HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

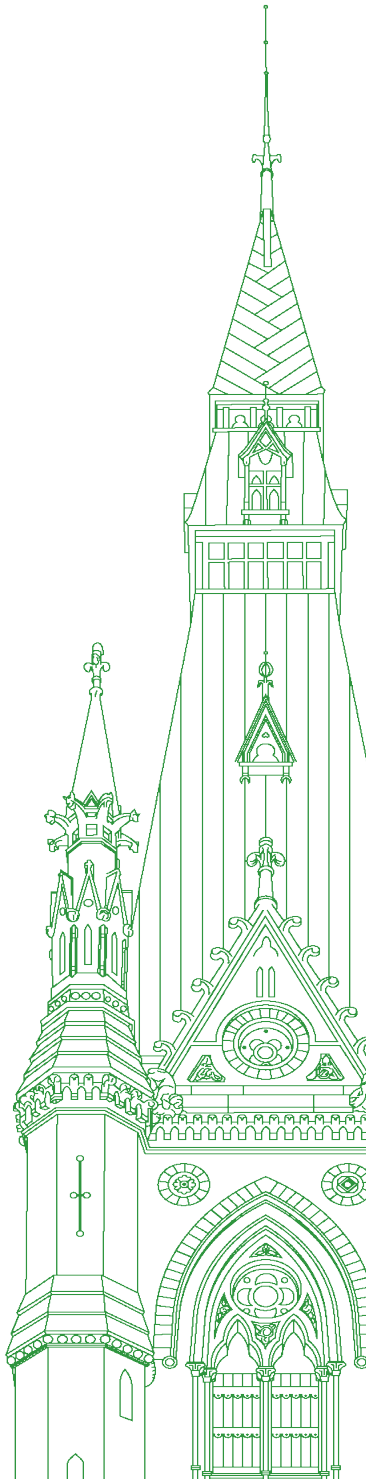
43rd PARLIAMENT, 1st SESSION

Standing Committee on Industry, Science and Technology

EVIDENCE

NUMBER 017

Thursday, May 21, 2020



Chair: Mrs. Sherry Romanado

Standing Committee on Industry, Science and Technology

Thursday, May 21, 2020

● (1700)

[*English*]

The Chair (Mrs. Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.)): Good afternoon. I now call this meeting to order.

Welcome to meeting number 17 of the House of Commons Standing Committee on Industry, Science and Technology. Pursuant to the order of reference of Saturday, April 11, the committee is meeting for the purpose of receiving evidence concerning matters related to the government's response to the COVID-19 pandemic.

Today's meeting is taking place by video conference. The proceedings are being made available via the House of Commons website.

I would like to remind the members and the witnesses to please wait before speaking until I recognize them by name. When you are ready to speak, please unmute your microphone and then return to mute when you are finished speaking. When speaking, please speak clearly and slowly so that the translators can do their work.

As is my normal practice, I will hold up a yellow card when you have 30 seconds left in your intervention, and I will hold up a red card when your time for questions has expired.

I'd now like to welcome our witnesses.

[*Translation*]

We're joined by François Perron, director of CyberQuébec.

[*English*]

From Google Canada, we have Colin McKay, head of government affairs and public policy. From IBM Canada, we have Eric Johnson, partner, British Columbia public sector, global business services. From Mimik, we have Fay Arjomandi, founder, president and chief executive officer; and Michel Burger, chief technology officer.

Each witness will present for seven minutes, followed by a round of questions.

With that, I will start with CyberQuébec, Monsieur Perron.

[*Translation*]

Mr. Perron, you have seven minutes.

Mr. François Perron (Director, CyberQuébec): Good afternoon, everyone. Thank you for inviting me to this meeting.

My name is François Perron, and I'm the director of CyberQuébec. I run the college centre for technology transfer at the Cégep de l'Outaouais. This CCTT consists of a team of cybersecurity researchers. It's one of 59 other centres in a network that currently involves over 1,400 researchers. I'm also a technology entrepreneur, a teacher and a researcher. I've worked on telecommunications, transportation and renewable energy projects.

