HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 155 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, May 29, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Wednesday, May 29, 2019

● (0835)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): I call to order this meeting of the Standing Committee on Access to Information, Privacy and Ethics. This is meeting 155.

This is the last of our international grand committee meetings this week, the International Grand Committee on Big Data, Privacy and Democracy.

With us today from Amazon, we have Mark Ryland, director of security engineering, office of the chief information officer of the Amazon web services.

From Microsoft Canada Inc., we have Marlene Floyd, national director of corporate affairs, and John Weigelt, national technology officer.

From the Mozilla Foundation, we have Alan Davidson, vice-president of global policy, trust and security.

From Apple Inc., we have Erik Neuenschwander. He is manager of user privacy.

We're going to get into your testimony. I wanted to say that the CEOs were invited today, and it's unfortunate that they didn't come. Again, as I've said to many of you just prior to the meeting, this is supposed to be a constructive meeting on how to make it better, and some of the proposals that your companies have right from the top are good ones, and that's why we wanted to hear them today and have the CEOs answer our questions, but we do appreciate that you're here.

We'll start off with Mr. Ryland for 10 minutes.

Mr. Mark Ryland (Director, Security Engineering, Office of the Chief Information Security Officer for Amazon Web Services, Amazon.com): Thank you very much.

Good morning, Chair Zimmer, members of the committee, and international guests.

My name is Mark Ryland. I serve as the director of security engineering in the office of the chief information security officer at Amazon web services, the cloud computing division of Amazon.

Thank you for giving me the opportunity to speak with you today. I'm pleased to join this important discussion. I'd like to focus my remarks today on how Amazon puts security and customer trust at the centre of everything we do.

Amazon's mission is to be the earth's most customer-centric company. Our corporate philosophy is firmly rooted in working backwards from what customers want and continuously innovating to provide customers better service, more selection and lower prices. We apply this approach across all our areas of business, including those that touch on consumer privacy and cybersecurity.

Amazon has been serving Canadian customers since we first launched amazon.ca in 2002. Amazon now has more than 10,000 full-time employees in Canada. In 2018, we announced plans to create an additional 6,300 jobs.

We also have two tech hubs, one in Toronto and another in Vancouver. These are clusters of offices employing more than 1,000 software engineers and a number of supporting technical workers, building some of our most advanced global systems. We also have offices in Victoria for www.abebooks.com, and our AWS Thinkbox subsidiary in Winnipeg.

We operate seven fulfillment centres in Canada, and four more have been announced. They will all open this year, in 2019.

I would now like to talk about our cloud platform.

Just over 13 years ago, Amazon launched Amazon web services, which is our cloud computing business. Montreal is home to our AWS Canada region, which is made up of a number of distinct data centres. We launched AWS, because after over a decade of building and running amazon.com, we realized we had developed a core competency in operating massively scaled technology infrastructure and data centres. We embarked on a broader mission of serving developers and businesses with information technology services that they can use to run their own businesses.

The term “cloud computing” refers to the on-demand delivery of IT resources over the Internet or over private networks. The AWS cloud spans a network of data centres across 21 geographic regions around the globe. Instead of owning and maintaining their own data centres, our customers can acquire technology such as compute power, storage, and databases in a matter of seconds on an as-needed basis by simply calling an API or clicking a mouse on a graphical console.

We provide IT infrastructure and services in the same way that you just flip a switch to turn on the lights in your home and the power company sends you electricity.

One of this committee's concerns was democracy. Well, we're really democratizing access to IT services, things that only very large organizations could previously do, in terms of the scale involved. Now the smallest organizations can get access to that same type of very sophisticated advanced technology with simply a click of a button and just paying for their consumption.

Today AWS provides IT services to millions of active customers in over 190 countries. Companies that leverage AWS range from large Canadian enterprises such as Porter Airlines, Shaw, the National Bank of Canada, TMX Group, Corus, Capital One, and Blackberry to innovative start-ups like Vidyard and Sequence Bio.

I want to underline that privacy really starts with security. Privacy regulations and expectations cannot be met unless systems are maintaining the confidentiality of data according to their design. At AWS, we say that security is “job zero”, by which we mean it's even more important than a number one priority. We know that if we don't get security right, we don't really have a business.

AWS and Amazon are vigilant about the security and privacy of our costumers and have implemented sophisticated technical and physical measures to prevent unauthorized access to data.

Security is everyone's responsibility. While we have a world-class team of security experts monitoring our systems 24-7 to protect customer data, every AWS employee, regardless of role, is responsible for ensuring that security is an integral component of every facet of our business.

Security and privacy are a shared responsibility between AWS and the customer. What that means is that AWS is responsible for the security and privacy of the cloud itself, and customers are responsible for their security and the privacy of their systems and their applications that run in the cloud. For example, customers should consider the sensitivity of their data and decide if and how to encrypt their data. We provide a wide variety of encryption tools and guidance to help customers meet their cybersecurity objectives.

We sometimes say, “Dance like no one's watching. Encrypt like everyone is.” Encryption is also helpful when it comes to data privacy. In many cases, data can be effectively and permanently erased simply by deleting encryption keys, for example.

● (0840)

More and more, organizations are realizing the link between IT modernization offered by the cloud and a better security posture. Security depends on the ability to stay a step ahead of a rapidly and continuously evolving threat landscape, requiring both operational agility and the latest technologies.

The cloud offers many advanced security features that ensure that data is securely stored and handled. In a traditional on-premises environment, organizations spend a lot of time and money managing their own data centres, and worry about defending themselves against a complete range of nimble, continuously evolving threats that are difficult to anticipate. AWS implements baseline protections, such as DDoS protection, or distributed denial of service protection; authentication; access control; and encryption. From there, most organizations supplement these protections with added security measures of their own to bolster cloud data protections and tighten access to sensitive information in the cloud. They also have many tools at their disposal for meeting their data privacy goals.

As the concept of “cloud” is often new to people, I want to emphasize that AWS customers own their own data. Customers choose the geographic location in which to store their data in our highly secure data centres. Their data does not move unless the customer decides to move it. We do not access or use our customers' data without their consent.

Technology is an important part of modern life, and has the potential to offer extraordinary benefits that we are just beginning to realize. Data-driven solutions possess potentially limitless opportunities to improve the lives of people, from making far faster medical diagnoses to making farming far more efficient and sustainable. In addressing emerging technology issues, new regulatory approaches may be required, but they should avoid harming incentives to innovate and avoid constraining important efficiencies like economies of scale and scope.

We believe policy-makers and companies like Amazon have very similar goals—protecting consumer trust and privacy and promoting new technologies. We share the goal of finding common solutions, especially during times of fast-moving innovation. As technology evolves, so too will the opportunities for all of us in this room to work together.

Thank you. I look forward to taking your questions.

The Chair: Thank you, Mr. Ryland.

Next up is Microsoft. Will it be Ms. Floyd or Mr. Weigelt?

Ms. Marlene Floyd (National Director, Corporate Affairs, Microsoft Canada Inc.): We will share.

The Chair: Okay. Go ahead.

[*Translation*]

Mr. John Weigelt (National Technology Officer, Microsoft Canada Inc.): Thank you, Mr. Chair.

We're pleased to be here today.

[*English*]

My name is John Weigelt. I'm the national technology officer for Microsoft here in Canada. My colleague Marlene Floyd, national director of corporate affairs for Microsoft Canada, joins me. We appreciate the opportunity to appear before this committee today. The work you've undertaken is important given our increasingly digital world and the impact of technology on jobs, privacy, safety, inclusiveness and fairness.

Since the establishment of Microsoft Canada in 1985, our presence here has grown to include 10 regional offices around the country, employing more than 2,300 people. At our Microsoft Vancouver development centre, over 700 employees are developing products that are being used around the world. Cutting-edge research on artificial intelligence is also being conducted by Ph.D.s and engineers at the Microsoft research lab in Montreal. That's in partnership with the universities there.

Powerful technologies like cloud computing and artificial intelligence are transforming how we live and work, and are presenting solutions to some of the world's most pressing problems. At Microsoft we are optimistic about the benefits of these technologies but also clear-eyed about the challenges that require thinking beyond technology itself to ensure the inclusion of strong ethical principles and appropriate laws. Determining the role that technology should play in society requires those in government, academia, business and civil society to come together to help shape the future.

Over 17 years ago, when Bill Gates asserted that “trustworthy computing” would be the highest priority at Microsoft, he dramatically changed how our company delivers solutions to the marketplace. This commitment was re-emphasized by our CEO, Satya Nadella, in 2016. We believe privacy is a fundamental human right. Our approach to privacy and data protection is grounded in our belief that customers own their own data. Consequently, we protect our customers' privacy and provide them with control over their data.

We have advocated for new privacy laws in a number of jurisdictions, and we were early supporters of the GDPR in Europe. We recognize that for governments, having computer capacity close to their constituents is very important. Microsoft has data centres in more regions than any other cloud provider, with over 100 data centres located in over 50 regions around the world. We're quite proud that two of these data centres are located here in Canada, in Ontario and Quebec.

Protecting our customers and the wider community from cyber-threats is a responsibility we take very seriously. Microsoft continues to invest over $1 billion each year in security research and development, with thousands of global security professionals working with our threat intelligence centre, our digital crimes unit, and our cyber-defence operations centre. We work closely with the Government of Canada's recently announced Canadian Centre for Cyber Security. We have partnered with governments around the world under the government security program, working towards technical information exchanges, threat intelligence sharing and even co-operative botnet takedowns. Further, Microsoft led the Cybersecurity Tech Accord, signed by over 100 global organizations that came together to defend all customers everywhere from malicious cyber-attacks and to do more to keep the Internet safe.

● (0845)

Ms. Marlene Floyd: Microsoft was also proud to be a signatory to the Paris call for trust and security in cyberspace announced in November by French President Emmanuel Macron at the Paris peace summit. With over 500 signatories, it is the largest ever multi-stakeholder commitment to principles for the protection of cyberspace.

Another focus of your committee has been the increasing interference by bad actors in the democratic processes of numerous countries around the world. We fully agree that the tech sector needs to do more to help protect the democratic process. Earlier this week, we were pleased to endorse the Canada declaration on electoral integrity announced by Minister Gould.

Microsoft has taken action to help protect the integrity of our democratic processes and institutions. We have created the Defending Democracy program, which works with stakeholders in democratic countries to promote election integrity, campaign security and disinformation defence.

As part of this program, Microsoft offers a security service called AccountGuard at no cost to Office 365 customers in the political ecosystem. It is currently offered in 26 countries, including Canada, the U.S., the U.K., India, Ireland and most other EU countries. It's currently protecting over 36,000 email accounts. Microsoft AccountGuard identifies and warns individuals and organizations of cyber-threats, including attacks from nation-state actors. Since the launch of the program, it has made hundreds of threat notifications to participants.

We have also been using technology to ensure the resiliency of the voting process. Earlier this month, we announced ElectionGuard, a free, open-source software development kit aimed at making voting more secure by providing end-to-end verification of elections, opening results to third party organizations for secure validation, and allowing individual voters to confirm that their votes were counted correctly.

At Microsoft, we're working hard to ensure that we develop our technologies in ways that are human-centred and that allow for broad and fair access by everyone. The rapid advancement of compute power and the growth of AI solutions will help us be more productive in nearly every field of human endeavour and will lead to greater prosperity, but the challenges need to be addressed with a sense of shared responsibility. In some cases this means moving more slowly in the deployment of a full range of AI solutions while working thoughtfully and deliberately with government officials, academia and civil society.

We know that there is more that we need to do to continue earning trust, and we understand that we will be judged by our actions, not just our words. Microsoft is committed to continuing to work in deliberate and thoughtful partnership with government as we move forward in this digital world.

Thank you, and we're happy to receive your questions.

The Chair: Thank you, Ms. Floyd.

We'll go next to Mr. Davidson from Mozilla.

Mr. Alan Davidson (Vice-President, Global Policy, Trust and Security, Mozilla Corporation): Members of the grand committee and the standing committee, thank you.

I'm here today because all is not well with the Internet. For sure the open Internet is the most powerful communications medium we've ever seen. At its best, it creates new chances to learn to solve big problems to build a shared sense of humanity, and yet we've also seen the power of the Internet used to undermine trust, magnify divisiveness and violate privacy. We can do better, and I'm here to share a few ideas about how.

My name is Alan Davidson. I'm the vice-president for policy, trust and security at the Mozilla Corporation. Mozilla is a fairly unusual entity on the Internet. We're entirely owned by a non-profit, the Mozilla Foundation. We're a mission-driven open-source software company. We make the Firefox web browser, Pocket and other services.

At Mozilla we're dedicated to making the Internet healthier. For years we've been champions of openness and privacy online, not just as a slogan but as a central reason for being. We try to show by example how to create products to protect privacy. We build those products not just with our employees but with thousands of community contributors around the world.

At Mozilla we believe the Internet can be better. In my time today, I would like to cover three things: first, how privacy starts with good product design; second, the role of privacy regulation; and third, some of the content issues that you folks have been talking about for the last few days.

First off, we believe our industry can do a much better job of protecting privacy in our products. At Mozilla we're trying to do just that. Let me give you one example from our work on web tracking.

When people visit a news website, they expect to see ads from the publisher of that site, from the owner of that website. When visitors to the top news sites, at least in the U.S., visit, they encounter dozens of third party trackers, trackers from sites other than the one that they're visiting, sometimes as many as 30 or 40. Some of those trackers come from household names and some of them are totally obscure companies that most consumers have never heard of.

Regardless, the data collected by these trackers is creating real harm. It can enable divisive political ads. It can shape health insurance decisions and is being used to drive discrimination in housing and jobs. The next time you see a piece of misinformation online, ask yourself where the data came from that suggested that you would be such an inviting target for that misinformation.

At Mozilla we've set out to try to do something about tracking. We created something we call the Facebook container, which greatly limits what Facebook can collect from you when you're browsing on Firefox. It's now, by the way, one of the most popular extensions that we've ever built. Now we're building something called enhanced tracking protection. It's a major new feature in the Firefox browser that blocks almost all third party trackers. This is going to greatly limit the ability of companies that you don't know to secretly track you as you browse around the web.

We're rolling it out to more people, and our ultimate goal is to turn it on by default for everybody. I emphasize that because what we've learned is that creating products with privacy by default is a very powerful thing for users, along with efforts like our lean data practices, which we use to limit the data that we collect in our own product. It's an approach that we hope others adopt, because we've learned that it's really unrealistic to expect that users are going to sort through all of the privacy policies and all the different options that we can give them to protect themselves. To make privacy real, the burden needs to shift from consumers to companies. Unfortunately, not everybody in our industry believes that.

Let me turn to my second point, which is that we believe that regulation will be an essential part of protecting privacy online. The European Union has been a leader in this space. Many other companies around the world are now following suit and trying to build their own new data protection laws. That's important because the approach we've had for the last two decades in our industry is clearly not working anymore. We've really embraced in the past this notion of notice and choice: If we just tell people what we're going to collect and let them opt out, surely they'll be fine. What we found is that this approach is really not working for people. We've been proponents of these new data protection rules, and we hope you will be too.

We believe that a good privacy law should have three main components. It needs clear rules for companies about what they can collect and use; it should have strong rights for individuals, including granular and revocable consent about specific uses; and it should be implemented within an effective and empowered enforcement agency, which is not always the case. We think that's an important component.

● (0850)

Critically, we believe that you can build those laws and you can include those components while still preserving innovation and the beneficial uses of data. That's why we're supporting a new federal privacy law in the U.S. and we're working with regulators in India, Kenya and in other places to promote those laws.

My third point is that given the conversation you have all had for the last few days, I thought it would be useful to touch on at least some of our views on the big issues of content regulation. Of all the issues being examined by the committee, we believe that this is the most difficult.

We've seen that the incentives for many in the industry encourage the spread of misinformation and abuse, yet we also want to be sure that our reactions to those real harms do not themselves undermine the freedom of expression and innovation that have been such a positive force in people's lives on the Internet.

We've taken a couple of different approaches at Mozilla. We're working right now on something we call “accountability processes”. Rather than focusing on individual pieces of content, we should think about the kinds of processes that companies should have to build to attack those issues. We believe that this can be done with a principles-based approach. It's something that's tailored and proportionate to different companies' roles and sizes, so it won't disproportionately impact smaller companies, but it will give more responsibility to larger companies that play a bigger role in the ecosystem.

We've also been really engaged in the issues around disinformation, particularly in the lead-up to the EU parliamentary elections that just happened. We're signatories to the EU Code of Practice on Disinformation, which I think is a very important and useful self-regulatory initiative with commitments and principles to stop the spread of disinformation. For our part, we've tried to build tools in Firefox to help people resist online manipulation and make better choices about and understand better what they're seeing online.

We've also made some efforts to push our fellow code signatories to do more about transparency and political advertising. We think a lot more can be done there. Candidly, we've met with mixed results from some of our colleagues. I think there is much more room to improve the tools, particularly the tools that Facebook has put out there for ad transparency. There is maybe some work that Google could do, too. If we can't do that, the problem is that we'll need stronger action from government. Transparency should be a good starting point for us.

In conclusion, I'd say that none of these issues being examined by the committee are simple. The bad news is that the march of technology—with artificial intelligence, the rise of the Internet of things and augmented reality—is only going to make it harder.

A concluding thought is that we really need to think about how we build our societal capacity to grapple with these problems. For example, at Mozilla we've been part of something called the responsible computer science challenge, which is designed to help train the next generation of technologists to understand the ethical implications of what they're building. We support an effort in the U. S. to bring back the Office of Technology Assessment to build out government's capacity to better understand these issues and work more agilely. We're working to improve the diversity in our own company and our industry, which is essential if we're going to build capacity to address these issues. We publish something every year called the “Internet Health Report”, which just came out a couple of weeks ago. It's part of what we view as the massive project we all have to help educate the public so that they can address these issues.

These are just some of the examples and ideas we have about how to work across many different levels. It's designing better products, improving our public regulations and investing in our capacity to address these challenges in the future.

We really thank you for the opportunity to speak with you today and we look forward to working with you and your colleagues around the world to build a better Internet.

Thanks.

● (0855)

The Chair: Thank you, Mr. Davidson.

Last up, from Apple Inc., we have Erik Neuenschwander, please. You have 10 minutes.

Mr. Erik Neuenschwander (Manager of User Privacy, Apple Inc.): Thank you.

Good morning, members of the committee, and thank you for inviting me to speak with you today about Apple's approach to privacy and data security.

