indeed, and I think that's a very reasonable amount of time. We look forward to it.

The Chair: Mr. Andrews of the Liberal Party.

Mr. Scott Andrews (Avalon, Lib.): Yes, that's fine.

The Chair: All right, it's agreed then. We'll advise the clerk to invite the Ethics Commissioner, Mary Dawson, to be our witness on Tuesday for a 90-minute presentation.

That's excellent.

Okay, gentlemen, in the order that we have you on our witness list, from Rogers Communications, Mr. Kenneth Engelhart, would you like to make your presentation, sir.

Mr. Kenneth Engelhart (Senior Vice-President, Regulatory and Chief Privacy Officer, Rogers Communications Inc.): Thank you for inviting Rogers Communications to appear before this committee.

You have broadened the scope of your hearings to include an examination of the disclosures that telecommunications carriers make to law enforcement agencies, and it is that topic that I will address in my remarks.

There has been considerable interest in this topic among members of the public and the media, and we are grateful for your committee's work and its allowing us to come forward to explain our procedures on the record.

Rogers is a diversified Canadian media and communications company, and the needs of our customers come first. We want to provide them with the best communications services possible and make sure they know that their personal information is safe and secure. However, as good corporate citizens, we also have to comply with law enforcement agencies who request Rogers' assistance in their efforts to keep our country safe.

I am pleased to share Rogers' “2013 Transparency Report” with the committee. It was just released this morning. This report is designed to provide more details on the number and types of requests we received from government and law enforcement agencies in 2013. We are proud to be the first telecommunications company in Canada to share this information publicly.

As you'll read in the report, Rogers received 174,917 requests for customer information in 2013. These requests fall into six categories, which l will detail for you now.

First, police and similar agencies provide us with court orders or warrants requiring us to release customer information to them.

Second, some government agencies have statutory authority to request information. For example, Revenue Canada has such authority under the Income Tax Act.

Third, we receive emergency requests from 911, public safety answering points, or police in life-threatening situations. These could include missing persons cases or cases of individuals in distress. We help them to locate someone with a cellphone and provide contact details for people who have called 911 and who may be unable to communicate.

Fourth, police sometimes send us a letter stating that they are investigating child exploitation and may need information so quickly that they do not have time to get a court order or warrant.

Fifth, we sometimes get an order from the courts pursuant to the Mutual Legal Assistance in Criminal Matters Act. These are requests from foreign jurisdictions that have contacted our Department of Justice. Because we have a treaty or convention with these countries, our courts process their requests. Note that we do not answer all requests that we receive. If we consider an order to be too broad, we push back and if necessary go to court to oppose the request.

The final area is the one which I believe has attracted the most attention. These are customer name and address checks. Very often the police are not sure which carrier they need to seek a warrant for. For example, they will come to us to ask whether a person who lives at a certain address or who has a certain phone number is a Rogers customer. We say either yes or no. There are other similar types of requests made under this category.

We believe this information is useful for the police so that they do not seek a warrant against the wrong carrier or regarding the wrong person. There has been a great deal of interest in the press about these warrantless searches, but they are a means by which the police can identify whom they should be getting a warrant or order against.

There has also been a great interest in the acquisition by some American agencies of metadata without search warrants. I can assure this committee that Rogers has not released and does not and will not release metadata to any law enforcement agency in Canada without a search warrant.

Further, as I said earlier, we would not process a request that amounted to a fishing expedition. Our customers' privacy is important to us. We believe more transparency is helpful and we encourage the Government of Canada to issue its own report to shed more light on these requests.

I would be most pleased to answer your questions.

● (1115)

The Chair: Thank you very much, Mr. Engelhart. We appreciate your remarks.

Next, we will invite Google Incorporated to present to us.

Mr. Colin McKay.

Mr. Colin McKay (Head, Public Policy and Government Relations, Google Inc.): Thank you very much, Mr. Chair.

I'm pleased to appear before the committee again, the first time this session, to speak about such an important subject, information security and identity theft.

My comments don't reflect this, but I'll just make a note right now that I'm glad that Rogers has come out with this transparency report. Much of what Ken has just described is contained in a similar report we issue every six months that can be found at www.google.com/transparency report.