My remarks will be divided into three main parts. First, I'll provide some context. I'll then give three impressions. Lastly, I'll give a short introduction to the principles that I believe are important for discussing geolocation solutions.

First, regarding the context, the needs are currently exacerbated. We're all going through a much-needed lockdown in response to a pandemic that's pushing all Canadians online. Our needs are universal. We know that the Internet must be accessible to everyone. Right now, I'm thinking a great deal about the most vulnerable people. It's not necessarily a matter of age. Isolation can also be a factor, along with, perhaps, the ability to use technology. Clearly, because of the current physical distancing and voluntary isolation, we have greater needs. All areas of our lives are affected. Basically, we're in an acceleration phase, where the expected transition to digital services has been catapulted at high speed.

In my view, for all this to work, the concept of online trust is very important. The quality and security of the digital services that we use revolve around a few key principles, including the ability to create trust during a transaction. The foundations of online trust depend on our ability to confirm the identity of those whom we're speaking to during a transaction and to leave non-refutable traces that can't be erased or falsified for the purpose of entering into contracts. That's the current context.

Three impressions emerge when we start talking about geolocation, particularly with regard to recent identity theft. I don't think that we need to go over what has happened in the industry in recent months. Clearly, the government's use of a unique identifier—I'm talking about the social insurance number—is completely outdated. Once this secret source that identifies us is revealed, there's no way to replace it.

I believe that, to interact properly on the Internet, we now need a digital identity system. I think that this system should be outsourced, in multiple parts, perhaps even in open source software, to ensure that it includes three key components.

First, if a government chooses to provide verifiable information, it must be able to do so. However, other verifiable sources must also be available online.

Second, I'd like the individual to be responsible for collecting this verified information and for choosing whether to submit it. I'll address this concept of choice a little later in my presentation.

Third, we need an identifiable and fully functional system that will make it possible to confirm ownership or a claim that someone could make, so that, ultimately, a minimal response can be provided to formal questions. The word “minimal” is very useful—

● (1705)

[*English*]

Mr. Brian Masse (Windsor West, NDP): I have a point of order, Madam Chair.

The Chair: Yes, MP Masse.

Mr. Brian Masse: I'm getting both translations at once. I'm on the English channel, as normal, so it could just be me.

The Chair: Thank you. We'll double-check that.

Ms. Fay Arjomandi (Founder, President and Chief Executive Officer, Mimik): It's the same for me.

The Chair: Okay. Thank you. We'll check that.

[*Translation*]

Mr. Perron, I stopped the clock.

Mr. François Perron: Okay. I just chose French as the language spoken. I think that the issue was related to this. Sorry about that. Let me know when I can start again.

The Chair: I think that this was indeed the issue. Thank you. You can continue.

Mr. François Perron: I had reached the third part. I was saying that it could be very useful to have the ability to provide responses with a minimal amount of information and that the individual would be responsible for choosing which information to submit during a transaction. This would be a paradigm shift towards a new system. Instead of having a single secret, such as the social insurance number or a fixed digital identity, we could enter into several contracts with several people. This would make it possible to share information.

This would also enable us to share information by choosing what we want to disclose. Perhaps we could also avoid making our identity known in this context by providing an authentication token that would make it possible to remain completely anonymous.

If we consider this type of system—and this is my second strong impression—we'll also need to look at biometrics. We'll need to have sources of biometrics that we won't be required to fully disclose and to maintain the ability to regenerate other biometric information about ourselves. We'll need to have a biometric data reserve so that we can create new secrets of our own to prevent a complete theft of our biometric identity.

My third strong impression is that personal information and the protection of that information is a matter of sovereignty, citizenship and autonomy. Individuals must understand the significance and value of their own data and their privacy. We likely have some work to do in this area.