My name is Erik Neuenschwander, and I've been a software engineer at Apple for 12 years. I worked as the first data analysis engineer on the first iPhone. I managed the software performance team on the first iPad, and I founded Apple's privacy engineering team. Today I manage that team responsible for the technical aspects of designing Apple's privacy features. I'm proud to work at a company that puts the customer first and builds great products that improve people's lives.

At Apple we believe that privacy is a fundamental human right, and it is essential to everything we do. That's why we engineer privacy and security into every one of our products and services. These architectural considerations go very deep, down to the very physical silicon of our devices. Every device we ship combines software, hardware and services designed to work together for maximum security and a transparent user experience. Today I look forward to discussing these key design elements with you, and I would also refer the committee to Apple's privacy website, which goes into far more detail about these and other design considerations in our products and services.

The iPhone has become an essential part of our lives. We use it to store an incredible amount of personal information: our conversations, our photos, our notes, our contacts, our calendars, financial information, our health data, even information about where we've been and where we are going. Our philosophy is that data belongs to the user. All that information needs to be protected from hackers and criminals who would steal it or use it without our knowledge or permission.

That is why encryption is essential to device security. Encryption tools have been offered in Apple's products for years, and the encryption technology built into today's iPhone is the best data security available to consumers. We intend to stay on that path, because we're firmly against making our customers' data vulnerable to attack.

By setting up a device passcode, a user automatically protects information on their device with encryption. A user's passcode isn't known to Apple, and in fact isn't stored anywhere on the device or on Apple's servers. Every time, it belongs to the user and the user alone. Every time a user types in their passcode, iPhone pairs that input with the unique identifier that iPhone fuses into its silicon during fabrication. iPhone creates a key from that pairing and attempts to decrypt the user's data with it. If the key works, then the passcode must have been correct. If it doesn't work, then the user must try again. We designed iPhone to protect this process using a specially designed secure enclave, a hardware-based key manager that is isolated from the main processor and provides an additional layer of security.

As we design products, we also challenge ourselves to collect as little customer data as possible. While we want your devices to know everything about you, we don't feel that we should.

For example, we've designed our hardware and software to work together to provide great features by efficiently processing data without that data ever leaving the user's device. When we do collect personal information, we are specific and transparent about how it will be used, because user control is essential to the design of our products. For example, we recently added a privacy icon that appears on Apple devices when personal information is collected. The user can tap on it to learn more about Apple's privacy practices in plain language.

We also use local differential privacy, a technique that enables Apple to learn about the user community without learning about individuals within that community. We have pioneered just-in-time notices, so that when third party apps seek to access certain types of data, a user is given meaningful choice and control over what information is collected and used. This means third party apps cannot access users' data like contacts, calendars, photos, the camera or the microphone without asking for and obtaining explicit user permission.

These and other design features are central to Apple. Customers expect Apple and other technology companies to do everything in our power to protect personal information. At Apple we are deeply committed to that because our customers' trust means everything to us. We spend a lot of time at Apple thinking about how we can provide our customers not only with transformative products, but also with trusted, safe and secure products. By building security and privacy into everything we do, we've proved that great experiences don't have to come at the expense of privacy and security. Instead, they can support them.

I'm honoured to participate in this important hearing. I look forward to answering your questions.

Thank you.

● (0900)

The Chair: Thank you, Mr. Neuenschwander.

We'll start with questions from committee members. My colleague Damian Collins will be here shortly. He regrets he had another thing to attend to.

We'll start with Mr. Erskine-Smith for five minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much.

Thank you all for your presentations. I know Microsoft supports the GDPR and stronger privacy rules. Obviously, Tim Cook has been public in support of the GDPR. Amazon, do you also support the GDPR?

Mr. Mark Ryland: We support the privacy principles of user control, consent and so forth. We think the actual legislation is new enough and creates some burdens that we don't think directly impact user privacy in a positive way. While we're fully compliant and fully supportive of the principles, we don't necessarily think it's something that should be applied universally at this point.

Mr. Nathaniel Erskine-Smith: Support of the principles includes the principle of data minimization.

Mr. Mark Ryland: Yes, as well as user control. That's really the key principle.

Mr. Nathaniel Erskine-Smith: Microsoft, would you agree with the principle of data minimization?

Mr. John Weigelt: Yes, we would.

Mr. Nathaniel Erskine-Smith: Good.

With respect to consumer privacy protection, one way to better protect consumer privacy is to have additional opt-in consents that are explicit for secondary purposes. For example, with Amazon's Echo, California was proposing smart speaker rules that there would have to be opt-in consents for that information to be stored. Do you agree with those rules?

● (0905)

Mr. Mark Ryland: We believe that the user experience should be very smooth and clear, and that people's expectations should be very reasonably met. For example, with the Echo device, you use a mobile application to set up your device, and it makes it very clear what the privacy rules are.

Mr. Nathaniel Erskine-Smith: Is there an explicit opt-in consent for recording of those conversations?

Mr. Mark Ryland: It's not an explicit opt-in consent, but it makes it clear about the recordings and it gives you full control over the recordings. It gives a full list of recordings and the ability to delete any particular one, or all of them. It's a very explicit and clear user interface for that.

Mr. Nathaniel Erskine-Smith: If the GDPR were in effect, there would be a requirement for explicit opt-in consent.

Mr. Mark Ryland: Possibly. There may be legal rulings that we.... That's part of the issue. A lot of specifics are unclear until there are more regulatory or judicial findings about what the exact meaning of some of the general principles is.

Mr. Nathaniel Erskine-Smith: Representative from Apple, does Apple engage in web tracking?

Mr. Erik Neuenschwander: We don't have the kind of destinations around the Internet that do that kind of web tracking. Of course, with our online store, for example, we have a direct first-party relationship with users who visit our sites.

Mr. Nathaniel Erskine-Smith: There's probably a reasonable expectation that when I visit the Apple site, I know that Apple's going to want to communicate with me afterwards, but if I'm visiting other non-related sites around the Internet, Apple wouldn't be tracking me.

Mr. Erik Neuenschwander: We're not, and in fact our intelligent tracking prevention is on by default in our Safari web browser, so even if Apple were to attempt that, intelligent tracking prevention would seek to prevent it.

Mr. Nathaniel Erskine-Smith: Microsoft and Amazon, are you similar to Apple, or do you engage in web tracking on a wide variety of websites across the Internet?

Mr. Mark Ryland: We are involved in the web ecosystem, with the ability to understand where people have come from and where they're going from our site.

Again, our primary business model is selling products to customers, so that's not the way we monetize our business.

Mr. Nathaniel Erskine-Smith: Was that a yes to web tracking, fairly broadly?

Mr. Mark Ryland: We participate in the advertising ecosystem, so yes.

Mr. Nathaniel Erskine-Smith: I think that's a yes.

Microsoft, would you comment?

Mr. John Weigelt: We have our properties, as do the other communities. We have the Microsoft store and the MSN properties, so we are able to determine where our customers are coming from.

Mr. Nathaniel Erskine-Smith: The reason I ask is that we had an individual yesterday talking about how consent in some cases isn't good enough, and in some cases, I understand that. I'm a reasonably busy person, so I can't be expected to read every agreement about terms and conditions; I can't be expected to read all of them. If secondary consents are in every single app I use and I have to agree to 10 different consents, am I really going to be able to protect my own personal information? I don't think we should expect that of consumers, which is why we have consumer protection law and implied warranties in other contexts.

McNamee yesterday suggested that some things should strictly be off the table. I put it to Google that maybe Google shouldn't be able to read my emails and target me based on ads—that should be off the table. Do you think, Apple, that certain things should just be off the table?

Mr. Erik Neuenschwander: Yes, when we.... Our iCloud service is a place where users can store their photos or documents with Apple, and we are not mining that content to build profiles about our users. We consider it the user's data. We're storing it on our service, but it remains the user's data.

Mr. Nathaniel Erskine-Smith: Similarly, Microsoft and Amazon: Do you think certain data collection should simply be off the table completely?

Mr. John Weigelt: One of the things we feel strongly about is users having visibility into what data they have shared with particular organizations. We've worked very closely—I have personally worked very closely—with information privacy commissioners across Canada to talk about the consent environment and what consent means. As we rolled out tools like Cortana, for example, we worked with the federal Privacy Commissioner's office to understand which of the 12 stages of consent for consumers were particularly important.

Mr. Nathaniel Erskine-Smith: But I'm suggesting that beyond consent, certain things be off the table. For example, my personal pictures on my phone—should those be able to be scanned, and then I get targeted ads?

Mr. John Weigelt: To be clear, we don't scan that information—

Mr. Nathaniel Erskine-Smith: Well, I know you don't—

Mr. John Weigelt: —however, we do provide—

Mr. Nathaniel Erskine-Smith: —but should certain things be off the table? That is my point.

Mr. John Weigelt: —visibility to customers so that they understand where their data is being used and give them full control.

Our privacy dashboard, for example, allows you to see what data is resident within the Microsoft environment and then you're able to control that and be able to manage that in a better fashion. It's all about having that user interaction so that they understand the value proposition of being able to share those things.

Mr. Nathaniel Erskine-Smith: Amazon, should certain things just be off the table?

Mr. Mark Ryland: I don't think you can say, a priori, that certain things are always inappropriate, because again, the customer experience is key, and if people want to have a better customer experience based on data that they share.... Consent, obviously, and control are critical.

Mr. Nathaniel Erskine-Smith: Let's take the case of kids under the age of 18, for example. Maybe we should not be able to collect information about kids under the age of 18, or under 16, or under 13.

Kids, let's say. Should that be off the table?

● (0910)

Mr. Mark Ryland: We're going to comply with all of the laws of the countries where we operate, if that is—

Mr. Nathaniel Erskine-Smith: Are you saying you don't have a view on an ethical basis with respect to collecting information from kids?

Mr. Mark Ryland: We certainly have a view that parents should be in charge of children's online experience, and we give parents the full control in our systems for that experience.

Mr. Nathaniel Erskine-Smith: Thanks very much.

It's so hard to say yes.

The Chair: We will go to Peter next, for five minutes.

Hon. Peter Kent (Thornhill, CPC): Thank you, Chair.

Thanks to all of our witnesses for appearing today.

My first question is for Mr. Ryland at Amazon.

In September of last year, your vice-president and associate general counsel for Amazon, Mr. DeVore, testified before a U.S. Senate committee and was very critical, I think it's fair to say, of the California consumer act that was passed.

Among the new consumer rights in that act that he was critical of was the right for users to know all of the business data that is collected about a user and the right to say no to the sale of that business data. It provides, in California, the right to opt out of the sale of that data to third parties. He said the act was enacted too quickly and that the definition of personal information was too broad.

I wonder if you could help us today by giving us Amazon's definition of protectable personal information.

Mr. Mark Ryland: First of all, let me say that I work in Amazon web services on our security and privacy of our cloud platform. I'm not a deep expert broadly across all of our privacy policies.

However, I will say that certain elements of consumer data are used in the core parts of business. For example, if we sell a product to a customer, we need to track some of that data for tax purposes and for other legal purposes, so it's impossible to say that a consumer has complete control over certain things. There are other legal reasons that data must sometimes be retained, for example.

Hon. Peter Kent: Have you had any users request or ask about the user data that has been collected about them and whether it has been sold?

Mr. Mark Ryland: Yes, absolutely.

First of all, we do not sell our customer data. Full stop.

Second, we have a privacy page that shows you all the data we have accumulated about you—your order history, digital orders, book orders, etc. We have a whole privacy page for our Alexa Voice Service. All that gives users control and insight into the data we're utilizing.

Hon. Peter Kent: Then despite Mr. DeVore's criticism, Amazon is complying with the California act and, I would assume, would comply with any other legislation passed anywhere in the world that was similar.

Mr. Mark Ryland: We will always comply with the laws that apply to us wherever we do business. Absolutely.

Hon. Peter Kent: Thank you.

I'd like to ask a question now to Mr. Davidson about Mozilla.

I know that Mozilla, with all of its good practices and its non-profit public benefit mandate, does work with Google and with Bing. I'm just wondering how you establish firewalls for user data accumulation that those two organizations would otherwise collect and monetize.

Mr. Alan Davidson: It's a great question. It's pretty simple for us. We just don't send data to them beyond what they would normally get from a visitor who visits their website—the IP address, for example, when a visitor comes and visits them.

We make a practice of not collecting any information. If you're using Firefox and you do a search on Bing or on Google, we don't collect anything, we don't retain anything and we don't transmit anything special. That has allowed us to distance ourselves, honestly, and we have no financial incentive to collect that information.

Hon. Peter Kent: I have a question for Mr. Neuenschwander.

In September of last year, the news broke that the Mac application Adware Doctor, which was supposed to protect Apple users from privacy threats, was in fact recording those users' data and delivering them to a server in China. Apple shut that down, but for how long was that exposure up? Have you determined who exactly was operating that server in China?

Mr. Erik Neuenschwander: I remember that event and the action the App Store team took on it. Off the top of my head, I don't remember exactly the exposure. I'd be happy to go back and look up that information and get back to you with it.

● (0915)

Hon. Peter Kent: You're unaware of how long the exposure—

Mr. Erik Neuenschwander: At this time, I don't remember exactly how long that exposure was.

Hon. Peter Kent: This was, I understand, a very popular Mac application. How thoroughly do you research those applications in the reasonable capitalist rush to monetize new wonders?

Mr. Erik Neuenschwander: For applications that are free on the store, there's no monetization for Apple in the App Store.

Since we introduced the App Store, we've had both a manual review and, in more recent years, added an automated review of every application that's submitted to the store, and then for every update of the applications on the store. Those applications undergo a review by a dedicated team of experts on the App Store side.

There is a limit that we don't go past, which is that we don't surveil our users' usage of the applications. Once the application is executing on a user's device, for that user's privacy we don't go further and take a look at the network traffic or the data that the user is sending. That would seem creepy to us.

We continue to invest on the App Store side to try to have as strong a review as we can. As applications and their behaviours change, we continue to enhance our review to capture behaviours that don't match our strong privacy policies on the stores.

Hon. Peter Kent: For Microsoft and Ms. Floyd, in 2013 the European Commission fined Microsoft in the amount of some €561 million for non-compliance with browser choice commitments. There doesn't seem to have been any violation since. Does that sort of substantial fine teach lessons? We're told that even hundreds of millions of dollars or hundreds of millions of euros—even into the billion-dollar mark—don't discourage the large digital companies. I'm wondering about compliance and the encouragement to compliance by substantial financial penalties, which we don't have in Canada at the moment.

Mr. John Weigelt: As we mentioned, trust is the foundation of our business. Any time there's a negative finding against our organization, we find that the trust is eroded, and it ripples throughout the organization, not only from the consumer side but also on the enterprise side.

That fine was substantive, and we addressed the findings by changing how we deliver our products within the marketplace, providing the choice to have products without that browser in place.

When we look at order-making powers here in Canada or whatnot, we can see that having that negative finding will really impact the business far more broadly than some of those monetary fines.

Hon. Peter Kent: Would you encourage the Canadian government to stiffen its regulations and penalties for non-compliance with privacy protection?

Mr. John Weigelt: I would encourage the Canadian government to have the voice you have around how technologies are delivered within the Canadian context. We have people here locally who are there to hear that and change the way we deliver our services.

Hon. Peter Kent: Thank you.

The Chair: Go ahead, Mr. Angus, for five minutes.

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you, Mr. Chair.

I was talking to my friend at Apple about how I bought my first Mac Plus in 1984 with a little 350k floppy disk, and I saw it as a revolutionary tool that was going to change the world for the better. I still think it has changed the world for the better, but we are seeing some really negative impacts.

Now that I'm aging myself, back in the eighties, imagine if Bell Telephone listened in on my phone. They would be charged. What if they said, “Hey, we're just listening in on your phone because we want to offer you some really nifty ideas, and we'll have a better way to serve you if we know what you're doing”? What if the post office read my mail before I got it, not because they were doing anything illegal but because there might be some really cool things that I might want to know and they would be able to help me? They would be charged.

Yet in the digital realm, we're now dealing with companies that are giving us all these nifty options. This was where my colleague Mr. Erskine-Smith was trying to get some straight answers.

I think that as legislators, we're really moving beyond this talk about consent. Consent has become meaningless if we are being spied on, if we're being watched and if our phone is tracking us. Consent is becoming a bogus term, because it's about claiming space in our lives that we have not given. If we had old school rules, you would not be able to listen in on our phones and not be able to track us without our rights, yet suddenly it's okay in the digital realm.

Mr. Davidson, I'm really interested in the work that Mozilla does.

Is it possible, do you think, for legislators to put some principled ground rules down about the privacy rights of citizens that will not completely destroy Silicon Valley and they will not all be going on welfare and the business model will still be able to succeed. Is it possible for us to put simple rules down?

● (0920)

Mr. Alan Davidson: Yes.

I can say more.

Mr. Charlie Angus: Say more.

Mr. Alan Davidson: I think that actually—

Mr. Charlie Angus: I love it when someone agrees with me.

Mr. Alan Davidson: We were looking for some yeses.

You've heard examples already. We firmly believe that you can build good and profitable businesses and still respect people's privacy. You've heard some examples today. You've heard some examples from us. You can see good examples of laws that are out there, including the GDPR.

There are things that are probably beyond the pale, for which we need to have either clear prohibitions or really strong safeguards. I would say that I wouldn't totally reject consent. What we need is more granular consent, because I think people don't really understand—

Mr. Charlie Angus: Explicit consent.

Mr. Alan Davidson: —explicit consent.

There are lots of different ways to frame it, but there is a more granular kind of explicit consent. That's because there will be times when some people will want to take advantage of health apps or sharing their location with folks and with their family. They should be able to do that, but they should really understand what they're getting themselves into.

We believe that you can still build businesses that do that.

Mr. Charlie Angus: Thank you.

Some of the concerns we've been looking at are in trying to get our heads around AI. This is the weaponization of digital media. AI could have a very positive role, or it could have a very negative role.

Mr. Ryland, certainly Amazon has really moved heavily in terms of AI. However, Amazon has also been noted as a company with 21st century innovation and 19th century labour practices.

With regard to the allegations that workers were being monitored right down to the level of being fired by AI tracking, is that the policy of Amazon?

Mr. Mark Ryland: Certainly our policy is to respect the dignity of our workforce and to treat everyone in a proper fashion.

I don't know the specifics of that allegation, but I'd be happy to get back to you with more information.

Mr. Charlie Angus: It was a pretty famous article about Amazon. It said that right down to the seconds, the workers were being monitored by AI, and those who were too slow were being fired.