Let me start off my comments with a short list. I have two, but I'll cut one to save time. It's just a series of phrases: 123456, password, welcome, ninja, abc123, 123456789, 12345678, sunshine, princess, and qwerty. That's right, those are passwords from a recent breach. The second list I have is quite similar.

Unfortunately, when it comes to information security, experience has shown that the weakest link in the chain is often the user.

Let's face it. None of us likes memorizing complex passwords made of strings of letters, numbers, and special characters, especially in a world where every website asks us to log in. Unfortunately, we're all possible targets. Not a month goes by without another effort to break into networks, steal passwords, and gain access to our accounts.

You've heard from previous speakers at this committee about the groups that try to hack payment systems, collect social insurance numbers, surreptitiously swipe financial data, and social engineer their way into offices and networks. These could be concerted criminal attacks or just the ham-handed attempts of relatively young script kiddies.

Many of their strategies rely on exploiting our habits, a willingness to believe a Facebook friend is truly stranded abroad, replying to a fake security warning from an e-mail provider, or believing network support is actually calling us at our desk but just needs our password to provide us with the support to make our work so much easier.

At Google we build systems and tools that alert our users to possible attempts to access their accounts and information. We give them information about sites that may try to inject malware and take over their computer and we work very hard to make the most secure networks in the world.

In a previous meeting, I asked this committee who uses Gmail, and so has my colleague and there's a consensus around the table.

Gmail processes billions of messages every day. It has an outstanding track record when it comes to protecting users from spam. Gmail users have become used to not seeing spam in their inbox for years and years. In fact, when a spammer tries a new type of junk mail, our systems often identify and block it from Google accounts within minutes and if it does happen to land in your inbox, you could press one button sending our systems a signal that we should consider similar messages as spam.

What about search results? Our technology examines billions of URLs across the web, looking for dangerous websites.

What do I mean by dangerous? It could be a site that injects malicious code. It could try to trick you into downloading a software package containing a virus. It could be a phishing site masquerading as a legitimate financial site.

We try to provide users with visual cues, like warning notes or even huge and obvious red interstitial images to prompt them not to click on dangerous links. The results? Every day we find more than 7,500 unsafe sites and show warnings on up to six million Google search results and one million downloads.

More than one billion people receive protection against phishing and malware every day because of the warnings we show users about unsafe websites through our safe browsing effort. We share this data with the other browsers Safari and Firefox, so their users are protected as well.

After all, the goal is to protect the Internet from illicit behaviour and extremely poor user experience, extremely poor being identity theft in its most horrible outcome.

At Google, we're continuously investing in network and data security. Security is a core part of our engineering culture. At our offices in California, New York, Munich, Zurich, and Montreal, we have a team of more than 250 full-time security engineering experts whose job is to help the company remain at the forefront of innovation in information security.

Let's return to passwords. We can agree that passwords are a compromise between security and convenience. We as users often abandon security in order to maximize convenience.

Just as a thought, do people around the room recognize why qwerty is a popular password? It's the sequence of five letters on the upper left-hand corner of the keyboard. It's the same combination in Russia on the Cyrillic keyboard.

● (1120)

The challenge is to create a verification process that is sufficiently complex to slow or halt attempts to access your accounts, but still convenient for the average user. Often this means innovation.

In 2011, we launched two-step verification for your Google account. Two-step verification demands that you verify your identity with a password and another passcode delivered to a separate device, whether a phone, a separate USB device on your computer, something specific. This provides a stronger layer of sign-in security. Even if a thief or hacker manages to steal your password, that's not enough to access your account. We offer this protection free to any account holder.

What about networks? Over the past year we've expanded session-wide secure sockets layer encryption to be the default when you're signed into Gmail, Google Search, Google Docs, and many other services. This protection stops others from snooping on your activity when you're on an open network, such as when you use your laptop at a coffee shop.

We've encrypted the data that flows between our data centres, and our security experts are continually working to extend and strengthen this protection across more services and links. This week we provided a tool to help our users identify how much e-mail sent between Gmail and external e-mail providers is encrypted in transit. After all, you can have the strongest encryption on your desktop, but if you're sending e-mails to someone with an unsecured system, that end of the system is insecure. This is important because e-mails are not encrypted in transit unless e-mail providers on both ends support it.