Businesses must follow suit. As we find the right rules to regulate the sharing of information, we can improve the situation. Some countries have started to do this. For example, in Europe, the general data protection regulation, or GDPR, sets out stiff penalties. If we don't deal with this, people will move here hoping to take advantage of laws that may be less stringent. We have some work to do to make the rink good for everyone.

In conclusion, I just want to tell you what role I think that the government should play. It must manage its own rink. People will play hockey if they want to play hockey. However, on the privacy rink, we must have the right to be forgotten. Businesses must be required to disclose incidents in which information has been compromised. We must work together to create an ecosystem where our digital identity can be monitored by the individual.

● (1710)

The Chair: Thank you.

[*English*]

Our next witness is Mr. McKay from Google Canada.

You have seven minutes. Just to remind you, when you see the yellow card, you still have 30 seconds.

Mr. Colin McKay (Head, Government Affairs and Public Policy, Google Canada): Thank you, Madam Chair.

It's a pleasure to be with you in such unusual circumstances. It looks like you've started to adjust, but this is my first experience like this, so please forgive any interruptions.

I want to thank you for the time to speak about Google's efforts to help our users and communities during this time of crisis. Since the first appearance of COVID-19, we've been through an exceptional transition at Google. Teams across the company have launched 200 new products, features and initiatives in response to the crisis and needs of our users and our communities. We have made $1 billion in grants and additional resources available to users, communities and countries to help them through this crisis, through the transition.

Our major efforts are focused around keeping people informed with trusted information, supporting them as they adapt to a changing world, and making our contribution to recovery efforts across the globe. Early on, we took steps to make sure that, when users searched for information related to COVID-19, they would immediately see guidance from the authoritative sources, such as the Public Health Agency of Canada, and information about symptoms, prevention and treatments.

On YouTube, we began showing users information panels about COVID-19 when they search for information about the outbreak. This is on desktop, on mobile and on the YouTube home page under any video related to COVID-19. Basically, you get bombarded by these information panels when you're using the YouTube service. We've delivered more than 20 billion impressions of these panels to date.

In a short time, we've all had to change how we live our lives. Google quickly recognized that we can provide resources to help small businesses, parents and teachers adapt. We've collected these at google.ca/covid19. I think every one of us here today is trying to adapt in some way, so that's a useful resource.

Educators and parents face the challenge of teaching remotely at an unprecedented scale. Over 90% of the world's student population has faced some sort of school closure. To help teachers, we created Teach from Home, a central hub of information, tips, training and tools. One hundred million students and educators are now using our Google Classroom product. This is double the number from the beginning of March. For parents, we launched Learn at Home, an enhanced YouTube learning hub to complement family learning with additional content and activities.

For employers and employees, we've consolidated tools and resources under our Grow with Google banner, trying to help them stay connected and productive, including smoothing the transition to remote work.

As the world tries to maintain relationships in a period of isolation, we've made Meet, our video conferencing product, free for everyone. We are seeing roughly three million new Meet users a day, with employees now working from home, students in virtual classrooms, and people looking to connect with friends and family.

We know that people everywhere are looking for a sense of culture and community. On YouTube, we launched the Stay Home #WithMe campaign, working with over 700 creators around the world to urge their combined two billion subscribers to stay home and connect virtually with videos like Bake with Me, Work Out with Me, and Jam with Me.

We're also supporting cultural moments here in Canada such as National Canadian Film Day, featuring Canadian films on YouTube; our Pray With Me initiative, enabling religious organizations like the Archdiocese of Toronto to livestream their services; and a virtual exhibit in partnership with the McMichael gallery to celebrate the 100th anniversary of the formation of the Group of Seven.

In this committee's previous meetings, you've commented on our launch of a new product, community mobility reports. We developed this report to provide insights into population movements that are relevant to public health needs, similar to the way we show popular restaurant times and traffic patterns in Google Maps. These help authorities see in aggregate how social distancing requirements are working in regions across Canada. They adhere to stringent privacy protections; the data does not reveal individual movement or visits to specific establishments. It's based on aggregated, anonymized, opt-in location history data. While the information in this report is not meant to provide a complete picture of the spread of COVID-19, it does provide information that can help public health officials respond to the crisis.