I may be old school, but I would think that this would be illegal under the labour laws in our country. That is apparently how AI is being used in the fulfillment centres. That, to me, is a very problematic misuse of AI. Are you not aware of that?

Mr. Mark Ryland: I'm not aware of that, and I'm almost certain that there would be human review of any decisions. There's no way we would make a decision like that without at least some kind of human review of machine-learning types of algorithms.

Mr. Charlie Angus: It was a pretty damning article, and it was covered in many international papers.

Would you be able to get back to our committee and get us a response?

Mr. Mark Ryland: I would be happy to follow up with that.

Mr. Charlie Angus: I don't want to put you on the spot here, but I'd rather get a response on this. I think we would certainly want to get a sense of Amazon's perspective on how it uses AI in terms of the monitoring of the workers within the fulfillment centres. If you could get that to our committee, it would be very helpful.

Mr. Mark Ryland: I will do that.

The Chair: Thank you, Mr. Angus.

We'll go next to our delegation.

We'll start off with Singapore.

Go ahead, for five minutes.

Ms. Sun Xueling (Senior Parliamentary Secretary, Ministry of Home Affairs and Ministry of National Development, Parliament of Singapore): Thank you, Mr. Chair.

I have some questions for Mr. Alan Davidson.

I was reading the Mozilla Manifesto with interest. I guess I had some time. I think there are 10 principles in your manifesto. Specifically on principle 9, it reads that "Commercial involvement in the development of the internet brings many benefits; a balance between commercial [benefit] and public benefit is critical."

That's what principle 9 says.

Would you agree, then, that tech companies, even with the desire for growth and profitability, should not abdicate their responsibility to safeguard against abuse of their platforms?

Mr. Alan Davidson: We absolutely agree with that. I would say that the manifesto, for those who haven't seen it, is really like our guiding principles. It was written almost 15 years ago. We just updated it with a new set of things we've added on to it to respond to modern times.

We think, yes, that balance is really important, and I think companies need to be thinking about the implications of what they're building. I also think government needs to put guardrails around it, because what we've seen is that not all companies will do that. Some companies need guidance.

Ms. Sun Xueling: Also, I think there was an Internet health report that Mozilla Foundation put out, and I'd like to thank your organization, a non-profit working for the public benefit. I think the Cambridge Analytica scandal was referred to, and your report says that the scandal is a symptom of a much larger systemic issue, that the dominant business model and currency of today's digital world is actually based on gathering and selling data about us.

Would you agree, then, that the Cambridge Analytica scandal somehow demonstrates a mindset whereby the pursuit of profit and the pursuit for company growth had somewhat been prioritized over civic responsibility?

● (0925)

Mr. Alan Davidson: Yes, but our hope is that some of those are isolated instances. I would just say that not every company operates that way. There are, I think, companies that are trying to do the right thing for the user, trying to put their users first, and it's not just for altruistic purposes; I think it's because many of us believe that you build a better business and in the long term should be rewarded in the market if you put your users first.

Ms. Sun Xueling: We also heard testimony yesterday. I think many of the grand committee members had spoken with businesses who talked about examples around Sri Lanka or Nancy Pelosi. It seemed that it was more about putting information out there, freedom of reach rather than real protection of freedom of speech, because there's no real freedom of speech if it is founded on false information or misleading information.

While we like to think that the Cambridge Analytica scandal is a one-off, I think our concern is that the existing business models of these corporate entities do not seem to give us the confidence that civic responsibility would be seen in the same light as company profits. I think that's where I'm coming from.

Mr. Alan Davidson: As somebody who has been in this space for a long time, it is really disappointing to see some of those behaviours online. I do think that part of it has been the evolution of these business models, especially the ones that reward engagement as a major overriding metric. Our hope is that companies will do more and do better.

There is a risk in too much government intervention in this space, because we do want to make sure that we respect free expression. When governments are making strong choices about what is true and not true online, there's a lot of risk there. I think there's a serious balance needed there, and I think the starting point is using this bully pulpit to really push companies to do better. That is the right starting point. Hopefully that is effective.

Ms. Sun Xueling: Yes. Thank you.

The Chair: We'll go next to our Ireland delegation and Ms. Naughton.

Ms. Hildegarde Naughton (Chair, Joint Committee on Communications, Climate Action and Environment, Houses of the Oireachtas): Thank you. Thank you all for coming before us this morning.

My first question is to Amazon. Last November, on Black Friday, I understand there were technical issues. Many of the customers' names and emails appeared on your website. Is that correct?

Mr. Mark Ryland: No, that's not correct.

Ms. Hildegarde Naughton: No? Okay. I thought there was some reporting in relation to that. Were there some technical issues last November?

Mr. Mark Ryland: It doesn't sound familiar to me at all, but I'd be happy to double-check. No, I'm not familiar with that.

Ms. Hildegarde Naughton: In relation to GDPR and data protection, from what my colleagues asked you earlier, you're saying you would be in favour of some form of GDPR being rolled out globally.

Mr. Mark Ryland: Again, we believe that the principles of consumer trust—putting customers first, giving them control over their data and getting their consent for usage of data—make sense. The specific ways in which that is done and the amount of record-keeping and the bureaucracy involved sometimes seem to outweigh the benefit to consumers, so we really think we need to work together as a community to find a right balance that's not too onerous.

For example, a large company like ours might be able to comply with a very onerous regulation that's very expensive to implement, but a small business might not. We have to find ways in which those principles can be implemented in a way that's efficient and relatively simple and straightforward.

Yes, we definitely support the principles behind GDPR. We think the actual legislation is still a bit of a work in progress, in the sense that we don't know exactly what the meaning of some of the legislation will be once it gets to the regulatory or judicial level—what exactly constitutes reasonable care, for example, on the part of a company.

Ms. Hildegarde Naughton: Okay, so are you open to that, or maybe to a different version of it across the world?

Mr. Mark Ryland: Yes.

Ms. Hildegarde Naughton: As you know, in the GDPR as it's currently working, there are those obstacles for some companies, but that has been worked through across the European Union.

Mr. Mark Ryland: Yes.

Ms. Hildegarde Naughton: I suppose you're waiting to see how that works out—

Mr. Mark Ryland: We think there will be a lot of good learnings from that experience. We can do better in the future, whether it's in Europe or in other places, but again, the principles make sense.

● (0930)

Ms. Hildegarde Naughton: Okay.

This is a question for Microsoft: Earlier this year, I understand a hacker compromised the account of a Microsoft support agent. Is that correct?

Mr. John Weigelt: That's correct. There was a disclosure of credentials.

Ms. Hildegarde Naughton: I understand at the time Microsoft was saying there was a possibility the hacker accessed and viewed the content of some Outlook users. Did that actually happen? Did they access the content of Microsoft users?

Mr. John Weigelt: Having that access from the support side gave them the possibility to be able to do so.

Ms. Hildegarde Naughton: How was it that a hacker was able to, I suppose, compromise your own security or data security features?

Mr. John Weigelt: That whole environment is an end-to-end trust-type model, so all you have to find is the weakest chain in the link. In this case, it was unfortunate that the administrative worker had a password that the hacker community was able to guess to get into that system.

Ms. Hildegarde Naughton: What have you done to ensure this doesn't happen again? It seems like kind of a basic breach of data security for your users.

Mr. John Weigelt: Absolutely. Any time there's an incident within our environment, we bring the Microsoft security response team together with our engineering teams to see how we can do better. We took a look at the environment to see what happened and to make sure we could put in place tools such as multi-factor controls, which would require two things to log in—something you know, something you have. We've been looking at things like two-person controls and tools like that, so that we can ensure we maintain our customers' trust and confidence.

Ms. Hildegarde Naughton: You're on record for having put these changes in place. Have you had a report? Did you do a report in relation to how many users' information was accessed, or the content?

Mr. John Weigelt: We'd have to come back to the committee on the report and its findings. I'm not aware of that report. I had not searched it out myself.

Ms. Hildegarde Naughton: Okay.

In relation to the measures taken following that.... Again, this is about the trust of users online and what your company has done. Would it be possible to get feedback about that?

Mr. John Weigelt: Absolutely.

Ms. Hildegarde Naughton: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): You have another minute.

Mr. James Lawless (Member, Joint Committee on Communications, Climate Action and Environment, Houses of the Oireachtas): Thank you, Chair.

To Amazon, first of all, Is Alexa listening? I guess it is. What's it doing with that information?

Mr. Mark Ryland: Alexa is listening for a keyword, the wake word, which alerts the system that you want to interact with it in some fashion. That information is not locally stored. There's nothing stored locally on the device. Once the keyword is recognized, it follows that. There's a light on the device that tells you that the device is now active, and the subsequent sound in the room is then streamed to the cloud.

The first thing the cloud does is to double-check the wake word. The software on the device often isn't sophisticated, so it occasionally makes mistakes. The cloud will then recognize that it wasn't a wake word, and then it will shut off the stream. However, if the cloud confirms that the wake word was used, that stream is then taken through a natural language processing system, which essentially produces a text output of it. From there, the systems take the next action that the user was asking for.

Mr. James Lawless: Okay.

Is that information used by Amazon for profiling and/or marketing?

Mr. Mark Ryland: That information becomes part of your account information, just as it would if you were buying books on our website. Therefore, it could influence what we present to you as other things you might be interested in.

Mr. James Lawless: Okay.

Mr. Mark Ryland: It's not passed to any third party. It's not used for advertising purposes and so forth.

Mr. James Lawless: Okay, but if you've asked about the weather in Bermuda and then you go on the Amazon website, you might be pitched a holiday book guide for Bermuda. Is that possible?

Mr. Mark Ryland: It's theoretically possible, yes. I don't know if that actual algorithm is there.

Mr. James Lawless: Is it likely?

Mr. Mark Ryland: I don't know. I'd have to get back to you on that.

Mr. James Lawless: Okay, but it is actually using the queries, which Alexa processes, to be of profit to the user. This could be used to make intelligent marketing pitches on the platform, yes?

Mr. Mark Ryland: This is because the user directly ties the device to their account and they have full visibility into the utterances. You can see a full list of what you've said and you can delete any one of those. Those will immediately get removed from the database and would not be the basis for a recommendation.

Mr. James Lawless: Do users consent to that when they sign up? Is that part of the terms and conditions?

Mr. Mark Ryland: I think it's very clear. The consent is part of the experience. To take a colloquial example, I haven't explicitly consented to my voice and video being recorded here today, but I understand from the context that it's probably happening. We believe that simple consumer experiences are best. We think our customers understand that for the service to work the way it's supposed to work, we are accumulating data about them—

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks.

Mr. Mark Ryland: —and we make it really, really easy to delete and to control that data.

● (0935)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much, although you may have a better understanding of what's going on today than most users of Alexa.

Mr. Charlie Angus: I'm sorry, Chair, but can I just make a point of order?

I want us to be really clear. When you're speaking before a committee, that's like speaking before a court. It's not about your consent to be recorded or that you think you may be recorded. This is a legal parliamentary process, so of course you're being recorded. To suggest that it's the same as Alexa selling you a thing in Barbados is ridiculous, and it undermines our Parliament.

I would just remind the witnesses that we are here to document for the international legislative community, and this will be on an official record.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks, Charlie.

We'll go to David for five minutes.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): Thank you. I'll start with Microsoft.

The Microsoft ecosystem is quite large, as you know. You have the majority of the world's desktops, with Office 365, LinkedIn, Bing, Skype, MSN, Live.com, Hotmail and so on. You obviously have the ability to collect a tremendous amount of data on a tremendous number of people. Can you assure me that there's no data about individuals interchanged between any of the different platforms?

Mr. John Weigelt: Do you mean data between, let's say, an Xbox user and your Office 365 type of user? Is that the type of question?

Mr. David de Burgh Graham: Yes, or LinkedIn and Bing. We heard quite a bit in the first couple of days of this committee about the creation of avatars of users of different companies. Does Microsoft create an avatar of their users? Does it create an impression of who is using their services?

Mr. John Weigelt: What we see is that if you have a common Microsoft account, that allows you to maintain and manage your data across those properties. The Bing product team would not necessarily go directly from the Xbox team and back and forth for the data that's required. You are in control of your data that's in the centre.

Mr. David de Burgh Graham: My question was whether there is an interchange of the data between the services. You have your common log-in, but once you've gone past the log-in, you can go to different databases. Do the databases interact?

Mr. John Weigelt: Again, across all the different platforms, I would have to look at each individual scenario that's done there to say largely that there's no data exchange across....

Mr. David de Burgh Graham: Okay.

You recently bought GitHub, an open-source company, which I thought was pretty interesting. Why?

Mr. John Weigelt: We recognize that the open-source community is a very vibrant community with a great development model. That open dialogue, that open discussion, has gone beyond simply the software conversation to broader projects. We saw that as an opportunity for us to help engage with that community.

In the past, you've seen that there was almost this animosity between ourselves and the open-source community. We've really embraced the concept of open source and concepts of open data to be able to help bring better innovation to the marketplace.

Mr. David de Burgh Graham: I come from the open-source community, so I can relate to that comment.

I'd like to speak to Mozilla for a second.

You talked about enhanced tracking protections. Would you describe tracking and anti-tracking as an arms race?

Mr. Alan Davidson: Unfortunately, yes. I think we are very clear-eyed about the fact that we will build this set of tracking protections. We think they provide real value. I'll give a shout-out to our friends at Apple. They're doing something similar with Safari that's really good.

The trackers will find other ways to get around this, and we'll have to build new tools. I think this is going to be an ongoing thing for some time, which is unfortunate for users, but it is an example of how we can do things to protect users.

Mr. David de Burgh Graham: Understood.

To go to Apple for a second, there was recently the sensor ID hack that was patched in 12.2 of iOS—I'm not familiar with it—that permitted any website anywhere in the world to track any iPhone and most Android devices based on sensory calibration data. You're probably familiar with this.

Mr. Erik Neuenschwander: Yes, it's the fingerprinting issue.

Mr. David de Burgh Graham: Yes, the fingerprinting issue. Can you tell us more about this, how it was used and if it is truly prevented now in iOS 12.2?

Mr. Erik Neuenschwander: First, I'll step back, I think, to explain a bit of the context. When we're talking about, say, tracking, there can be some technologies that are explicitly for tracking, such as cookies. One of the evolutions we've seen is the development of what we call a synthetic fingerprint. It's just a unique digital number that is synthesized by a third party, probably to attempt to track. It can also be used for anti-fraud and some other reasons, but certainly it is fit for the purposes of tracking.

You're right. Some researchers, by looking at variations in sensor manufacture, identified that there was the ability to try to synthesize one of these unique identifiers. Fingerprinting, much like anti-tracking, is going to be something that will continually evolve and that we're committed to staying in front of. When you ask how it was used, I don't have any data that it was used at all, but I also can't assure you that it was not.

We introduced a number of mitigations in our most recent update, which the researchers have confirmed have blocked their version of the attack, but again, I'd put this in the context of fingerprinting being an evolving area, so I choose my word “mitigations” also carefully. Without actually removing sensors out of the device, there will continue to be a risk there. We're also going to continue to work to mitigate that risk and stay on top of it.

● (0940)

Mr. David de Burgh Graham: I have only about 20 seconds left. I have one more question for Apple.

On iOS, when you switch between applications, one application suspends and the next one opens. When you come back to the original application, if it's been more than a few seconds, it will reload the data. Is that not providing ample tracking opportunity to any website you're on, by saying that this is the usage of the device? I find it strange to have to do that, instead of storing the content that you're actually using.

Mr. Erik Neuenschwander: I'll split that into two parts, I guess.

One, when the application gains the foreground and is able to execute, they can reload the content, if they see fit to reload the content. At that point, you've transferred control to that application, and it will be able to execute and reload, if you'd like.

It's our goal, actually, to minimize those reloads as part of the user experience. It's also our goal that the application currently in the foreground should get, within a sandbox, within a set of limitations we have, the maximum execution and other resources of the device. This can mean that the operating system will remove some of the resources of background applications.

In terms of the reloading that you're seeing, iOS, our operating system, could contribute to that, but fundamentally, regardless of what resources are preserved for that background application, when you transition back to an app, it has execution control and it can reload if it sees fit.

Mr. David de Burgh Graham: Thank you.

The Chair: Thank you, Mr. Graham.

We'll go to my co-chair, Mr. Collins.

Go ahead with your opening comments. It's good to have you back.

Mr. Damian Collins (Chair, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): Thank you.

My apologies, since the other U.K. representatives and I were not here for the start of the session, but we're delighted to see all of the witnesses here on the panel.

We had focused yesterday on some of the social media platforms, but I think our interests are much broader, looking at a range of technology companies.

I wonder if I could start with a couple of questions first for Apple.

As I came in, there was a discussion about data collected about voice. Could you tell me a little bit about the sort of data Apple collects in terms of sound captured by its devices? With smart devices, are the devices capturing ambient background sound to gain an understanding of the users—maybe the environment they're in or what they're doing when they're using the device?

Mr. Erik Neuenschwander: In terms of the information on our devices that support Siri, there is a part of the device that is constantly listening. On some of our devices we've isolated it beyond even iOS, beyond our operating system, into a dedicated coprocessor, basically a specialized piece of hardware, which is not recording or storing that information but is listening only for the wake-up word to trigger our personal assistant, so that information isn't retained on the device.

Further to the point of your question, it isn't being collected into any sort of derived profile to identify something about the users' behaviour or interests. No.

Mr. Damian Collins: Is it collecting information about the environment they're in at the moment? Let's say, for example, I was commuting to work and I was on the bus. Would it pick up that sort of ambient sound?

Mr. Erik Neuenschwander: It's not collecting it all. There's what we call a "ring buffer". There's basically a short period that is transiently recorded to analyze for that wake-up word, and then it's continually overwritten as time progresses. There isn't any collection for more than just the ephemeral milliseconds of being able to listen for that wake-up word.

Mr. Damian Collins: The only purpose of the listening is for a command to Siri.

Mr. Erik Neuenschwander: That's correct. Yes.

Mr. Damian Collins: For product development or training purposes, is any of that information retained by the company?

Mr. Erik Neuenschwander: Again, it's not even retained by the device. As it's transiently listening, it's being continually overwritten. When the user uses a wake-up word, there is some machine learning that happens on the device as it adapts the audio model to the speaker to reduce the number of false positives or false negatives for that wake-up word. Then if the user is using Siri, at the point Siri is woken up and being communicated with, that is the initiation of transmission of data to Apple.