Finally, we react quickly to identified security threats. We have chromium and web vulnerability reward programs and pay hackers and security researchers significant amounts of money to identify security exploits and weaknesses in our programs and services. Over the past four years, we've paid out nearly $3 million to researchers.

Importantly, when a security exploit is identified, we have it patched and rolled out to hundreds of millions of users within hours. The sequence goes like this: A security researcher, who's worked on a particular weakness in our system and identified a way to win control of our system over a matter of months, comes to a contest and tells us about it. We tell them we're going to give them a large chunk of money, and by the end of the day, that's no longer a weakness because our engineers jump on it and solve that problem.

Google goes above and beyond to make sure our users' information is safe, secure, and always available. Our commitment to the security of our users' data is absolute, and we will keep fighting against anyone and everyone who tries to compromise it.

Thank you very much.

The Chair: Thank you, as always, for a very good and useful presentation.

Happily, we have about 20 minutes remaining. We understand the bells will begin at about 11:45. That leaves us, I would say, enough time for one round of five minutes for each party. If that's agreeable to committee members, we'll go ahead with that.

First up is the official opposition, the NDP, Mr. Mathieu Ravignat.

You have five minutes, please, Mathieu.

Mr. Mathieu Ravignat: Thank you, witnesses, for being here. It's a pleasure to see you in committee.

I think it's fair to say that Canadians are more worried about their privacy than they have ever been, that in a way, we're not keeping up with technological changes, and maybe the education of the public is not keeping up. I think, to a certain extent, telecom businesses in this transitional period have a social and corporate responsibility to inform their clientele.

I'm also concerned about privacy breaches that go on in government, and the relationship between government and telecom companies. It would seem that this government has requested personal information from you at an alarming rate. I was wondering whether or not you could speak to why you don't inform your clients when that information is asked from you by government.

● (1125)

Mr. Kenneth Engelhart: Thank you very much for that question.

I think the report we've circulated this morning is the first step in at least giving our customers and this committee and the government and interested parties an understanding of the extent to which law enforcement agencies request the information. I think, as other companies provide this information, it will start to provide some data so that informed debate can take place.

In terms of the specifics—

Mr. Mathieu Ravignat: Sorry, you've made me think of something. In the absence of a warrant, you're not obligated to give that information to law enforcement, right?

Mr. Kenneth Engelhart: That's correct.

Mr. Mathieu Ravignat: But you choose to do so?

Mr. Kenneth Engelhart: That's only in very limited circumstances, and it's really name-and-address type information, or in an emergency situation.

In an emergency, of course we're going to do it, because someone's life is at risk and they don't have time to get a warrant. For the name-and-address information, for example, whether Colin McKay is a Rogers customer, yes or no, we'll answer "yes" or "no"; otherwise, they get a warrant against us. If it turns out he's not our customer, then they will go to Telus. If it turns out he's not their customer, then they will go to Bell. It saves the police time. We don't think it's an infringement of our customers' rights, because it's just a way to save the police the difficulty of knowing whom to get the warrant against. That's why we do it.

Mr. Mathieu Ravignat: But this information is available elsewhere.

Mr. Kenneth Engelhart: In many cases it is. They could do a reverse lookup for some of it on the Internet. That's another reason we don't think it's terribly significant.

Mr. Mathieu Ravignat: My cynicism steps in and asks why, then, they are coming to you. It doesn't seem to make any sense to come to you for information they could get elsewhere, or that they're used to getting elsewhere, unless they're getting other types of information.

Mr. Kenneth Engelhart: Let me give you an example of why they might.

We have something in the telecommunications system called number portability. Say you were a Rogers customer and you made the terrible decision to become a Bell customer. Then you could port your number or move your number from Rogers to Bell. It could happen that the number you looked up on the Internet was yours, but it's not the number of a Rogers customer anymore. That's one reason they might want to come to us.

It can also happen that the number was returned to the number pool and is now held by another customer and the Internet is still showing it as customer A but it's now customer B.