I also note that this committee has discussed contact tracing. Since COVID-19 can be transmitted through close proximity to affected individuals, public health organizations have identified contact tracing as a valuable tool to help contain its spread. To help in this effort, Apple and Google are in the process of launching an exposure notification solution that includes application programming interfaces and operating system-level technology to help public health authorities in enabling a contact tracing program.

● (1715)

This joint effort will enable the use of low-power Bluetooth technology on mobile devices, both Android and iOS, to help the authorities reduce the spread. Just yesterday, we announced the release of this exposure notification API. We're providing a tool that enables public health authorities to build their own apps in a way that is both privacy-preserving and working reliably across both operating systems.

Here in Canada, all of us are only just beginning to explore how we are going to reopen our communities and re-establish ways of working and living within those communities. At Google, we know that small businesses are the backbone of our economy. We've committed funds and resources to helping these businesses, which are our customers, our partners and our users, to weather the storm created by COVID-19.

As we are all isolated and have fundamentally changed our buying habits, businesses were forced to react and adapt. At Google, we made changes to our Google Maps and Google My Business products to help them communicate more clearly to their customers and their neighbours. We are collaborating with small business networks to work together to create and provide tools to speed this transition for SMBs. We've partnered with Digital Main Street and the City of Toronto's ShopHERE program so that independent businesses can build a free digital presence, enabling them to overcome challenges as they try to react to the ever-evolving marketplace.

We at Google feel that our greatest contribution to this crisis can be through empowering others, whether they are the teachers and the small businesses keeping the wheels of society turning, researchers and public health experts, or creators who are keeping people connected and entertained. We know that this work is far from over, and we're committed to continuing to provide helpful products and useful support as we navigate this crisis together.

I have to underline that since the beginning of this outbreak we've turned our attention and our teams to creating tools and services, and revising our existing tools and services, to support the breadth of our community.

Thank you very much, Madam Chair.

The Chair: Thank you very much, Mr. McKay.

Our next witness is Mr. Johnson, from IBM Canada.

You have seven minutes.

Mr. Eric Johnson (Partner, British Columbia Public Sector, Global Business Services, IBM Canada): Thank you, Madam Chair and members of the committee.

Hello, and thank you for the opportunity to speak about IBM and the Canadian response to the COVID-19 pandemic.

My name is Eric Johnson, and I am speaking to you today from Vancouver, British Columbia. I am a partner with IBM Canada, supporting public sector clients for over 30 years. For the last 10 of those years, I have focused primarily on public health and disease surveillance. I am also part of the IBM global COVID-19 task force.

IBM is a global leader in business transformation, serving clients in more than 170 countries around the world. Here in Canada, we are headquartered in Markham, Ontario. Our history of a hundred-plus years in Canada and our unique approach to collaboration provide small and large businesses, start-ups and developers with the business strategies and computing tools they need to innovate and keep the Canadian economy competitive. We are guided by principles of trust and transparency in technology to create a more inclusive society.

During the pandemic, our priority has been, and will continue to be, protecting the health and safety of IBM employees and our clients. At present, we have about 90% of our global workforce working from home, without any interruption in our ability to support clients worldwide. Now we are thinking and planning carefully for a phased return to the workplace, taking into account local health and government directives and conditions, employee roles, the availability of testing and tracing, employee sentiment and more. We have developed a data-driven, evidence-based global return-to-workplace guidance, which lays out a set of principles being used to serve IBM and our clients.

Since the start of the pandemic, we've been working closely with governments around the world to find all available options to put our technology and expertise to work to help organizations be resilient and adapt to the consequences of the pandemic, and to accelerate the process of discovery and enable the scientific and medical community to develop treatments and ultimately a cure.