Mr. Damian Collins: What would the scope of that data be?

Mr. Erik Neuenschwander: The scope of the data is the utterance until it reaches a termination point and Siri thinks the user has stopped talking, along with information like the device model to tailor the response back to the device and a random device-generated identifier, which is the key to the data that is held by Siri for purposes of your interactions with Siri. This is an identifier that is separate from your Apple ID and not associated with any other account or services at Apple.

Mr. Damian Collins: Would Apple keep a record of the sort of things I've asked Siri about, the commands I've given?

Mr. Erik Neuenschwander: Yes.

● (0945)

Mr. Damian Collins: Is that used by the company, or is that just used to inform the response to my device?

Mr. Erik Neuenschwander: I guess the second part is a form of use by the company. Yes, we use it for Siri, and for Siri purposes alone.

Mr. Damian Collins: To get at what the Siri purposes are, are the Siri purposes just actually making Siri more responsive to my voice —

Mr. Erik Neuenschwander: Yes.

Mr. Damian Collins: —or is the data kept by the company to understand what sorts of things people ask? Do you have metadata profiles of people based on how they use Siri?

Mr. Erik Neuenschwander: The only metadata profile that we have is one that is used to tailor your actual interactions with Siri. For example, we are training our voice models to do natural language recognition on the sound profile. This is really just within the Siri business or the Siri experience. If your question is whether it informs some broader profile used by the company to market products and services, the answer is no.

Mr. Damian Collins: Mark Ryland, does Amazon do that?

I'd be interested to know the difference between how Amazon uses data gathered from voice compared to how Apple does. There was a recent case of a user who actually put in a request for data that Amazon held. That included a series of voice recordings from their home that the company was apparently using for training purposes. I'm interested in how Amazon gathers data from voice and how it uses it.

Mr. Mark Ryland: Similarly, the device listens for a wake-up word. It doesn't store any of that ambient data. Once it's awakened, it will begin to stream data to the cloud to do analysis of what the user is actually requesting. That data is stored; it's explicit in the user's profile, and they can see all the utterances. They can see what Alexa thought they said; they can actually see the text that it was translated into. It also gives them some understanding of where there may be some communication issues, and so forth.

They have the ability to delete that data, either individually or collectively. We use the data just as we would use data with other interactions with that person's account. It's part of their Amazon account. It's part of how they interact with our overall platform.

Mr. Damian Collins: The representative from Apple has said that the device is constantly listening, but only for the Siri command. It would appear that if you have an Alexa device in your home, that is different. The device is always listening and it is actually retaining in the cloud the things it has heard.

Mr. Mark Ryland: No. It's very similar. We're retaining the utterances after the wake word. It is just like Siri in that regard.

Mr. Damian Collins: I know from my own personal experience that Alexa responds to commands other than the wake word. It might be triggered by something it has heard in the room that's not necessarily the wake command.

Mr. Mark Ryland: That sounds like a malfunction to me. It's not supposed to respond randomly to ambient sounds.

Mr. Damian Collins: Roger McNamee, who gave evidence to us yesterday, discussed how he put his Alexa in a box after the first day he got it because Alexa starting interacting with an Amazon TV commercial. I think most people who have these devices know that all sorts of things can set them off. It's not just the Alexa command or the wake word.

Mr. Mark Ryland: Well, we're certainly constantly working to refine the technology and make sure the wake word is the way by which people interact with the device.

Mr. Damian Collins: If you were retaining data from the device that is based on things that it's heard and is then retained in the cloud—which seems to be different from what Apple does—are you saying that it's only sound data that is based on commands that Alexa has been given?

Mr. Mark Ryland: Yes. It's only the data that is in response to the user's attempt to interact with Alexa, which is based on the wake word.

Mr. Damian Collins: Would Amazon be in a position to respond to a police request for data or information about a crime that may have been committed in a domestic setting based on sound picked up from Alexa?

Mr. Mark Ryland: We happily obey the laws of all the countries in which we operate. If there is a binding legal order that's reasonable in scope and so forth, then we will respond to that appropriately.

Mr. Damian Collins: That would suggest you're retaining more data than just simply commands to Alexa.

Mr. Mark Ryland: No, the only thing we could respond with is the information that I just described, which are the responses that come from the user once they've awakened the device. There's no storage of ambient sound in the environment.

Mr. Damian Collins: You're saying that when someone gives the wake word to the device, then the command they've given—their dialogue with Alexa, if you like—is retained?

Mr. Mark Ryland: That is correct.

Mr. Damian Collins: You're saying that unless the wake word is given, the device isn't triggered and it doesn't collect ambient data.

Mr. Mark Ryland: That is correct.

Mr. Damian Collins: Okay.

I'm interested in the data case I referenced earlier. The concern there seemed to be that ambient sound was being kept and recorded and the company was using it for training purposes.

Mr. Mark Ryland: No. The reference to training is simply that we improve our natural language processing models using the data that the customers give to us through their interaction with the device. It's not at all based on ambient sound.

● (0950)

Mr. Damian Collins: It would seem that all of their commands to Alexa that are triggered by the wake word are being retained by the company in the cloud. Do you think your users are aware of that?

Mr. Mark Ryland: I think so. In my experience with using a mobile device to set up the device at home, I immediately noticed that there is a history icon, essentially, where I can go and see all my interaction with the system.

Mr. Damian Collins: I don't remember reading that anywhere. Maybe it's in the huge sort of *War and Peace*-like terms and conditions that are attached to the device.

I think that although it may be the same as using any other kind of search function, the fact is that he was talking to a computer, and I'm not sure users are aware that this information is stored indefinitely. I did not know that was being done. I had no idea how you'd go about identifying that. I'm slightly intrigued as well that you can, in fact, see a transcript of what you've asked Alexa.

Mr. Mark Ryland: Yes, absolutely. It's in the mobile app, on the website and on the Alexa privacy page that you can see all of your interactions. You can see what the transcription system believed you said, and so forth.

Mr. Damian Collins: Presumably all of that is merged into a bucket of data that Amazon holds about me in terms of my purchasing habits and other things as well.

Mr. Mark Ryland: It's part of your account data.

Mr. Damian Collins: It's a lot of data.

The Chair: Mr. Davidson wants to respond.

Mr. Alan Davidson: I wanted to jump in to just say that I think this also highlights the problem we've been talking about with consent.

I'm a loyal Amazon Echo user. They've done a wonderful thing by putting this up. A couple of weeks ago, I went with my family, and we saw the data that was stored, but I have to say it is....

I'm a total privacy nut. I read all this stuff that you get, and I was shocked, honestly, and my family was shocked to see these recordings about us and our young children from years ago that are stored in the cloud. It's not to say that something was done wrongly or unlawfully. I think it's wonderful to see this kind of level of transparency, but users have no idea it's there. I think that many users have just no idea that this data is out there, and they don't know how it's going to be used in the future either.

I think that as an industry, we need to do a much better job of giving people better granular consent about this, or better information about it.

The Chair: Yes.

Mr. Alan Davidson: I don't mean to pick on Amazon; it's a wonderful product.

The Chair: We'll move on next to Mr. Gourde.

I see a lot of hands going up. There's going to be lots of time for everybody today.

Go ahead, Mr. Gourde, for five minutes.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): Thank you, Mr. Chair.

My question will focus on a more technical subject.

You, and especially Amazon and other similar organizations, have a lot of information and personal data on your clients.

I'm sure that you're taking every possible measure to secure all the data. However, given the emergence of artificial intelligence, you may have received services to help you predict the market in the future.

It could be useful—especially for Amazon—to be able to predict, let's say for next summer, which item on order could qualify for a discount and be put on sale.

Perhaps some subcontractors or individuals have provided services related to the new algorithm systems. Basically, they sold these services to help you.

Can these subcontractors, if you use them—of course, you don't need to tell us—guarantee that, when they use your company's data to provide this type of service, they won't sell personal information to other people or to larger organizations? These organizations would be very happy to obtain the information, whether they use it to sell advertising or for other purposes.

Do any organizations provide this type of service?

[*English*]

Mr. Mark Ryland: We do contract with third parties for certain delivery of some services and, under very carefully controlled conditions, we share personal data.

For example, if we're contracting with a delivery service, we share the name and address of the customer where the package has to be delivered, but I think, for all of these core machine-learning cases of the kind you're talking about, that is all internal to our company. We do not contract out access to the core business data that we use for, essentially, running our business. It's only going to be around the peripheral use cases, and in cases where we do share data, we have audit rights and we carefully control, through contract and audit, the usage that our contractors make of any data of our customers that we do share with them for these very limited purposes.

● (0955)

[*Translation*]

Mr. Jacques Gourde: Do any other organizations use algorithm strategies to promote your products?

[*English*]

Mr. John Weigelt: We have a very robust data governance model at Microsoft whereby we recognize and are able to attribute and mark data and appropriately protect it. In areas where we need subcontractors, we use a very limited set.

A lot of adjudication occurs before we select our subcontractors, and they must enter into agreements with us to maintain the privacy of the data they are safeguarding. We have strict rules around the use of that data and the return of that data to us. We have a very robust program of policies, procedures and technical safeguards around subcontractor use to ensure that data isn't misused.

Artificial intelligence is an area of key interest to us, and certainly Satya Nadella, in his book *Hit Refresh*, has put together principles around the responsible use of AI to empower people. It's really the first principle. We've embraced them within our organization, ensuring that we have a robust governance structure around AI. We have a committee that looks at application of AI both inside and outside the organization to make sure we use it responsibly.

Putting these pieces in place internally helps us better manage and understand how those tools are being used and put them in place in an ethical framework. We're quite pleased that we're working with governments around the world, be they the EU with their AI ethics work or the recent OECD guidelines, or even here in Canada with the CIO Strategy Council's work on an AI ethics framework, so that we can help people and other organizations get a better sense of some of those responsible techniques, processes and governance models that need to be put in place.

Mr. Erik Neuenschwander: I'm not aware of Apple doing the kind of modelling you're talking about. Instead, our machine learning tends to be on device intelligence.

For instance, as the keyboard learns about the user, the device itself collects and uses this information to train itself for that user without the information leaving the device. Where we are collecting data to help inform community models, we're using things like local differential privacy, which applies randomization to the data before it leaves the user's device, so we're not able to go back and tie the individual user inputs and their content to a user. It's very much a device focus for us.

[*Translation*]

Mr. Jacques Gourde: Mr. Davidson, do you want to add anything?

[*English*]

Mr. Alan Davidson: We don't deploy any of those kinds of systems. In some of our research we have been looking at experimenting on devices also. I think that's a very solid approach to trying to protect people's privacy.

The Chair: Thank you, Mr. Gourde.

Next up, from the U.K., we have Mr. Ian Lucas.

Mr. Ian Lucas (Member, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): If I can pick up on what Mr. Collins was asking, I was intrigued about both the phone for Apple and the Alexa device. Have there been any attempts to hack into the systems you have and access the information you retain?

Mr. Erik Neuenschwander: Apple's systems are under constant attack. I don't know precisely if Siri itself has been a subject of attack or not, but I think a good default position would be to assume it has. However, because the Siri data is not associated with the overall Apple account, while we consider it very sensitive and will strive to protect it, it would also be challenging to gather an individual user's data out of the Siri system, even if it were breached.

Mr. Ian Lucas: Has there ever been a successful hack into the system with respect to a particular individual?

Mr. Erik Neuenschwander: I'm not aware of any, no.

Mr. Mark Ryland: Similarly, we've been protecting customer data very successfully for 20-plus years. This is a new kind of data, obviously a very sensitive kind, but we continue to have a very successful record there, and there's no indication of any kind of compromise of Alexa-related data.

The Chair: We'll move next to Mr Lawless for five minutes.

Mr. James Lawless: Thank you.

Going back to security and data privacy and encryption, I think Apple talked about the Key Store on the iPhone and iPad, and Mozilla, I think, also has a Key Store-type feature in the browser.

One of the challenges of security is that our passwords, I think, have become so secure that nobody knows what they are anymore, except for the devices themselves. On the Apple Key Store—I think it's called the Key Store application—you can ask it to generate a password for you, and then you can ask it to remember it for you. You don't know what it is, but the app and the device know what it is, and I guess that's stored in the cloud somewhere. I know you gave an overview at the start.

I suppose Mozilla has a similar feature that allows you to ask the platform to remember the password for you, so you have multiple passwords, and I think probably Microsoft does as well in its browsers. Again, if you log in to Mozilla or Edge or any browser, you find you can autopopulate all your password keys. We end up with this situation like Lord of the Rings, in a “one ring to rule them all” scenario. In our attempts to complicate and derive better security, we've ended up with one link in the chain, and that link is pretty vulnerable.

Maybe I could get some comments on that particular conundrum from all the platforms.

● (1000)

Mr. Erik Neuenschwander: I think the application you're referring to is the Keychain Access application on the Mac and on iOS devices. Within “settings”, “passwords” and “accounts”, you can view the passwords. They are, as you say, auto-generated by the platform. Most users experience that through our Safari web browser, which offers a feature to link into the keychain. It is, as you say, stored in the cloud.

It is stored in the cloud end-to-end encrypted—I want to make that clear—so it's actually encrypted with a key that Apple never possesses. While we put that in the cloud, both to allow you to recover the passwords and to synchronize them among all devices that you've signed in to iCloud, we do that in a way that does not expose the passwords to Apple.

I think that you're right that passwords continue to be an area of challenge in terms of protecting user accounts. You see many companies, certainly Apple among them, moving to what's called two-factor authentication, in which merely the password is not sufficient to gain access to the account. We're very supportive of that. We've taken a number of steps over the years to move our iCloud accounts to that level of security, and we think that it's good industry progress.

The last thing I would say is that absolutely, the password data is extremely sensitive and deserves our highest level of protection. That's why, separate from the Keychain Access application you're talking about on the Mac, on our iOS devices and now on our T2—that's the name of the security chip in some of our latest Macs—we're using the secure enclave hardware technology to protect those passwords and separate them from the actual operating system. We have a smaller attack surface for that, so while it's absolutely a risk that we're highly attentive to, we've taken steps, down in our hardware design, to protect the data around users' passwords.

Mr. Alan Davidson: It's a great question. I would just add that it seems counterintuitive, right? I think that 10 years ago we would have said, “This is crazy. You're going to put all your passwords in one place?” We offer a similar product—Lockwise—on our browser to help people.

I think that today the security experts will tell you this is a far better solution for most people because the biggest problem that we all have is that we can't remember our passwords, so we end up using the same password everywhere, or we end up using dumb passwords everywhere, and then that's where we get into trouble.

Our own polls of security experts and our own internal experts have said that it is actually far smarter to use a password manager, to use one of these systems. For most of us, the threat of that central vulnerability is actually a lot lower than the threat otherwise. I'd encourage you all to use password managers and think about that.

I've just sent out a note to all of our employees saying that they should do it. We all take that incredibly seriously. Two-factor authentification is an important part of this, and it's an important part of how those managers work. We take the responsibility to guard those things very seriously, but it is actually, as it turns out, a better solution for most consumers today.

Mr. John Weigelt: Just to chime in, we see that local hardware-based protections based on encryption are important to help support that password protection. Work that together with multifactor authentication, perhaps using something you have, something you own.

I think an interesting counterpoint to this and an interesting add-on is the ability to make very robust decisions about individuals, about their use of a particular system. We use anonymized, pseudonymized data to help organizations recognize that “Hey, John's logging in from here in Ottawa, and there seems to be a log-in coming from Vancouver. He can't travel that fast.” Let's alert somebody to do that on an organizational perspective to intervene and say, “Look, we should perhaps ask John to refresh his password.”

There's another thing that we're able to do, based upon the global scope of our view into the cyber-threat environment. Often malicious users share dictionaries of user names and passwords. We come across those dictionaries, and we are able to inform our toolsets so that if organizations—say, food.com—find out that one of their names is on there, they are able to go back there as well.

For data associated with the use of a particular toolset, anonymization and pseudonymization help to provide greater assurance for privacy and security as well. Let's make sure we recognize that there's a balance we can strike to make sure that we maintain privacy while at the same time helping safeguard those users.

● (1005)

Mr. James Lawless: It's a very interesting area, and it continues to be challenging. There's a usability trade-off versus security.

I remember an IT security manager in a large corporation telling me about a policy he implemented before there were password managers, going back maybe a decade. He implemented a policy of robust passwords so that everybody couldn't use their household pet or their birthplace and so on. Then he found that despite having this enforced policy, everybody was writing their passwords down because there was no way they could otherwise remember them, so it was kind of counterproductive.

I have one final question, and then I'm going to share time with my colleague. I think there's a website called haveyoubeenhacked.com or haveibeenhacked—something like that—which basically records known breaches. If your data and any of your platforms or other third party apps or sites are in the cloud and are compromised, you can do a search for yourself or for your details and pull it back.

Is there any way to remedy that? I ran it recently, and I think there were four different sites that had been compromised that my details were on. If that happens on your platforms, how do you do that? How do you mitigate that? Do you just inform the users? Do you reach out, or do you try to wipe that data set and start again? What happens there?

Mr. John Weigelt: We have breach notification requirements, obligations, and we notify our users if there's a suspected breach of their environment and recommend that they change their passwords.

For the enterprise set, like that toolset that I mentioned—"Have I been pwned?", I think it's called—

Mr. James Lawless: That's the one, yes.

Mr. John Weigelt: —that site has readily available dictionaries, so we feed those back to enterprise users as well. There's the notification of the individual users, and the we also help enterprises understand what's happening.

Mr. Alan Davidson: We do the same thing in the sense that we all have data breach obligations and would do those things in such a situation. We've also put together our own version of that "have I been hacked" Firefox monitor. For Firefox account holders who opt into it, we'll actually notify them affirmatively of other attacks that we're notified about, not just any breach on our system but on others as well. I think that's going to be a service that people find valuable.

Mr. James Lawless: That's good.

Mr. Erik Neuenschwander: If Apple security teams, in addition to the steps that have been discussed here, become aware that an account has likely been breached, then we can take steps through what's called "automated reset" on the account. We will actually force a password reset and do additional challenges to the user if they have two-factor authentication using their existing trusted devices to re-establish access to that account.

Mr. James Lawless: Yes, it's very hard to get back in when you're out, because I've had that experience.

Voices: Oh, oh!

Mr. Erik Neuenschwander: You mentioned balancing usability and security.

Mr. James Lawless: Yes.