There are all those different reasons why, to save time, they come to us.

I can assure you that we would rather just provide telephone service. If we had our druthers, we would rather not respond to these police requests at all, but we're good corporate citizens and we try to do a balancing act between doing everything we can—

Mr. Mathieu Ravignat: Internally, do you have criteria or standards in place or a review process in place whereby you deal with these demands and sometimes say, "No, I'm sorry, but I can't give you that information"?

As well, does the government ask for information that you don't give out? Can you confirm that they've asked you for information that you don't give out?

Mr. Kenneth Engelhart: Oh, of course.

The Chair: It will have to be a very brief answer, please, Mr. Engelhart.

Mr. Kenneth Engelhart: Yes, indeed.

Mr. Mathieu Ravignat: They have asked you for more information than you're willing to give out.

Mr. Kenneth Engelhart: They ask for both warranted and warrantless, and we often push back.

Mr. Mathieu Ravignat: That's worrying.

The Chair: I'm afraid your time is up, Mr. Ravignat.

We'll move to the Conservatives, to Mr. Calandra, for five minutes, please.

● (1130)

Mr. Paul Calandra: Thank you, Mr. Chair.

Thank you very much, witnesses.

Mr. McKay, I have to tell you that I've been on the committee a number of times when Google has had an extraordinarily difficult time of it, but I think that today I'm going to just focus on Rogers for a little bit.

It might be surprising to you, but I want to congratulate you on this report, Mr. Englehart. I'm not sure if Bell or Telus does this, but this is actually very informative. I don't know if we could inquire with Bell or Telus to see if they put something like this together, but I think this really helps us understand what access is.

Mr. Ravignat talked about government accessing or calling you. I think he has left the impression that the Prime Minister's Office is calling you and seeking the information on a subscriber. Is that what we're talking about here? When we talk about government, your statistics seem to suggest that either the revenue department is calling you or a law enforcement agency is calling you. Am I correct that those are the types of requests you're getting?

Mr. Kenneth Engelhart: That is absolutely correct, sir. It's either a department that has a specific statutory power to make that request, or it's a law enforcement agency.

Mr. Paul Calandra: In the law enforcement agency, we've heard a lot about this and I've done reverse lookups myself. When I got back here in October there was a little bit of an issue going on with the Senate and there were some e-mails and phone calls that were almost troubling, let's put it that way. In the course of that, you do a reverse lookup and you can see, but your number portability is a cause of grief because people do transfer now from Rogers to Bell.

I'm wondering, when the police are contacting you, if you have some examples of emergency situations. Do you have any examples at all of an emergency situation where Rogers was asked by the police to help and what type of information you provided or what the situation was?

Mr. Kenneth Engelhart: Yes. In fact, my colleague Mr. Storr and I flew up on the plane today and he showed me an e-mail that he got this morning, which was an e-mail of thanks. What happened was a police officer on a post-traumatic stress disorder website posted that they were going to commit suicide. Mr. Storr's group got an emergency request, could they give them the name associated with this IP address. He provided the name and address information and this morning the thank you note he got told him that a life had been saved as a result.

Those type of events are very common. We get those type of requests all the time.

Mr. Paul Calandra: This might be an unfair question to ask. I guess I can ask both of you. What kind of investments are you talking about? I assume protecting identity is a massive...I don't want to say it's a new problem, but the way people are attacking and getting access to identity now is changing, obviously. What kind of resources...I know you say you have 250 engineers, Colin, but what type of financial investment are you talking of making, both of you, to combat this?

Colin, do you want to start?

Mr. Colin McKay: I think the answer can only be anecdotal because, obviously, we're in a very well-placed position to make significant investments. The reason you see new companies and new software initiatives frequently being the victims of data breaches and large scale criminal enterprise is they don't have the resources to apply to security. They have the barest skills and investments.

We are talking about significant investments in the technical infrastructure. Also there is a skills war for people that understand this space and understand the latest vulnerabilities and how to resolve them. As well, there's the compliance and legal regime that it takes to build the sort of reporting structure that Rogers has just announced today that we have in order to deal with law enforcement requests in a fair, equitable, and rapid manner. It's a sizeable investment.