In addition to the many efforts that IBM and IBMers are leading across the country to support our communities, today I want to stress three key areas in which we're exploring the use of our technology and our expertise to drive meaningful progress in this global fight.

The first is putting technology in the hands of first responders. Annually, IBM puts out a call to developers around the world to build solutions that address some of the most pressing issues of our time. This year, we encouraged developers around the world to put forth solutions that would fight against COVID-19 and climate change. This is perhaps the largest software developer effort in history, and we have dozens of IBM technical experts donating open source code and access to Watson on the IBM cloud.

The second is solutions focused on business resiliency and trusted data. Our cloud-based resiliency and business continuity solutions have supported businesses to implement digital capabilities by providing mobility tools and infrastructure that resulted in seamless transitions of our clients' workforce towards working from home.

IBM and the Weather Company created a new and precise incident map, driving unprecedented hyperlocal understanding of the outbreak with health data from trusted sources, and it's updated every 15 minutes on the IBM cloud.

IBM Watson Assistant for citizens was created for local and regional governments and health agencies, and it brings together years of investments in AI and speech recognition to create chatbots that can help guide citizens in a dynamic situation and free up important resources. This tool is currently being used by a number of organizations around the world, including the City of Markham in Ontario.

The IBM solution for disease surveillance is implemented in seven Canadian provinces and one territory. It provides a unified data model managing immunization data, vaccine inventory data and, for some provinces, outbreak management. We're currently focused on the provincial health requirements, with the goal to help integrate the multiple data sources coming from contact tracing and lab results into the existing provincial public health databases so that the data may be used by our clients as a single source of truth for analysis, reporting and predictive modelling. In addition, we are already helping provinces prepare for the upcoming mass immunization events that will need to take place once a vaccine is developed.

Finally, we're leading the way to a cure with supercomputers. In collaboration with the White House Office of Science and Technology Policy and the U.S. Department of Energy, IBM helped launch the COVID-19 high-performance computing consortium. These high-performance computing systems allow researchers to run very large numbers of calculations in epidemiology, bioinformatics and molecular modelling. These experiments would take years to complete if worked by traditional computing platforms. Since the consortium was announced, on March 22, we have received 55 research proposals from the U.S., Germany, India, South Africa, Saudi Arabia, the United Kingdom, Spain and Croatia.

● (1720)

Those are just a few of the initiatives we have launched. IBM is also supporting Canada's faculty, students and families across academia by offering tools and resources to meet this new reality in real time. IBM has extended its online education resources to all for free, including IBM Skills, Open P-TECH, and the IBM AI Education series for teachers.

Now the focus is towards rebuilding and relaunching. There is emphasis on cybersecurity, expanded emergency operations management, social programs and technology that will support the focus on the mental well-being of Canadians.

There is no question that this pandemic is a powerful force of disruption and an unprecedented tragedy, but it is also a critical turning point. It's an opportunity to see what we're all capable of and how we emerge stronger.

Thank you.

The Chair: Thank you very much, Mr. Johnson.

Our next presenter is Madame Arjomandi.

You have seven minutes.

Ms. Fay Arjomandi: Thank you, Madam Chair and esteemed members of the committee.

My name is Fay Arjomandi, and I also have Michel Burger, our CTO, on the call. I'm the co-founder, president and CEO of Mimik, a software company based in Vancouver, British Columbia. For the past 10 years, Mimik has been pioneering the development of hybrid edge cloud computing, a technology that adds cloud capability to devices and apps to increase data privacy, reduce infrastructure costs and radically improve real-time interactions. It's eco-friendly and provides access to rural communities. Mimik's technology is already empowering some innovative companies in health tech, fintech, AI, smart cars and smart cities.

I'm grateful for the opportunity to speak to you as a fellow citizen, entrepreneur and technologist. Our platform is already being evaluated by large enterprises as part of a "going back to the workplace" solution and gaining traction from some of the indigenous communities, but we believe that with your support it can be used across Canada and globally for contact tracing.