Mr. Erik Neuenschwander: We try to strike a balance there between whether you are the good guy trying to get back in, so let's not make it hard for you, or let's definitely keep that bad guy out. That's an evolving space.

Ms. Hildegarde Naughton: Can I just come into that, please?

The Chair: We're actually way over time. The chair is taking the second round, and I already have you as number one on our second round, Hildegarde. Once we get through everybody, we'll start through that next round. It shouldn't be very long.

We'll go to Ms. Vandenbeld now for five minutes.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you very much.

I'd like to begin with the lack of utility of the idea of consent anymore. When you want to use a certain app or you want to use something, there are good purposes and bad purposes. Let's say that, for instance, I'm on my iPhone and I'm leaving Parliament and it's 9 p.m. My iPhone tells me exactly which route to take to get to my home. It knows where I live because it has seen that I take that route every day, and if I suddenly start taking a different route to a different place, it will know that as well.

Well, that's great when I want to know whether or not I should take the 417, but for my phone to know exactly where I'm sleeping every night is also something that could be very disturbing for a lot of people.

We don't really have a choice. If we want to use certain services, if we want to be able to access Google Maps or anything like that, we have to say yes, but then there's that alternate use of that data.

By the way, on the comment about this being a public hearing, we have a tickertape right on the side of the wall there that says this is in public. I wish there were a tickertape like that when you're searching on the Internet so that you know whether what you're doing is going to be recorded or made public.

My question, particularly to Apple, is on your collection of data about where I've been. It's not just a matter of where I'm going that day. It's not that I want to get from A to B and I want to know what bus route I should take; it's that it knows exactly the patterns of where I am travelling in terms of location.

How much of that is being stored, and what are the other purposes that this could be used for?

● (1010)

Mr. Erik Neuenschwander: I'd like to be really precise, madam, about the “you” and the “it” in your sentences because I think you used them correctly, but there is a subtle distinction there. “It”—your phone—does know that. Your phone is collecting based on sensor data and behavioural patterns and tries to infer where your home is—and that is your iPhone. “You”, being Apple, does not know this information, or at least not via that process. If you leave a billing address with us for purchases or something, that's different, but the information that your iPhone is becoming intelligent about remains on your phone and is not known by Apple.

When you ask about how much of it is collected, well, it's collected by the phone. It's collected under our “frequent locations” feature. Users can go and browse and remove those inside the device, but the collection is just for the device. It's not actually collected by Apple.

As for the purposes to which it can be put, over our versions of the operating system we try to use that information to provide good local experiences on the device, such as the time-to-leave notifications or notifications of traffic incidents on your route home; but that isn't going to extend to purposes to which Apple, the corporate entity, could put that data, because that data is never in our possession.

Ms. Anita Vandenbeld: I think that goes to what Microsoft started talking about in their opening statement, which is the ability of hackers to access the data. Apple's not using this data, but is it possible, through cyber-threats, that other bad actors might be able to get in and access this data?

I'm actually going to ask Microsoft.

You talked about doing $1 billion a year in security research and development, and there's a term that you threw out, “co-operative botnet takedowns”. I'd like you to explain that a bit, as well as the work that you're doing on cybercrimes.

We know that once the data is out there, it's impossible to put back, and a lot of these Cambridge Analyticas and other data aggregators are using it, so what are you doing to make sure that this data doesn't get out there in the first place?

Mr. John Weigelt: When we look at the marketplace, we see it's continuously moving, right? What was put in place for security controls 10 years ago is different today, and that's part of the efforts of the community that's out there securing the IT environment.

From our case, we analyze those common techniques. We then try to make sure that those techniques go away. We're not just trying to keep up; we're trying to jump ahead of the malicious user community so that they can't repeat their previous exploits and they will have to figure out new ways to do that.

We look at tools like encryption, tools like hardening up how the operating system works, so that things don't go in the same place every time. Think of it as if you change your route when you go home from Parliament at night, so that if they are waiting for you at the corner of Sparks, then they won't get you because you have changed your route. We do the same thing within the internal system, and it breaks a whole bunch of things that the traditional hacker community does. We also include privacy within that, and accessibility, so our whole work is around trust, security, privacy and accessibility.

At the same time, there is a broader Internet community at large, so it's nothing we can do alone. There are Internet service providers, websites, and even home computers that get taken over by these zombie networks. Hackers have started to create networks of computers that they co-opt to do their bidding. They may have up to a million zombie computers attacking different communities. It really takes the Internet down and bogs it down with traffic and whatnot.

In order to take that down, you need technical sophistication to be able to take it over, but you also need the support of legal entities within regions. One of the things that's unique for us is that our cybercrime centre has worked with government authorities in finding novel legal precedents that allow these networks to be taken down, so in addition to the technology side, we make sure we're on side from the legal side to conduct our operations.

Lastly, what we did for the Zeus and Citadel botnets, which were large zombie networks that had placed themselves into corporate Canada, was work with the Canadian Cyber Incident Response Centre as well as the corporation to clean up those infections from those machines so they would go quietly, and they could start up again.

Ms. Anita Vandenbeld: Mr. Davidson, would you comment?

Mr. Alan Davidson: I have two quick points.

First, we work on something that we call “lean data practices”. It's the idea that we should not keep data if we don't need it. The best way to secure data is not to retain it. Sometimes it's needed, but sometimes it's not. The industry could do a better job and consumers could learn more about insisting that data not be kept if it's not needed.

Second, location is a particularly sensitive area. It's probably an area that is ultimately going to need more government attention. Many users probably would feel really comfortable with an Apple or a Microsoft holding this data, because they have great security experts and stuff like that. We worry a lot about some of the smaller companies and third parties that are holding some of this data and maybe not doing it as securely.

● (1015)

The Chair: We will go to Ms. Jo Stevens from the U.K.

Ms. Jo Stevens (Member, Digital, Culture, Media and Sport Committee, United Kingdom House of Commons): Thank you, Chair.

I would like to turn to a different subject altogether, competitions and markets. I would like to ask Mark and Erik if they think different competition and antitrust rules should apply to tech giants, considering their unprecedented influence and market power.

Mr. Erik Neuenschwander: When it comes to antitrust regulations, I'm working with an engineering organization, so I can't say I've given a lot of thought to the regulation side. I would be happy to take any questions and refer them back to our legal or government affairs teams.

Ms. Jo Stevens: As a consumer, do you think that large global tech giants have too much market influence and power?

Mr. Erik Neuenschwander: My focus, in terms of our platforms, is to put the user in control of data and to leave as much control as possible in the hands of users.

Mr. Mark Ryland: We're a relatively large company, but of course, that is largely the result of the fact that we operate globally. We operate in a lot of different markets. In any given market segment, we typically can be often a very small or middle-size player.

Again, I'm not going to opine in any depth about competition laws. It's not my area of expertise, but we feel the existing competition law as it exists today is adequate to deal with technology companies.

Ms. Jo Stevens: How about you, John?

Mr. John Weigelt: We've been around for quite some time, since the 1970s, so we've had some focus on the organization and the way we do our business. I think we've made appropriate adjustments, which we made based on the input and the perspective of governments around the world.

One thing that is important to me as a Canadian working for Microsoft here in Canada is the partner ecosystem and the enabling of Canadian innovation and Canadian business. Over 12,000 partners who make a living off of the toolset have the reach from a consistent platform to be able to sell innovation around the world based upon these toolsets and have a multiplying factor for the revenue that they generate here in the nation.

Sometimes with packaged software it's an eight-to-one multiplier. For cloud computing, it's estimated to be as high as a 20-to-one multiplier for the use of these toolsets, so we see that as a great economic enabler. Having that global reach is an important factor for the partners we work with.

Ms. Jo Stevens: That quite neatly leads me on to my next question. I think there is quite a strong argument that global tech giants are a bit like a public utility and should be treated as such because of the power you wield.

Bearing in mind what you said just now about innovation, do you think that if that was the case and there was a bigger antitrust emphasis, it would negatively impact innovation? Is that your main reason?

Mr. John Weigelt: I was making a linkage between those themes. My sense was that, look, we democratize technology. We make it silly simple for emerging nations and emerging companies with great ideas to leverage very advanced technology. When you think about artificial intelligence and the work that's happening in Montreal, Toronto, and even globally, the ability to make use of these tools to provide a new market is critically important.

I see this as a catalyst for the innovation community. We're working across the five Canadian superclusters, which is Canada's innovation engine around agriculture, oceans and advanced manufacturing, to build out new toolsets. Our ability to look across those communities and do cross-platform types of approaches and leverage our experience on a platform provides for activities in the community's best interest.

For example, in the ocean supercluster, working with data and having data about our oceans and having that sharing of a common commodity across the community is something we advocate to help that community grow . Having that platform and easy access to it provides that innovation.

● (1020)

Ms. Jo Stevens: Would either of you like to comment on the innovation point from your company's perspective?

Mr. Mark Ryland: Yes, I would be happy to.

We face robust competition in all the markets we operate in. Cloud computing is a great example. There are not a large number of players in the cloud market, but competition is very strong, prices are dropping, and it enables, as my colleague was saying, new kinds of business models that were really previously impossible.

I worked for some years in our public sector business at Amazon Web Services. What I saw there was that we had very small companies, 10-, 20- or 30-person companies, competing for large government contracts that would have been impossible for them to compete for prior to the existence of cloud computing. It would have required a very large, dedicated government contractor to compete for these large contracts because they required so much infrastructure and so much capital investment in order to go after a large contract.

With the ability to get onto many IT services from cloud, you now have this great democratization, to reuse that word, of international market access, of mom-and-pop shops with international market access, whether through Amazon sellers on our retail site or through using our cloud platform. I think competition is really strengthened because some of these large-scale players enable people to access a broader set of markets.

Ms. Jo Stevens: But they have to do it through you, don't they? Where else would they go?

Mr. Mark Ryland: No, you can do it through us or our competitors.

Ms. Jo Stevens: But there aren't that many competitors, are there?

Mr. Mark Ryland: There are not a huge number of competitors, but the competition is fierce.

Ms. Jo Stevens: It sounds a bit odd to me that you have very few competitors, yet it's fierce. That's not what I'd normally assume to be the case.

How about you, Erik?

Mr. Erik Neuenschwander: From what little I know about legislation, it appears to be very challenging to write. I would presume that a goal of any legislation would be not to limit innovation, not to put a ceiling on what companies can do, but instead to try to put a floor for good behaviours.

Ms. Jo Stevens: Okay, thank you.

The Chair: Thank you, Jo.

We'll go next to Raj Saini for five minutes.

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning, everybody.

I'm sure you're all aware of the term “data-opoly”. Right now, in front of us, we have Apple, which controls a popular mobile operating software system. We have Amazon, which controls the largest online merchant platform software. We also have Microsoft, which has the ability to acquire a lot of data and use it to gain market advantage.

In talking about competition, I want to go beyond what Ms. Stevens said. When we look at the European Union right now, we see that Apple violated European state aid rules when Ireland granted undue tax benefits of 13 billion euros. In some cases, you paid substantially less tax, which was an advantage.

In the case of Amazon, the European Commission targeted Amazon's anti-competitive most favoured nation clause, and Luxembourg gave Amazon illegal tax benefits worth some 250 million euros.

My point is not in any way to embarrass you, but obviously there is a problem with competition. The problem stems from the fact that there are different competitive regimes or competition laws, whether it be in Europe, whether it be the FTC, or whether it be Canada. In European competition law, a special duty is imposed on dominant market players. That is not the same as the United States, because the same infractions were not charged in the United States. Do you think it's something that should be considered because of your dominant market status?

Mr. Mark Ryland: As I said, I'm not an expert on competition law. We certainly obey the laws of the countries and regions in which we operate, and we will continue to do so.

Mr. Raj Saini: Well, the European Commission fined Amazon, so you didn't really follow the law.

My question is about the special duty imposed in European competition law on dominant market players. Do you think that should come to the United States and Canada also?

Mr. Mark Ryland: I really should get back to you on that. I'm not an expert in that area. I'd be happy to follow up with our experts in that area.

Mr. Raj Saini: Sure.

Apple, would you comment?

Mr. Erik Neuenschwander: I am aware that the state aid story made a great deal of press, I think, but I'm really aware of it as a consumer of the news. I haven't done a lot of reading on European competition law. Similarly, as I'm focused on privacy by design from the engineering side, for questions on that I'll have to get the company to get back to you.

Mr. Raj Saini: Okay.

Amazon is probably the most dominant bookseller in the market. Do you agree with that?

Mr. Mark Ryland: No, I don't agree with it.

Mr. Raj Saini: You don't? Who's bigger than you?

Mr. Mark Ryland: There's a huge market in book sales from all kinds of retailers, from Walmart to—

● (1025)

Mr. Raj Saini: Who sells more books than you?

Mr. Mark Ryland: I don't know the answer to that, but I'd be happy to look it up for you.

Mr. Raj Saini: Okay.

One of the approaches you use when you allow books to be sold —I read this somewhere, so correct me if I'm wrong—is that you approach small booksellers and you exact a sizable fee from them to list their books. You don't pay authors per copy when they download the book, but you pay per page. If they don't finish the book, then you pocket the difference. You track online what people read. If people are reading popular authors, you don't provide a discount to them, because you know they will buy the book anyway.

Do you think this is fair, or is what I'm saying wrong?

Mr. Mark Ryland: I don't know the facts surrounding the questions you just raised, so I can't really answer. I would be happy to get back to you on that.

Mr. Raj Saini: Okay.

This is my final question. Let's suspend animation for a second and look at Amazon as a mall. You own the mall. You grant space to other retailers. You allow them to be on your platform. You control access to customers and you collect data on every site. You're operating the largest mall in the world.

In some cases, whenever small retailers show some success, you tend to use that information to diminish competition. Since you have access to all the third party people who are selling products on your site, do you think that's fair?

Mr. Mark Ryland: We don't use the data we acquire for supporting our third party seller marketplace. We don't use that data for purposes of our own retail business or for purposes of product lines that we launch.

Mr. Raj Saini: You're sure about that.

Mr. Mark Ryland: Yes.

Mr. Raj Saini: You're saying that if anybody lists a product on your website, you do not track the sales of that product to know which product is popular and which product is not popular.

Mr. Mark Ryland: We track the data for supporting that business and the customers of that business. We don't use that data in our retail business.

Mr. Raj Saini: You won't see which product is selling more or selling less and try to compete with that in any way.

Mr. Mark Ryland: In terms of the part of our business that supports this vast third party marketplace, which has enabled great success for thousands of companies and mom-and-pop shops around the globe, absolutely that part of our business uses the data to maximize the success of the marketplace. It's not used in our retail business.

Mr. Raj Saini: One of the complaints in the area of innovation is that a number of market players are dominant because of the access to data they have and because of their ability to retain and use that data. In many cases, smaller companies or smaller players don't have access to the data, don't have access to the market. More importantly, in some cases, when emerging companies are on the rise, the larger companies will buy the technology to kill the technology so it does not compete.

Is that something Amazon or Apple or Microsoft is involved in, in any way?

Mr. Mark Ryland: If you look at our history of acquisitions, they tend to be very small and very targeted, so in general, the answer would be no.

Mr. Erik Neuenschwander: I believe that's also the answer for Apple.

Mr. Raj Saini: I mean any emerging technology, any company that's emerging that might be a competitor to any of your platforms. You don't engage in that, or you just...? I don't get what you mean.

Mr. Erik Neuenschwander: The acquisitions that I'm familiar with have been companies like, say, AuthenTec, which was a firm whose technology we used to build the first version of touch ID into our phones. We look for technological innovations that we can integrate into our products, but I don't really see that as a fingerprint sensor company directly competing with Apple.

Mr. John Weigelt: We're actively involved with the start-up community around the world. Programs like BizSpark and Microsoft Ventures help our partners and start-ups really get their legs under them so that they can sell their product. We are a commodity software provider—we provide a common platform that helps communities around the world—so there will be areas that are innovated on top of our platform. We saw one such platform here built out of Montreal, Privacy Analytics, which was a start-up here that was doing perfect forward privacy. That was a technology that we didn't have that we thought would help catalyze our business, and as a result we acquired the company with the goal of building that into our products.

We make a decision about whether we build or buy based on the resources that we have, and in some cases there's great innovation out there that we acquire and build into our toolset. That's really how we look at that acquisition strategy.

Mr. Raj Saini: Thank you.

The Chair: Thank you, Mr. Saini.

Last up will be Mr. Baylis.

What's going to happen is Mr. Baylis will finish, and then we're going to start the rounds all over again. Delegations will all start from the top again, just to be clear.

Mr. Baylis, go ahead for five minutes.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Thank you, Chair.

Thank you to the witnesses. You're both very knowledgeable and very open and willing to answer questions, which was not exactly what we had yesterday, so I'm very grateful for that.

Mr. Davidson, in your opening remarks you mentioned that Google and Facebook have an opportunity to improve their transparency. Could you expand a bit on that, please?

● (1030)

Mr. Alan Davidson: Sure.

We do think that ad transparency is a major tool to think about in how we fight disinformation protection, particularly in the election context. We've been working with some of the other big players as part of this EU code of practice, to try to get better transparency tools out there for consumers to see what ads they're seeing and for researchers and for journalists to understand how these big disinformation campaigns happen. We have a fellow at the Mozilla Foundation working on this. The big frustration, honestly, is that it's very hard to get access to these archives of ads, even though some of our colleagues have pledged to make that access available.

We recently did an analysis. There are five different criteria that experts have identified—for example, is it historical? Is it publicly available? Is it hard to get the information? It's those kinds of things.

We put out a blog post, for example, that Facebook had only met two of the five criteria, the minimum criteria that experts had set for reasonable access to an ad archive. Not to pick on them—we've already picked on them publicly—but I'll say we hope we can do more, because I think without that kind of transparency....

Google did better. It got four out of five on the experts' chart, but without more transparency around ads, we're really stuck in trying to understand what kinds of disinformation campaigns are being built out there.

Mr. Frank Baylis: You mentioned that if they're not willing to self-regulate, you felt that they should be regulated. Did I understand that correctly?

Mr. Alan Davidson: What I was trying to say is that if we can't get better information....Transparency is the first step here, and it can be a really powerful tool. If we could have transparency and more notice to people about what political advertising they're seeing, that could go a long way toward helping to deal with these disinformation campaigns and this election manipulation. If we don't get that transparency, that's when it will be more reasonable for governments to try to step in and impose more restrictions. We think that's a second-best answer, for sure. That's what I think we were trying to get at.

Mr. Frank Baylis: My colleague, Charlie, my senior colleague—

Mr. Charlie Angus: Your older brother.