For us it's one that we're willing to make because we need to maintain our users' trust and provide them with accountability, but honestly it's a continuing challenge. In many cases it's one where you have to share resources between companies as well.

● (1135)

The Chair: Thank you, Mr. Calandra. Your time is up.

I do apologize to everybody for this truncated version of what is otherwise really interesting and important information.

To the Liberals now, Scott Andrews, for five minutes, please.

Mr. Scott Andrews (Avalon, Lib.): Thank you very much, Mr. Chair.

Mr. Engelhart, the 87,000 yes or no requests obviously take a lot of time. Is there a centralized port for these requests in your organization? If it goes beyond a yes or no and it gets to an emergency level, how do you process these internally?

Mr. Kenneth Engelhart: There's a group of professionals that Mr. Storr manages that is staffed 24-7. They do those type of requests and also 911 requests.

Mr. Scott Andrews: You talked about no IP addresses are given. Could you give an example of where an IP address would be given? Under what conditions would an IP address be given?

Mr. Kenneth Engelhart: It's only with a warrant, or if you notice from the numbers, there are 711 child exploitation requests. We will give an IP address with a child exploitation request. The third category is an emergency. Those are the three categories.

Mr. Scott Andrews: The emergency number is 9,000. Do you think that's high or is that reasonable? I did some quick math on it and it's some 25 a day. Is that a reasonable number?

Mr. Kenneth Engelhart: Yes, but you have to realize that these are for the most part from the police. There's another probably five times that number that come from 911 operators which are sometimes police and sometimes not, so it's even bigger than that number, but because those are 911 operators, we don't consider that to be a law enforcement request, but a telephone request. That's why they're not included in that number.

Mr. Scott Andrews: When we hear about identity theft, we hear about people building identities. Quite often, commonly, that's around obtaining an address, a phone number, and all that. Could you shed some light on that, on people trying to gain someone's identity, getting a phone number, and building up this type of identity? Could you then tie that into burner phones and people who are reselling phones? Is that a big issue for identity thieves?

Mr. Kenneth Engelhart: Yes, I would agree with everything that Colin said. There are high-tech breaches or high-tech attacks, and there are also low-tech attacks. We have a huge bunch of engineers and computer scientists who are constantly protecting our networks from attack, but there's also low tech. For example, the Target breach in the U.S., when the information of 40 million customers was stolen, started with someone getting a job as a caretaker at a Target store so that he could attach some devices at night when no one was looking.

That's a real problem, too, when organized crime is infiltrating call centres and infiltrating stores to try to steal identities. You have to be very vigilant about the high-tech stuff and also very vigilant about the low-tech stuff. Then there are the good old-fashioned con artists, who will call the call centre and pretend to be you or pretend to be me. We have to be vigilant with all that too.

Those are the kinds of areas where we're fighting identity theft every day.

Mr. Scott Andrews: Colin, in regard to fictitious e-mail accounts and people setting up fictitious e-mail accounts to establish identity, do you see a lot of this? Do you have a lot of interaction with law enforcement in terms of people setting up these types of accounts to build identities for individuals?

Mr. Colin McKay: I can't speak specifically to whether we've had a relationship with law enforcement about that, but certainly, any open e-mail system provides some level of anonymity or pseudonymity, and you can create an e-mail account under whatever name and specific identity you'd like. There are certain safety measures as you try to build out that relationship with us as a company, because then you start to provide more information about you as an individual, which is harder to fake. It needs more of an element of verification, but it's certainly still quite an easy process to follow through on.

On the tail end, as law enforcement is looking for information about that account, I have to echo what Ken has been saying about the processes Rogers follows. We don't hand over information without a warrant, without a court order, except in a situation where there are exigent circumstances, where there's going to be harm, or specifically in the case of child sexual imagery, where we take as many steps as we can with partners that we have worked with over the long term to shut down that activity and provide information so that the case can be followed up.

● (1140)

The Chair: You have 30 seconds.

Mr. Scott Andrews: Kenneth, on Rogers helping with victim support for people whose identities have been stolen, does Rogers have any mechanisms to support victims of identity theft?