Mr. Frank Baylis: My older brother Charlie here has made an argument that some things should require consent—you talked about granular consent—while some things should just be prohibited. Do you agree with this line of thought?

Mr. Alan Davidson: We have said we believe that. We think it's important to recognize that there is a lot of value that people get out of different kinds of tools, even around things like health or financial or location information, so we want to give people that ability. Probably when you get to kids and certain kinds of health information, the bar needs to be very high, if not prohibited.

Mr. Frank Baylis: My colleague here, my younger brother Nathaniel, has said that certain age things.... For example, we prohibit driving at a certain age and we prohibit drinking at a certain age. Are there any thoughts from the rest of the panel on this concept of just out-and-out prohibiting some data collecting, whether it's age related or some type of data? Do any of you have anything to add to that?

Mr. Erik Neuenschwander: In my earlier answers I talked about how we seek to leave the data on the user's device and under their control. I'd separate collection by a corporate entity from collection from a device that's under the user's control. Where possible, we want to leave that control in the hands of the users through explicit consent and through retaining the data on their device.

Mr. Frank Baylis: If it's collected, but not used or seen by a corporation such as yours.... If the corporation has collected it and just held it, and then I can delete it or not, you see that as differentiated from collecting it for use elsewhere. Is that what you're saying?

Mr. Erik Neuenschwander: I do see collection from a company compared to being on the user's device as different. I almost wouldn't want to use the word “collection”. Maybe we should say “storage” or something.

Mr. John Weigelt: I take pause when I try to answer that question, to be thoughtful around potential scenarios. I try to imagine myself as a parent and how these tools would be used. I really think it depends on the context in which that interaction occurs. A medical setting will be dramatically different from an online entertainment setting.

The context of the data is really important in managing the data, in terms of the obligations for safeguarding protections or even for the prohibition of collecting that data.

Mr. Frank Baylis: Do I have time for another question, Mr. Chair?

The Chair: You do if you have a very quick, 30-second comment.

Mr. Frank Baylis: Leading into cloud computing, it sounds like a beautiful cloud, but there's no cloud. There's a physical server somewhere. That's what we're talking about. Let's forget the cloud; it's a physical server. The laws that apply to it depend on where that server actually sits.

We talk about Apple, Microsoft or Amazon—and Amazon, this is a big part of your business. If we Canadian legislators make a bunch of laws that protect Canada, but your server happens to be outside of Canada, our laws have zero impact.

Are you doing anything about aligning with government laws by making sure that these servers sit within the confines of the country that's legislating them?

● (1035)

Mr. Mark Ryland: We do have our data centres in multiple countries around the world, including Canada. There is legal control there, but we have to obey the laws of all the countries where we operate. Those laws may have extraterritorial impact as well.

Mr. John Weigelt: We have delivered data centres in 54 regions around the world and we've put data centres here in Canada, in Toronto and Quebec City. I happen to be accountable for making sure that they're compliant with Canadian laws and regulations, be it the Office of the Superintendent of Financial Institutions, the federal government's legislation or provincial privacy legislation. It's critically important to us that we make sure we respect the local legal environment. We treat data that's stored in those data centres like a piece of paper. We want the laws to make sure that they treat that electronic information like the piece of paper.

We have been staunch advocates for the CLOUD Act, which helps to clarify the conflict of laws that are a challenge for multinational companies like ours. We abide by laws around the regions, but sometimes they conflict. The CLOUD Act hopes to set a common platform for understanding around mutual legal assistance treaties, or to follow on from that—because we all understand that mutual legal assistance treaties are somewhat slow and based upon paper—this provides new legal instruments to to provide confidence to governments that their residents' information is protected in the same manner that it would be protected in local data centres.

The Chair: Thank you.

Thank you, Mr. Baylis.

It hasn't come up yet, so that's why I'm going to ask the question.

We're here because of a scandal called Cambridge Analytica and a social media company called Facebook. We wanted to differentiate between who you are. You're not social media; social media was here yesterday. You're big data, etc.

I have a comment specifically for Apple. This is why we wanted Tim Cook here. He has made some really interesting comments. I'll read exactly what he said:

> First, the right to have personal data minimized. Companies should challenge themselves to strip identifying information from customer data or avoid collecting it in the first place. Second, the right to knowledge—to know what data is being collected and why. Third, the right to access. Companies should make it easy for you to access, correct and delete your personal data. And fourth, the right to data security, without which trust is impossible.

That's a very strong statement. Apple, from your perspective—and I'm also going to ask Mozilla—how do we or how would you fix Facebook?

Mr. Erik Neuenschwander: I don't know that I would presume to even understand the aspects of Facebook enough to fix it.

What I know we can focus on is primarily two ways. I always put technological solutions first. What we want to do is put the user in control of the data and of access to the data on their device. We've taken it upon ourselves as part of our platform to put the operating system as a barrier between applications and the user's data, and to require that user's consent, as mediated by the operating system, to come in between that app and its data. This is a set of things that we've evolved over time.

You've heard comments today about trying to keep usability front of mind as well, so we're trying to keep things clear and simple for users to use. In doing that, we've built refinements into our technology platform that allow us to expand that set of data that the operating system.... Again, this is separate from Apple, the corporate entity. The operating system can take a step forward and put the user in control of that access.

That's a process that we're going to remain committed to.

The Chair: To me, changing legislation around this is very difficult, given all the parameters that are around us. It might be simpler for somebody like Tim Cook and an ideology that considers users as paramount. It might be simpler for Apple to do this than for legislators around the world to try to pull this off. However, we're giving it a soldier's try. We're definitely trying.

Mr. Davidson, do you have any comment on how we fix Facebook?

● (1040)

Mr. Alan Davidson: It's very hard from the outside to decide how to fix another company. I think a lot of us are really disappointed in the choices they've made that have created concern among a lot of people and a lot of regulators.

Our hope would be for privacy and more user control. That's a huge starting point.

I guess if I were going to say anything to my colleagues there, it would be to be a little less short term in their thinking about how to address some of these concerns. I think they have a lot of tools at their disposal to give people a lot more control over their information.

There are a lot of tools in the hands of regulators right now to try to make sure we have good guardrails around what companies do and don't do. Unfortunately, it sets a bad standard for other companies in the space when people aren't obeying good privacy practices.

We all can do things on our side too. That's why we built the Facebook container in our tracking tools: to try to give people more control.

The Chair: Thank you for your answer.

I'm getting signals for questions again. We'll start with my co-chair and we'll go through our normal sequencing. You'll have time. Don't worry.

We'll go to Mr. Collins to start it off.

Mr. Damian Collins: Thank you.

I will start with Mr. Ryland and Amazon.

Following on from the chair's comments about Facebook, if I connect my Amazon account to Facebook, what data am I sharing between the two platforms?

Mr. Mark Ryland: I'm not familiar with any way in which you do connect your Facebook account to Amazon. I know that Amazon can be used as a log-in service for some other websites, but Facebook is not one of those. I'm not familiar with any other connection model.

Mr. Damian Collins: You're saying you can't do it. You can't connect your Facebook and Amazon accounts.

Mr. Mark Ryland: As far as I know, that's true. I'll follow up to make sure that's true.

Mr. Damian Collins: There was the Digital, Culture, Media and Sport Committee in London, which I chaired with my colleagues here. We published some documents in December of last year that were relevant to the Six4Three case.

At the same time, there was also an investigation by The New York Times that suggested a series of major companies had entered into special data reciprocity agreements with Facebook so that they had access to their users' Facebook data and to their friends' data as well. Amazon was listed as one of those companies.

Could you say what sort of data protocols you have with Facebook and whether that gives you access not just to your customers' data or Facebook account holders, but also their friends as well?

Mr. Mark Ryland: I'll have to get back to you on that. I really don't know the answer to that question.

Mr. Damian Collins: It was a quite major story in The New York Times last year. I'm amazed that you were not briefed on it.

I'll ask the same question of Microsoft as well.

You can log into Skype with your Facebook account. Again, if you're connecting your Skype and your Facebook accounts, what sort of data are you sharing between them?

Mr. John Weigelt: As far as I understand, it's a simplified log-in from Facebook into your Skype account. When you connect, there should be a pop-up that provides you with an indication of what Facebook is giving to the Skype environment.

It's a simplified log-in type of environment.

Mr. Damian Collins: What type of data is shared between the different accounts? For users who do that, what type of data about their Skype usage is shared with Facebook?

Mr. John Weigelt: It's simply a log-on.

Mr. Damian Collins: Yes, but all these Facebook log-ins have data reciprocity agreements built into them as well. The question is whether—

Mr. John Weigelt: It's simply a simplified way to share an identity token, so to speak, so that you can log in to Skype.

Mr. Damian Collins: I know the way the basic log-in works, but these log-in arrangements with Facebook give reciprocal access to data between the two. There's actual connecting, effectively.

Mr. John Weigelt: It's nothing that would not have been disclosed in that initial connection, so when you connect, when you actually do that linkage, there is a pop-up that says this is the data that will be interacted or interchanged.

Mr. Damian Collins: Then it's in the terms and conditions.

Mr. John Weigelt: It's in the actual pop-up that you have to go through. It's a simplified term, and as I understand it, it's a tiered notice. It provides you notice of what the category of data is, and then as you click through it, you have the ability to dig deeper to see what that is.

Mr. Damian Collins: In layman's terms, would Facebook know who I was engaging with on Skype?

Mr. John Weigelt: I don't believe so, but I'd have to get back to you on that. I really don't believe so.

Mr. Damian Collins: Okay.

I'll just go back to Amazon. I want to quickly get this out.

Under "How do I connect my Facebook account to Amazon?", Amazon.com says:

> From Settings, tap My Accounts, and then tap Connect your social networks.
>
> Tap Connect Your Facebook Account.
>
> Enter your log-in information, and then tap Connect.

That is a pretty simple way of connecting your Facebook account with your Amazon account, so I'll just ask again: If you do that, what type of data are you sharing between the two platforms?

● (1045)

Mr. Mark Ryland: I'll need to get back to you on that. I really don't know the answer to that.

Mr. Damian Collins: Okay. I think this is pretty basic stuff. My concern is that data is being shared between the two platforms.

Again, in a question asked in The New York Times investigation, it said there were preferential data reciprocity agreements between Amazon, between Microsoft and Facebook, so that they not only had access to the data about the Facebook accounts of their users but the users' friends as well, which was a setting that had been turned off for other apps. However, the major partners of Facebook, in terms of the money they spend together or the value of the data, have preferential access.

Again, I'll ask one more time whether either Amazon or Microsoft can say something about that—the nature of the data, what it includes, and whether you still have those arrangements in place.

Mr. John Weigelt: I can't comment on—

Mr. Damian Collins: I don't know whether that means you don't know what to say or you don't know. Either way, if you could write to us, we'd be grateful.

Mr. Mark Ryland: Yes.

Mr. John Weigelt: Absolutely.

Mr. Mark Ryland: We'll follow up on that.

The Chair: We'll go next to Mr. Erskine-Smith for five minutes.

Mr. Nathaniel Erskine-Smith: Thanks very much.

I first want to talk about ethical AI. This committee started a study on this topic, and the Government of Canada now requires algorithmic impact assessments for government departments when they employ an algorithm for the first time, as a risk assessment in the public interest. Do you think that should be a requirement on large public sector, big-data companies such as yourselves?

I'll start with Amazon and go down the table.

Mr. Mark Ryland: We strive very hard to work on good algorithmic fairness, and it's one of our fundamental principles. We have test data sets to make sure that we're constantly meeting the bar on that.

Mr. Nathaniel Erskine-Smith: Do you think there should be transparency to the public so that there's proper public accountability with the algorithms that you employ with such large troves of data and personal information?

Mr. Mark Ryland: I think the market is doing a good job of making sure that companies set a good bar on that.

Mr. Nathaniel Erskine-Smith: You see, the frustrating thing is that previously you said you agree with the principles in the GDPR, and algorithmic explainability is a principle in the GDPR.

Apple, what do you think about it?

Mr. Erik Neuenschwander: In the machine learning that we employ, we do want users to understand that we do it primarily by putting it on the users' devices and training it on their data, as I've said. When we're training generalized models, we're doing that based on public data sets. Primarily, we're not training on personal data.

Where we would be training on personal data, we absolutely want to make sure that it is explainable and understandable by users.

Mr. Nathaniel Erskine-Smith: Then you believe in that public transparency.

Mr. Erik Neuenschwander: We believe in transparency across many things.

Mr. Nathaniel Erskine-Smith: Microsoft, would you comment?

Mr. John Weigelt: We're participating and we're contributing to the work that's happening here in Canada and one of the challenges around definitions. For large-scale unhuman intervention-type systems, there needs to be ability to tell the user what's happening behind the scenes.

It's a big area of controversy, a big area of research around explainability, generalizability, and how we look at outcomes.

The way that documentation is currently written, it almost looks as though if you have website localization—for example, if I am coming from Quebec and I then present a French website because of that—it would require algorithmic risk assessment and notice to the public.

Mr. Nathaniel Erskine-Smith: You're concerned with definition, but in principle you agree with the idea.

Mr. John Weigelt: In principle, we agree with the idea and applaud the Government of Canada for putting that in place right now, and others should examine similar opportunities.

Mr. Nathaniel Erskine-Smith: Including the private sector and Microsoft.

On competition law, I read a quote yesterday from the German regulator, who noted Facebook's superior market power and said, "The only choice the user has is either to accept comprehensive combination of data or to refrain from using the social network. In such a difficult situation the user's choice cannot be referred to as voluntary consent."

Does the same principle apply to your companies?

Mr. Mark Ryland: We face robust competition in the markets we're in. In the cloud business, for example, our main competition is the old way of doing IT business, and there's a vast array of competitors across that.

Mr. Nathaniel Erskine-Smith: I appreciate that. I'll flip it a bit. Should the impact on consumer privacy be a consideration in competition law?

Mr. Mark Ryland: Again, it's an area outside of my expertise. I hate to give that answer.

Mr. Nathaniel Erskine-Smith: It's frustrating, because I did specifically let Amazon know that competition would be a matter we'd be discussing today.

Other companies, do you have a view as to whether the impact on consumer privacy should be a consideration in competition law?

Mr. Erik Neuenschwander: You imply that there is, at least in some cases, a single, all-or-nothing sort of consent, and we're very cognizant of that. What we do is offer very nuanced and fine-grained consent. It's possible to use an Apple device without signing in to or creating any Apple account, so we try to differentiate and separate those things.

● (1050)

Mr. Nathaniel Erskine-Smith: I appreciate that.

Does Microsoft have a view?

Mr. John Weigelt: It's all about the data, and in particular safeguarding the data and how the data is used. I think you need to look more broadly at the data use. Perhaps data sheets for data would help in that regard, because I think privacy is about that data's security and accessibility.

Mr. Nathaniel Erskine-Smith: I'm interested in seeing what the associate general counsel says tomorrow at the competition commissioner's data forum.

I'm moving forward with a secondary question on competition law.

In the 1990s, Explorer was free, and yet Microsoft was prevented from monopolizing the browser space. It wasn't protecting consumers on price; it was actually protecting innovation.

I'm going to pick on Amazon a bit. You said before that what I input into Alexa becomes part of my user profile. I assume that also means that what I watch on Prime, purchase from any number of sellers and search for on Amazon or beyond on the Internet all combine into a single profile, presumably to direct targeted ads.

I also wonder if my user profile, combined with everyone's user profile, drives your decisions to create new products. Is that fair?

Mr. Mark Ryland: We certainly look at the trends, purchases and behaviour of our customers, in terms of determining future—

Mr. Nathaniel Erskine-Smith: Far apart from that, and in answer to Mr. Saini's questions, you said you're not tracking the information of third party sellers on your websites. If you look at it from the other perspective, you are tracking all of our individual purchase decisions on Amazon and combining all of those decisions in order to compete against those third party sellers in your marketplace. How is that not use of dominance?

Mr. Mark Ryland: I think the fact that the third party marketplace is wildly successful and that there are a huge number of very successful businesses in it is a very clear indicator that this is not a problem.

Mr. Nathaniel Erskine-Smith: You don't think you have an unfair market advantage.

Mr. Mark Ryland: No.

Mr. Nathaniel Erskine-Smith: The last question I have was raised by—

The Chair: Please go very quickly, because I know we're trying to squeeze everybody in.

Mr. Nathaniel Erskine-Smith: With respect to the monetization of personal data, I raised the point with experts yesterday that the business model is the problem. That was put forth by a number of folks, and Apple, I think—Tim Cook—made the same point about the industrial data complex.

Microsoft and Amazon, do you think the business model is itself a problem? You just want to collect more and more information about us. What's the value to us in your collecting so much information about us? Is the business model a problem?

Mr. John Weigelt: To be clear, the information we collect is only there for the products. We're not looking at doing things personalized to you and you only, to target to you.

When we find that people aren't using a feature, grosso modo we anonymize, pseudonymize, and that's a great feature. We try to surface that feature in subsequent releases. That's simply there to help enhance our business. We're a software and services company. That's what we do, and that's our business line.

Mr. Mark Ryland: Our business model is very consistent with consumer privacy, because it's all about meeting customer choice through a traditional purchase-and-sale model of capabilities and products and services.

Mr. Nathaniel Erskine-Smith: Thank you.

The Chair: Now we'll go to Mr. Angus for five minutes.

Mr. Charlie Angus: Thank you very much.

Diapers.com was an online business selling diapers in this competitive market that Amazon says is out there. Jeff Bezos wanted to buy it. They refused, so Amazon went to predatory pricing. Amazon was losing $100 million on diapers every three months to put a competitor out of business or to force them to sell. They finally agreed, because they were afraid Amazon would drop prices even lower.

We talk about antitrust because of the "kill zone" of innovation that The Economist is talking about, but with Amazon, it's the kill zone of competition—the power that you have through all of your platforms to drive down prices and actually put people out of business. Shaoul Sussman says that the predatory pricing practices of Amazon are antitrust in nature and need legislation.

What do you say?

Mr. Mark Ryland: Again, I have to say that I'm not an expert in competition law and I don't know the history or the details of some of the things you mention.

In the general business that we're in, we see robust competition across all these businesses. There are a lot of new start-ups, and we even have a great number of competitors who use our Amazon Web Services platform. Some of the largest online commerce platforms in, say, Germany and Latin America use AWS and trust us with their businesses, so we think competition is working.

Mr. Charlie Angus: Yes, so you've got all the people to use your cloud services and then you can drive down prices against mom and pop. Lena Kahn, from Open Markets, says that because you are controlling so much market dominance in so many various areas, you can use your profits from the cloud to run predatory pricing and to run down competition. She says that your "structure and conduct pose anticompetitive concerns—yet it has escaped antitrust scrutiny".

This is an issue that I think legislators need to think about. We see that in Canada one of the great advantages you have is that you're not paying taxes the way our poorest businesses have to. In the U.K., you made 3.35 billion pounds and paid only only 1.8 million pounds in taxable income. I mean, you're like our biggest welfare case on the planet if you're getting that.

In the U.S., it's even better. You made $11 billion in profits and you got a $129-million rebate. You were actually paying a negative 1% tax rate. That seems to me to be an extraordinary advantage. I don't know of any company that wouldn't want to get a rebate rather than pay taxes—or any citizen.

How is it that we have a marketplace where you can undercut any competitor and you can undercut any book publisher and you're not even properly paying taxes? Don't you think that it's at least our job to rein you guys in and make sure that we have some fair rules in the marketplace?

● (1055)

Mr. Mark Ryland: Again, I apologize. I'm not an expert in the competition law area. The panel discussion was on security, consumer protection and privacy, where I do have some expertise, but I'm not able to answer your questions on that area.

Mr. Charlie Angus: Yes, that's unfortunate. I mean, this is why our chair asked that we get people who would be able to answer questions, because these are the questions that as legislators we need to have answered. We're dealing in this new age, and your colleagues at Facebook have put us in this situation. If Facebook had better corporate practices, we might not even be paying attention, but we're having to pay attention. If Amazon was not engaged in such anti-competitive practices, we might think that the free market was great, but it's not great right now, and you can't answer those questions for us.

It puts us in a bind, because as legislators we're asking for answers. What's a fair taxation rate? How do we ensure competition in the marketplace? How do we ensure that we don't have predatory pricing that is deliberately driving down prices and putting businesses—our businesses— out of business because you have such market dominance and you can't answer the question? It leaves us very confused. Should we call Alexa or Siri? Would they help?

Voices: Oh, oh!

Mr. Mark Ryland: I apologize, but I don't have the expertise to answer those questions.

Mr. Charlie Angus: Thank you.

The Chair: I would like to highlight what Mr. Angus said. This is the reason we asked Mr. Bezos to come. He can answer those kinds of questions before this grand committee. He's exactly the person who could have answered all our questions. We wouldn't have kept anybody off the panel, but certainly we wanted people who could give us comprehensive answers with regard to the whole package.

I will go next to Mr. Lucas from the U.K.

Mr. Ian Lucas: John, could I return to transfer of data within Microsoft? You mentioned that Microsoft has acquired a number of companies. LinkedIn, which you mentioned, was one of them. Can you just be clear? If I give information to LinkedIn, within the Microsoft organization is it then transferred to other businesses within Microsoft?

Mr. John Weigelt: Absolutely not. LinkedIn remains rather independent from the organization.

Mr. Ian Lucas: You're saying there is a wall around the information that is collected by LinkedIn and it's not transferred within the Microsoft organization.

Mr. John Weigelt: Any transfer of.... Excuse me. Let me step back from that. Any connection between your LinkedIn profile and, let's say, your Office toolset is done by the user, and that's a connection that's done explicitly. For example, in your email clients, you may choose to leverage your LinkedIn connection there. That's something that the user intervenes with in their LinkedIn profile. It's their Office—

Mr. Ian Lucas: I'm interested in the default position. If I join LinkedIn and I don't go through the terms and conditions and I give information to LinkedIn, does it get transferred or is it capable of being transferred to other businesses within the Microsoft family, as you guys like to call it?

Mr. John Weigelt: LinkedIn doesn't share that information across the business from the back end.

Mr. Ian Lucas: As a general rule regarding the separate businesses within the Microsoft organization, is the information transferred generally?

Mr. John Weigelt: As a general rule, each business line is independent.

● (1100)

Mr. Ian Lucas: Is the information transferred between the separate businesses?

Mr. John Weigelt: Personal information is maintained by each individual business line.

Mr. Ian Lucas: I just asked a very specific question. Is the policy of the Microsoft organization to allow transfer of personal data between separate businesses owned by Microsoft?

Mr. John Weigelt: This is a consistent purpose—

Mr. Ian Lucas: Can I have a yes or no?

Mr. John Weigelt: It's a consistent purpose question, right? So we, as a—

Mr. Ian Lucas: It's a question to which either yes or no is the answer.

Mr. John Weigelt: I will have to answer that I cannot affirm or deny that there is.... I don't have that knowledge.

Mr. Ian Lucas: Right, okay. That's not very helpful.

Could you come back to me on that question?

Mr. John Weigelt: Absolutely.

Mr. Ian Lucas: Thank you.

Erik, I have in front of me two very impressive Apple devices, although my techie colleagues tell me that my iPhone is really very old.

The issue I have is that people access, for example, Facebook, very much through Apple, through the hardware that you provide. You have said that a lot of information goes into the Apple phone or the iPad, and it's not transferred elsewhere, and it's not your responsibility to transfer it elsewhere. I don't really buy that argument, because people access other platforms through your hardware.

You are one of the biggest businesses on the planet and you can deal with whom you like. Why should you be allowing businesses that don't agree with your approach to privacy to use your hardware to do business?

Mr. Erik Neuenschwander: I don't know if the businesses agree or disagree with our approach. I think we'd certainly encourage.... We try to demonstrate that people can copy us in our approach to privacy.

What my team seeks to do and what I think the focus is, as I said, is to put the information on the device, but I do think we have a responsibility about where it goes. That's why we've taken steps in our operating system to get in between an application and certain data on the device.

There is some data that we've never exposed on the device, and I don't think we would. For instance, the user's phone number or hardware identifiers that could be used for tracking have never been available on our platform.

We did this with the design of a technology we call sandboxing, which actually separates applications from themselves and from data in the OS.

Mr. Ian Lucas: My point is that you set out the principles. The chairman set them out, and it's really complex and difficult for us to legislate on these issues, as we're all discovering.

You can do business with Facebook or not. You could disallow access to Facebook through your hardware if you so chose if they did not adhere to the principles. Facebook has done your industry a lot of damage. Why do you continue to do business with them?

Mr. Erik Neuenschwander: I guess if you're talking about their availability on the App Store, I think there are two—

Mr. Ian Lucas: Well, it's a fact that so many people access Facebook through your devices.

Mr. Erik Neuenschwander: Right, so on one hand, under the hypothetical, if the Facebook application wasn't there, Facebook offers a website, and people would still be able to access Facebook through the website, through our browser, or through a competing browser.

If we go further down that route and say that we should actually begin imposing what I would call—

Mr. Ian Lucas: It's not imposing; it's about agreement. If you believe in your principles and you're an ethical company, then you should deal with people who abide by your principles. That's within your power.

Mr. Erik Neuenschwander: Well, I suppose what's within my power are the technical controls. My approach is to say that underneath any application or any service running on the phone, we should find technical measures to keep the user in control of their data.

Mr. Ian Lucas: What you could do is not do business with Facebook. You could choose an approach whereby you set out your principles and you apply them in dealing with who you want. Why don't you do that?

Mr. Erik Neuenschwander: If I take that as the availability of Facebook on our App Store, it would not measurably impact privacy to withdraw that application from the App Store.

Mr. Ian Lucas: You really don't?

Mr. Erik Neuenschwander: I think that users—

Mr. Ian Lucas: Do you think you'd get a bit of a headline?

● (1105)

Mr. Erik Neuenschwander: We'd get headline, sure. I don't personally believe that headlines necessarily impact privacy, with respect. I think users would—

Mr. Ian Lucas: Don't you think it would make a substantial impact on the approach that Facebook has been taking?

Mr. Erik Neuenschwander: As you point out, Facebook is an extremely popular service. Users would turn to web technologies in other ways to continue to access Facebook. I don't personally see a way that either Apple could or, out of respect for an individual's privacy, that I would be—

Mr. Ian Lucas: What concerns me is that you're presenting yourselves as the good guys, but you're facilitating the bad guys through the use of your hardware.

Mr. Erik Neuenschwander: We have taken many steps over the years to continue to constrain and raise the bar higher than any other platform on privacy and user control over the data on our hardware. It's precisely because of our hardware integration that we've been able to take so many positive, proactive steps toward putting users in control of data and finding ways to encourage date minimization.

Mr. Ian Lucas: But you still want to do business with the bad guys.

The Chair: Thank you, Mr. Lucas. We have to move on.

Next is Ms. Naughton, from Ireland.

Ms. Hildegarde Naughton: Thank you.

I want to go back to Mr. Ryland and my earlier question in relation to Amazon displaying the names and email addresses of customers. Were you categorical that it did not happen?

Mr. Mark Ryland: I'm certainly not familiar with the incident. I don't believe so, but we'll follow up.

Ms. Hildegarde Naughton: There were two articles on November 21, 2018, in The Guardian and The Telegraph. Both of them stated that Amazon suffered a major data breach that caused the names and email addresses of customers to be disclosed on its website.

Mr. Mark Ryland: I'd be happy to follow up on that.

Ms. Hildegarde Naughton: Thank you. I just wanted to clarify that. It's very much on the record.

The Chair: Go ahead, Mr. Lawless.

Mr. James Lawless: I have a question about data portability and the GDPR principle. It struck me as an issue.

In terms of big data, it's where it sits, how it's housed and what form it's kept in, etc. Is that something you embrace? Do you want to hold proprietary data, so that it's exclusive to your corporation, or is it something you're comfortable with using open formats to share? Where are each of you at on data portability at the moment?

Mr. Alan Davidson: We think access and data portability are extremely important parts of the GDPR and are actually really important pillars of any good privacy rules. Not only that, but they also could have a positive effect in the competition space. We think there's a lot of promising work to be done in not just getting people to be able to see what people have—and we do that when we hold data—but also in making it useful.

It's not just, "I can download my entire Facebook corpus of data"—which I've done and people should do, and it's really interesting—but it's also making it useful, so that I could take it somewhere else if I wanted to.

Mr. John Weigelt: We're committed to the GDPR and the data portability principles. The big question comes around the interoperability of those profiles or that data, and making sure that you can move them from one place to another in a format that's appropriate. The jury is still out about where people want to move their data and in what formats.

Mr. James Lawless: Microsoft has advanced on that. I know at one stage there was an alleged issue at Microsoft in terms of proprietary formats, but I know now there's always an option to "save as" in a more open format. Is that where you've gone with that?

Mr. John Weigelt: Absolutely. We've even seen in cloud computing the industry move to take arbitrary activities and move them from one place to another. That's something that we've embraced. We've also looked to the open-source/open data community for advice and guidance.

Mr. Erik Neuenschwander: In the expectation of GDPR, Apple launched a data and privacy portal. Users can download their personal information, both under access and under portability, in human and machine-readable formats.

Mr. Mark Ryland: Speaking for Amazon web services, where I work, importing and exporting are fundamental capabilities of our platform. We never have an import service that doesn't have an accompanying export service, whether they are virtual machine formats or other kinds of import/export data formats. We have tools always going bidirectionally.

We also work a lot with the open-source community for the portability of application codes and so forth. For example, a lot of our platforms are supporting things like docker formats for containers, Kubernetes for cluster management and so forth. Users can very readily create highly portable systems and data portability across platforms. That's something customers expect, and we want to meet those customer needs.

● (1110)

Mr. James Lawless: You're saying it's the likes of Apache and the open-source foundations and those sorts of guidelines. We're merging open standards, and I suppose they're being embraced to an extent, or maybe they were pre-GDPR-type community concepts, but they're pretty much across the board now. Is that the case?

Mr. John Weigelt: Absolutely.

Mr. James Lawless: Yes, okay. That's very good. Thank you.

Thank you, Chair.

The Chair: Next we'll go to Singapore for five minutes.

Ms. Sun Xueling: Mr. Davidson, you mentioned earlier in a reply to Mr. Baylis that with regard to political ads, your first preference was for company action to promote transparency. I'd like to highlight two instances in which it seems that company action has fallen short.

In April 2018, Facebook implemented new rules for political ad transparency. They acknowledged they were slow to pick up foreign interference in the 2016 U.S. elections. They said they were increasing transparency around ads and that this would increase accountability, yet in late October 2018, Vice News published a report showing how easy it was to manipulate the so-called safeguard that Facebook had put in place. The reporters had been required to have their identification verified as having U.S. addresses before they could buy ads, but once verified, the reporters were able to post divisive ads and lie about who paid for them.

That's for Facebook.

Separately, in August 2018, Google said it had invested in robust systems to identify influence operations launched by foreign governments, but shortly after that, a non-profit organization, Campaign for Accountability, detailed how their researchers had posed as an Internet research agency and bought political ads targeting U.S. Internet users. According to CFA, Google made no attempt to verify the identity of the account and they approved the advertisements in less than 48 hours. The adverts ran on a wide range of websites and YouTube channels, generating over 20,000 views, all for less than $100.

Therefore, it does not sound as if the platforms are anywhere close to fulfilling their assurance to safeguard against foreign interference.

Would you agree with that?

Mr. Alan Davidson: I think we clearly have a long way to go, absolutely, and it's been frustrating for those of us working in this space because we think that ad transparency is an incredibly important tool in being able to do this, and the other tools are not as good.

Ms. Sun Xueling: Yes. It does not seem that it's a technical problem per se, because the researchers flagged that they used the Russian IP address to access Google's Russian advert platforms and supply the details of the Internet research agency, and they went as far as to pay for the adverts using Russian rubles.

That seems to suggest to us that it's more about a desire to sell ads rather than to cut foreign interference.

Mr. Alan Davidson: I'd caution you a little. The jury is still out. It's still early days. There's a lot more to do, I think. Perhaps the experience in the parliamentary elections in Europe and the elections in India will be informative. That's where people were trying to take much more proactive steps. I think we need to be able to assess that. That's partly why transparency is important.

Platforms need to do more, but as somebody else among your colleagues has pointed out, we should also look at who is perpetrating these acts—

Ms. Sun Xueling: Definitely, yes.

Mr. Alan Davidson: —and this is where we as companies need the help of government when nation states are attacking companies.

Ms. Sun Xueling: You used the term earlier about having guardrails.

Mr. Alan Davidson: Yes.

Ms. Sun Xueling: I think that's important to prevent all of us from dropping into the abyss of disinformation.

Mr. Alan Davidson: Agreed.

Ms. Sun Xueling: Thank you.

Chair, thank you.

The Chair: Thank you.

We'll go to Anita next. Go ahead.

Ms. Anita Vandenbeld: To change the topic a little, in your opening remarks, Mr. Davidson, you talked about the fact that your company's workforce is focusing more on diversity. We know and we've heard testimony that algorithms are influenced by the social biases of those who are programming them, so if most of the programmers are young 20-something males, their social bias will be perpetrated through the algorithms.

How important is it that the workforce be diversified? How are you doing that, and what impact is it having?

Mr. Alan Davidson: We think it's extremely important. It's essential not just because it's the right thing to do—and it is the right thing to do—but also because our argument is we all will build better products if we have a more diverse workforce that reflects the broader base of the communities we serve.

It's been a big struggle in Silicon Valley, in the tech industry generally, and I think we all should acknowledge that. We constantly need to work on it.

We've made it a very big priority in our company. As an example, every executive in our company has goals for the year. We call them objectives and key results. We all set our own, but one is mandatory for everybody: How well did you do in diversity in your hiring? It adds that little extra push to know you're being graded on it.

We need to do more of that, and we will be the first to say we have a way to go. I think we've probably made a lot of progress in gender diversity, particularly within our technical community. We've done less well and still have a long way to go on other kinds of ethnic diversity, and we are really working on it.

● (1115)

Ms. Anita Vandenbeld: Thank you.

Mr. Alan Davidson: Thank you for raising it.

Ms. Anita Vandenbeld: Could I ask the other platforms to each comment on that aspect?

Mr. John Weigelt: At Microsoft, Satya Nadella has made it a top priority, and we recognize that our decisions and our products are better if our company better reflects the communities we serve.

Here in Canada, we're working to have Microsoft Canada reflect the cultural mosaic that Canada has, which includes not only gender but ethic backgrounds and orientation. Also, for those people who have unique adaptive requirements and unique work styles, such as visual challenges or hearing challenges or perhaps mental attention challenges....

Really, we're creating that community, and we build that into our AI ethics program. We have a governance committee that looks at sensitive uses of AI, but then we convene a very diverse community to do a 360° view of that sensitive use. We want very explicitly to have that cross-sectional perspective from every person in the organization who has a comment and to represent, again, that cultural mosaic. That way, we feel we can address some of those potential unintended consequences up front and be able to provide advice and guidance going forward.

Ms. Anita Vandenbeld: Go ahead.

Mr. Erik Neuenschwander: Diversity is one of the four corporate values that our CEO Tim Cook has espoused, in addition to privacy. They're both quite important. It goes far beyond AI. Certainly speaking from a privacy dimension, it's very much about the human condition, and having a diversity of viewpoints will help us make good choices.

I don't have the numbers at hand about how our diversity is today. I'm sure we still have a long way to go. We have taken steps not only to improve our hiring and our outreach in terms of bringing diverse people into the workforce, but also in taking a look at churn, or career longevity. It's one thing to get somebody in the door, but you also want to make sure they have a productive and fulfilling career experience to stay and continue contributing.

As I said, we have more work to do on both of those dimensions.

Ms. Anita Vandenbeld: Thank you.

Mr. Mark Ryland: You'll hear a similar story from Amazon. We place a big focus on diversity. It's a big part of our corporate goals, and hiring managers and executives are given specific goals in that area.

Of course, it's not just a matter of hiring. It's also a matter of career longevity, career management and creating communities of interest within our company that allow people to feel both integrated into the larger organization and to have communities of interest that they feel very much at home in.

We do a lot of work across all those areas to increase the diversity of the business. Again, we think that's best for business. Not only is it the right thing to do, but it will help us to build better products, because the diverse backgrounds of our employees will match the customers we're trying to serve.

Ms. Anita Vandenbeld: Thank you.

The Chair: Thank you, Ms. Vandenbeld.

I have an explanation of what's going to happen. We have a few more comments, and then we're going to have some final closing comments of the IGC from our vice-chairs, my co-chair and then me. Then we'll be done. It might go a little past 11:30, but it will be very close.

I have Mr. Kent for five minutes.

Hon. Peter Kent: Thank you, Mr. Chair.