Mr. Kenneth Engelhart: If we have a breach that has happened to one of our customers, we of course inform them right away. Then we will give them free access to credit-limit monitoring so they can monitor their credit score and make sure no one is impersonating them.

Mr. Scott Andrews: Thank you.

The Chair: That's great timing. Thank you very much, Mr. Andrews.

We still have a few minutes left. I've decided that we should go until we can't go any further, so it's the Conservatives' turn, with Mr. Calandra again.

Mr. Paul Calandra: Thank you very much.

Can we inquire with Bell and Telus, before they come, if they actually have something like this?

I don't know if you guys would know if they actually do something like this.

The Chair: We could direct the analysts.

Mr. Kenneth Engelhart: We're the first, so I think they'll put one together now.

Voices: Oh, oh!

Mr. Paul Calandra: That's a very good idea, and it's obviously something we might even consider in our report. I appreciate it.

I just want to go, again, more into the....

I'm sorry. I feel guilty and maybe I should make a disclosure, Mr. Chair. I used to work at Rogers when I was in high school and university, on the telephones trying to put through cable requests. I will admit that even back then—this is the reason I feel guilty—Rogers was really hard core when it came to people's privacy. I thought they had, at that point, one of the most advanced systems I had ever seen.

When I got into the provincial government, I brought government ministers in to see how your systems work—and this was back in 1995 or 1996—to protect people's privacy and make it easier for people to get information. I have always felt that you guys were a leader in that area.

I want to deal with the name and address check again, because this is the one that has caused much of people's concern.

On this side of it, you're basically just confirming something so that police know where they're going. You're just talking about a time-saving mechanism, so that in certain cases the police avoid extraordinary duplicate information or avoid going to multiple sources when they can just come to you and make sure that they get the right information so that they get the warrant. You are still in essence protecting people's charter rights, but you're providing basic information for the police.

Mr. Kenneth Engelhart: That's correct, sir.

Mr. Paul Calandra: Yes, and it's not government widely coming in, snooping, and saying.... Paul Calandra is not calling through to Rogers and saying, this is the information I want. It's just emergency services and government institutions that have legislative power to do so.

Mr. Kenneth Engelhart: Yes. It's primarily police.

Mr. Paul Calandra: Can you just explain, because metadata...? Can either one of you explain what the power of...? I'm again now ultimately embarrassed, because I should.... I keep getting different definitions of what damage this could do.

Colin, or both of you, from your point of view, talk to me about metadata and why I have to be traumatized by it.

Mr. Colin McKay: I think in the context of your study today on identify theft, metadata is an element, but a small element, of what is used to construct an identity. If someone is trying to engage in identity theft, there are very specific pieces of information that they need to know about an individual or need to create concerning an identify in order to create a viable, semi-functioning cyber organism.

Metadata itself is more about the transactions. It's more about your interests. It's more about the transmission of the data. In particular contexts, that can be extremely relevant, as in the case of IP addresses, but it is less relevant in terms of your search preferences, your search results, maybe even your location history. The reason you have heard many different definitions of it is that within the context of whom you're speaking to and within the way it is applied, it can have very many different and many constructive applications.

● (1145)

Mr. Kenneth Engelhart: So, for the telephone system, metadata is not what you say on the call. It is whom you are calling, who called you, and the relationship between the callers. It can even be where you called from.

Metadata is a very useful law enforcement tool. If they think that a person is a suspect and they know that someone else was definitely involved in the crime, if those two people call each other, that is an important tool for the police.

Again, we would only provide metadata with a warrant or an order. We would never provide metadata without a warrant or order.

Mr. Paul Calandra: Okay.

The Chair: We'll have to stop you there. Not only is your five minutes up, but I see that the bells are in fact ringing and the lights are flashing. This isn't an optional thing for us: when the bells go, we have to scamper.

We want to thank both Rogers Communications and Google for taking the time and making the effort to help us as we continue with this very important study. We very much benefited from your input, as always. We offer our thanks to you and your organizations for helping us today.

I'm going to adjourn the meeting, and we won't be reconvening after the votes, ladies and gentlemen. I'll see you on Tuesday.

The meeting is adjourned.