If I could come back to the topic of competition, antitrust and monopolies in the new marketplace, there's been a lot of discussion recently, particularly in the United States, about the new digital monopolies and the fact that they may be a lot more durable than monopolies in the past—the railroads, the phone companies and so forth. They can overwhelm competition by either buying it or destroying it.

Yesterday I quoted, to the Facebook representative who was before us, the writings of Chris Hughes, the disillusioned former co-founder of Facebook. I know there's been some suggestion from some of our panellists today that their companies may be willing to accept versions of the European legislation, but one of Mr. Hughes' headlines suggests that Facebook should, in fact, be broken up and be subject to antitrust application. He said, “Facebook isn't afraid of a few more rules. It's afraid of an antitrust case”.

I know the defence against antitrust prosecution is a little more difficult because your big data monopolies use the excuse that your service is free and that there's not a tangible or identifiable dollar cost to what consumers are buying.

Again, this question may be greater than your job descriptions allow, which is why we asked that CEOs be present with us today, but I wonder, particularly in the case of Amazon and Microsoft, if you could discuss your companies' views with regard to countering these growing antitrust discussions and calls for breakup in the interests of greater competition and greater consumer protection.

I'll start with Mr. Ryland.

● (1120)

Mr. Mark Ryland: I'd be happy to say a few words about that.

Again, our business model is very traditional. We're selling goods and services—they have monetary value—both in our retail Amazon.com business and our cloud computing business, and we are facing robust competition across all kinds of different services and platforms that are not limited to online. There's a vast variety of channels and mechanisms that people use to acquire IT services, whether it be for a cloud or other kinds of capabilities. It's just a very different business model from our perspective, and our use of data to enhance the consumer experience is, we believe, very much adding value for consumers, and they really enjoy the experience of using these technologies.

I think it's a very different approach to some of the issues that you raise. Again, that's kind of a high-level statement, and beyond that, in terms of specifics around competition law, I've already disclosed that I'm not an expert.

Again, I think our business model is very traditional in that regard, so I think it's a bit different.

Hon. Peter Kent: Thanks.

I'll go to Microsoft.

Mr. John Weigelt: I think that as you look at our longevity since the seventies, we've seen ebbs and flows. We used to have a phone. We have a great browser, but it has undergone a number of revisions. The vision of having a PC on every desktop has now changed to a phone in every pocket. We see these ebbs and flows that move through the environment.

As for the consumer data environment, consumers will go to services that are popular to them, and they will have ebbs and flows. Certainly if you speak with millennials today, the millennials are off in different places. For example, my children, who are kind of in that space, although they'll disagree that they're millennials, will say, "Dad, I'm not there, so don't talk to me on that channel—talk to me on this channel." These things ebb and flow.

The data then lends itself to algorithms. We see an algorithmic age coming, and people using algorithms as a monetization technique. We see a move from algorithms to APIs and people monetizing APIs.

What we have is this continual innovation engine that's moving forward. We need to work together to try to figure out those unintended consequences, the lessons that we are learning along the way when it comes to disinformation, such as, for example, the squishy bag that happens when we push down on one place and then are surprised when it's "Oh, we didn't think about that." Working together, then we can put in place those instruments to be able to do that.

I've abstracted this out, I know, from your question around anti-competition and antitrust, but I'd like to look at it from the macro level and how these things ebb and flow. How do we then put in place strong protection mechanisms for businesses and for people? That's through partnerships.

Hon. Peter Kent: Next are Apple and then Mozilla.

Mr. Erik Neuenschwander: I don't know that I have much to add to the comments of the other panellists. I think that we are very much about both trying to put the diversity of the App Store in front of our users and trying to enable great competition. I think that has been wildly successful for many different companies in that space.

When it comes to personal data, we practice data minimization and are not trying to empower Apple but instead to empower users.

Mr. Alan Davidson: I would just say that I work at a company that in some ways has its roots in a reaction to a dominant player in the market, which at the time was Internet Explorer. I think we do believe that antitrust law provides some really important guardrails in the market. We want what everybody wants, which is a level playing field of competition.

We think there are a lot of concerns out there about size. With size comes responsibility. We also think that there are a lot of very powerful tools in the hands of antitrust regulators today. We probably need to think about how to give them more information, more tools and a better understanding of things such as APIs and the power of data in their analysis. That's really where the upgrade needs to happen first, even as we think about how to expand the roles. This is a very important area.

● (1125)

Hon. Peter Kent: To contemporize digitally...?

Mr. Alan Davidson: A contemporized digital antitrust enforcer is what we need out there.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Last in the line of questions is David. Go ahead, Mr. Graham.

Mr. David de Burgh Graham: Thank you.

I got everybody else earlier, so I want to go to Mr. Ryland from Amazon for a bit.

Earlier you were talking to Mr. Lucas about whether Alexa has ever been compromised. As I recall, you said that it has not. Is that correct?

Mr. Mark Ryland: That's right.

Mr. David de Burgh Graham: Are you not familiar with the Checkmarx hack of only a year ago that did a complete compromise of Alexa and could cause Alexa to stream live audio in an unlimited amount?

Mr. Mark Ryland: I wasn't familiar with that particular.... I'll get back to you on that.

Mr. David de Burgh Graham: Are you not the director of security engineering?

Mr. Mark Ryland: What's that?

Mr. David de Burgh Graham: Are you not the director of security engineering?

Mr. Mark Ryland: I am, at Amazon Web Services, yes.

Mr. David de Burgh Graham: You're at Amazon Web Services; so we weren't sent someone from Amazon proper. I just wanted to get that clear.

Amazon has an integrated marketing system. If I go and search for something on Amazon, and then I go onto another computer on another website, I will have ads pop up for me from Amazon saying, "Hey, do you want to buy this thing that you searched for on a different device on a different day at a different time with a different IP address?" How does Amazon know that? What kind of data exchange happens between Amazon and other sites like Facebook and other websites all across...? For example, National Newswatch does that to me.

What is the information exchange there? How do you know who I am on another device?

Mr. Mark Ryland: We do participate in ad exchanges. We have a whole privacy site on our website that allows you to opt out of advertising. Again, that's not personal data. That's anonymized data. It's based on demographic profiling.

Again, it's straightforward to opt out of that on our website, or you can use some of the industry's tools, such as AdChoices, to opt out from participating in ad networks.

Mr. David de Burgh Graham: It's anonymized data, but it knows exactly that one thing that I looked for three hours ago.

Mr. Mark Ryland: I can't speak to the very specific experience you had, but we're not using your personal data for that type of use case.

Mr. David de Burgh Graham: Okay.

At the very beginning of the meeting, you had some interesting perspectives on consent for the use of data. It caused a very good intervention from Mr. Angus. In Amazon's opinion or in your opinion, what is the limit of consent for the sharing of data? Is it explicit? If something is advertised on the box as a "smart" device, is that enough for consent to share data?

Mr. Mark Ryland: We think context awareness makes sense. The reasonable consumer consuming a certain experience will have some idea of what is involved. If that is not there, then we want that to be more explicit. It's very contextual.

It also depends, obviously, on the type of data. Some data is much more sensitive than other data. As one of the other panellists mentioned, using an online gaming platform is different from using a health care site, so it's being context aware and content aware. Context-based consent makes a lot of sense.

Mr. David de Burgh Graham: Okay.

You mentioned earlier that you're a customer-oriented company. Are you also a worker-oriented company?

Mr. Mark Ryland: Yes. We very much try to be very worker-oriented.

Mr. David de Burgh Graham: Do you not get engaged in anti-union practices?

Mr. Mark Ryland: Again, it's not my area of expertise, but I would say that we treat our workers with respect and dignity. We try to pay a solid wage and give them reasonable working conditions.

Mr. David de Burgh Graham: Do you engage in any data collection from your own employees?

Mr. Mark Ryland: Like all companies, we collect data around things like web access and an appropriate use of our technology to protect other workers in the workforce.

Mr. David de Burgh Graham: Then at no time did Amazon distribute anti-union marketing materials to newly acquired companies.

Mr. Mark Ryland: I'm not familiar with that particular scenario.

Mr. David de Burgh Graham: Well, the next time we have this committee, I hope we have somebody at Amazon who knows the policies of Amazon rather than AWS. You do very good work at web services, but we need to know about Amazon as a whole company.

I think that's all I have for the moment. Thank you.

The Chair: Thank you, David.

I did neglect Jo from the U.K., and—

Mr. James Lawless: Chair, before you hand it to Ms. Stevens, I must apologize; we need to catch a flight.

I would just thank the committee for the engagement over the last few days.

The Chair: All right. Thank you. We will see you again in November of this year.

Mr. James Lawless: Absolutely.

The Chair: Give our best to Ms. Naughton. Thank you for coming.

Mr. James Lawless: Thank you very much.

The Chair: Go ahead, Jo.

Ms. Jo Stevens: Thank you very much, Chair.

I want to go back to something you said earlier, John, about a board or a group that you have to look at sensitive use of AI. Can you give me an example of what sort of AI deployment you would describe as "sensitive"?

● (1130)

Mr. John Weigelt: One area is the use of artificial intelligence in medical diagnosis. We look at three criteria: Can it approve or deny consequential services? Is there infringement on human rights or human dignity? Are there health and safety issues at hand?

In one case, researchers were training artificial intelligence algorithms on chest X-rays. They then wanted to put that onto the emergency room floor, and they said, "Hey, this might impact patients. We need to understand how this works." Our committee came together. We reviewed the datasets. We reviewed the validity of that open-source dataset and the number of people there. Then we provided guidance back to the researchers who were putting this in place. The guidance was along the lines of, "Hey, this is not for clinical use", because software as a medical device is a completely different area. It requires certifications and whatnot.

However, if we're trying to assess whether or not artificial intelligence could potentially have the ability to learn from these scans, then that would be a good use. That's how we would tend to look at that situation.

Ms. Jo Stevens: That's a really useful example. Thank you.

We do know, and there's plenty of evidence about this, that there is both deliberate and unconscious bias inherent in AI. I think there's quite a strong argument for a regulatory approach to govern AI deployment, much like we have in, say, the pharmaceutical sector. When you look at a product, before you can put it on the market, you have to look at what might be the unintended side effects of a particular medicine.

What do you feel about that? Do you think there is an argument for a regulatory approach, particularly because, as we know, the current deployment of AI does discriminate against women and does discriminate against black and ethnic minority citizens? People are losing jobs and are not gaining access to services like loans and mortgages because of this.

Mr. John Weigelt: Absolutely. I think your point is well made around the unintended creep of bias into AI decision-making solutions, so we do need to guard against that. It's one of those engineering principles that we're working hard on to come out with guidance and direction to our teams.

There are some areas where we've advocated for very swift and direct action to move more carefully and more deliberately, and one area is facial recognition software. It's to your very point that a lot of these models have been trained on a very homogeneous community and are therefore not looking at the diverse community that they must serve.

We are quite strong advocates for putting in place legislative frameworks around some of the consent regimes, such as whether you have banners on the streets that say that, whether you have measurements, what the difference is between public and private space, and things like that.

Ms. Jo Stevens: How willing are you to make the work that you've been doing public? I appreciate if you're doing it behind the scenes. That's great, but it would be useful to know what you're doing and what your colleagues are doing.

Mr. John Weigelt: Absolutely. Clearly, we need to do more about advising and alerting the community about all the great work that's under way. We've published guidance around bots and how to make sure that bots are behaving properly, because we've had our own negative experience around a foul-mouthed, bigoted bot that was trolled for a while. We learned from that. Our CEO stood behind our team, and we did better. Now we've provided guidance, and it's publicly available.

We have what is called the AI Business School, which has a complete set of lectures for business leaders to put in an AI governance model. We're working with that community to help them. We're working to evangelize the work that we're doing internally around our AI ethics overview.

Lastly, I would say that we're working in the 60-plus different regulatory guidance document activities that are happening around the world so that we can start to socialize this from a practical experience perspective. Here in Canada there's the AI impact assessment and the AI ethics guidance standard that are being developed.

Ms. Jo Stevens: It would be really nice to see a virtual assistant that is not a subservient female in the future. I look forward to seeing something different.

Thank you.

The Chair: Thank you, Jo.

Now we'll get into our closing comments from our vice-chairs and then the co-chair.

Nate, would you start with your 60 seconds, please?

Mr. Nathaniel Erskine-Smith: I think if we've learned anything from the last few days, it's that we continue to live in an age of surveillance capitalism that has the potential for serious consequences to our elections, to our privacy and to innovation, frankly.

While it has been frustrating at times, I do think we have made progress. We have had every single platform and big data company now say what they haven't said previously: They are going to embrace stronger privacy and data protection rules.

We had the platforms yesterday note that they need public accountability in their content control decisions and yesterday they acknowledged corporate responsibility for algorithmic impacts, so there is progress, but there is also a lot more work to do with respect to competition and consumer protection, and with respect to moving from an acknowledgement of responsibility for the algorithms that they employ to real accountability and liability when there are negative consequences to those decisions.

I think there's a lot more work to do, and that will depend upon continued global co-operation. I think our Canadian community has worked across party lines effectively. This international committee has now worked effectively across oceans, in some cases, and across countries.

The last thing I will say is that it's not just about addressing these serious global problems with serious global co-operation among parliamentarians; it requires global co-operation from companies. If there is any last takeaway, it is that the companies simply didn't take it seriously enough.

● (1135)

The Chair: Thank you, Mr. Erskine-Smith.

Next we will go to Charlie.

Mr. Charlie Angus: Thank you to our two excellent chairs. Thank you to our witnesses.

I think we have seen something extraordinary. I've been very proud of the Canadian Parliament and our willingness to be part of this process.

There's been some extraordinary testimony in terms of the quality of questions, and I've been very proud to be part of it. Two extraordinary facts are that we have never in my 15 years ever worked across party lines on pretty much anything, and yet we came together. Also, we have never, ever worked across international lines. We can thank a Canadian whistle-blower, Christopher Wylie, who opened the door to the digital Chernobyl that was happening around us.

As politicians, we stay away from complex technical things. They frighten us. We don't have the expertise, so we tend to avoid them, which I think was a great advantage for Silicon Valley for many years.

These things are not all that technical. I think what we've done these last two days with our international colleagues—and what we will continue to do internationally—is to make it as simple and clear as possible to restore the primacy of the person in the realm of big data. Privacy is a fundamental human right that will be protected. Legislators have an obligation and a duty to protect the democratic principles of our country, such as free expression and the right to participate in the digital realm without growing extremism. These are fundamental principles on which our core democracies have been founded. It's no different in the age of the phone than it was in the age of handwritten letters.

I want to thank my colleagues for being part of this. I think we came out of this a lot stronger than we went in, and we will come out even further. We want to work with the tech companies to ensure that the digital realm is a democratic realm in the 21st century.

Thank you all.

The Chair: Thank you, Charlie.

Go ahead, Damian.

Mr. Damian Collins: Thank you very much, Mr. Chairman.

I'd just like to start by congratulating you and the members of your committee for the excellent job you've done in hosting and chairing these sessions. I think it's done exactly what we hoped it would do. It has built on the work we started in London. I think it's a model for co-operation between parliamentary committees in different countries that are working on the same issues and benefiting from related experience and insights.

The sessions have been split between what we call social media companies yesterday and other data companies here. Really what we're talking about is that while there are different functions, these are all basically huge data businesses. What we're interested in is how they gather their data, what consent they have for doing so and how they use it.

Across the sessions, time and again we saw companies unwilling to answer direct questions about how they gather data and how they use it. Whether it's asking how Amazon and Facebook share data.... Even though this is widely reported, we don't know. My colleague, Mr. Lucas, asked about LinkedIn and Microsoft data being shared. It's possible to totally integrate your LinkedIn data with your Microsoft tools, and a quick Google search can tell you exactly how to it.

I don't understand why companies are unwilling to talk openly about the tools they put in place. People may consent to use these tools, but do they understand the extent of the data they're sharing when they do? If it's as simple and straightforward as it seems, I'm always surprised that people are unwilling to talk about it. For me, these sessions are important because we get the chance to ask the questions that people won't ask and to continue to push for the answers we need.

Thank you.

The Chair: I'll speak to the panellists first and then get into some closing comments.

I want to encourage you. You had promised, especially Mr. Ryland, about giving us a lot of the documents that you didn't.... Various commenters didn't have all the information that we were asking for. I would implore you to provide the information we requested to the clerk next to me so we can get a comprehensive answer for the committee. We'll provide it to all the delegates here.

Something that's really going to stick with me is a comment by Roger McNamee about the term "voodoo dolls".

I watch my kids. I have four children. One is 21, one is 19, one is 17 and one is 15. I watch them becoming more and more addicted to these phones. I see work done by our colleagues in London about the addictive capabilities of these online devices. I wondered where are they going with this. You see that the whole drive from surveillance capitalism, the whole business model, is to keep them glued to that phone, despite the bad health it brings to those children, to our kids. It's all for a buck. We're responsible for doing something about that. We care about our kids, and we don't want to see them turned into voodoo dolls controlled by the almighty dollar and capitalism.

Since we like the devices so much, I think we still have some work to do to make sure we still provide access. We like technology and we've said that before. Technology is not the problem; it's the vehicle. We have to do something about what's causing these addictive practices.

I'll say thanks and offer some last comments.

Thanks to our clerk. We'll give him a round of applause for pulling it off.

He has that look on his face because events like this don't come off without their little issues. We deal with them on a real-time basis, so it's challenging. Again, I want to say a special thanks to Mike for getting it done.

Thanks also to my staff—over to my left, Kera, Cindy, Micah, Kaitlyn—for helping with the backroom stuff too. They're going to be very much de-stressing after this.

I'll give one shout-out before we finally close—oh, I forgot the analysts. Sorry. I'm always forgetting our poor analysts. Please stand.

Thank you for everything.

Thanks to the interpreters as well. There were three languages at the back, so thank you for being with us the whole week.

I'll give a little shout-out to our friend Christopher Wylie, despite being upstaged by sandwiches. I don't know if somebody saw the tweets from Christopher Wylie: “Democracy aside, Zuckerberg also missed out on some serious sandwich action.” He suggested that I mail the leftovers to Facebook HQ. Maybe that's the way we get the summons delivered into the right hands.

I want to thank all the media for giving this the attention we think it deserves. This is our future and our kids' future.

Again, thanks to all the panellists who flew across the globe, especially our U.K. members, who are our brothers and sisters across the water.

Singapore is still here as well. Thank you for coming.

Have a great day.

We'll see you in Ireland in November.

The meeting is adjourned.