COVID-19 has caused the loss of many Canadian lives and is impacting our economy and the livelihood of our citizens. It has attacked our way of life. Contact tracing is essential to implementing intelligent social distancing to send our citizens back to work safely and revive our economy. However, it evokes fears of surveillance, privacy abuse and stigmatization, and rightfully so, because solutions implemented by other countries are exactly that. One could say that such solutions will be another attack on our way of life.

Mimik's platform can be used to implement effective contact tracing without compromising citizens' privacy or patients' anonymity, and at the same time avoid many pitfalls along the way.

There are three important aspects to an effective contact tracing implementation.

● (1725)

The Chair: Ms. Arjomandi, please move the microphone back just a bit. It's too close for the interpretation.

Thank you.

Ms. Fay Arjomandi: The first is about ensuring adoption. Adoption is poor if citizens have concerns that their personal data, however limited, is being held centrally by any external entity or that third parties can track their location and access their contact history. Countries such as South Korea and Singapore have resorted to force to ensure compliance. This is unthinkable in Canada.

With our platform, each edge or client device, such as a smart phone, acts as its own server system capable of receiving, storing and sending information. The system detects exposure by combining several technologies, including network address and Bluetooth proximity. This exposure log is recorded, calculated and processed locally on each device, eliminating the need to send this information to a central system. All devices remain anonymous and the only source of data, putting citizens in complete control of their data.

The second is about anonymity in action. Some of the better attempts with contact-tracing apps preserve anonymity until a positive case is identified. However, as soon as a user tests positive, the entire contact log from the user can be accessed by a central authority. The core issue here is not about the data of the user who tested positive, but rather the violation of the privacy of everyone else who was in contact with the user. By contrast, our platform can verify a valid positive test ID and then use a token to send out alerts to the exposure log anonymously, directly from a user's device.

The third and perhaps most critical aspect is that any contact-tracing solution needs to be adaptable. This means avoiding points of failure. We see several major issues with current attempts at contact tracing. I'll list a few.

One, many apps require users to register with a central health authority to get started. This not only creates privacy issues but also complexity, as users in proximity might not be registered with the same health authority.

Two, some approaches require adding COVID-19-specific features into device operating systems. This is unnecessary, plus it adds the additional pain of dismantling. Citizens may be concerned that once a function gets implanted in my phone and theirs, it will not go away, which may inhibit adoption.

Three, apps that save tracing logs on a central system need to connect with that system frequently to poll information. This creates a heavy load on the network, causing all sorts of issues.

I'll conclude by saying that hybrid edge cloud computing was developed for data exchange and transactions in a private manner with the ability for central oversight to curtail any abuse of our communications systems by bad actors. This solution can work seamlessly across health authorities, technologies and networks. Most importantly, by eliminating the need for sending or saving contact-tracing history on central systems, we can protect citizens' privacy, avoid network loads and implement a truly scalable solution across Canada in the health sector and others.

As I have mentioned today, adoption, anonymity and adaptability are the three important As of contact tracing. Every citizen deserves a solution with this triple A rating.

Thank you. I will be happy to answer any questions.

● (1730)

The Chair: Thank you very much.

We'll now move into our round of questions. Our first round of six-minute questions will start with MP Dreeshen.

You have the floor.

Mr. Earl Dreeshen (Red Deer—Mountain View, CPC): Thank you very much, Madam Chair.

In Canada, we're facing a major dilemma. We have advocated for putting our frailest seniors in solitary confinement, with inadequate care and no visitors. Truly it's a mixed-up society.

We have blindly followed new, disproved advice from our health ministry, and we're ready to convince ourselves that the government's knowing our daily whereabouts is a good thing. My niece had to hear about her husband's death through a long-term care centre's window. This is in a community where you'd be hard-pressed to find a single COVID case. Whatever we've done so far is cruel and unusual punishment.

When I look at the many concerns, I think one of them has to do with jurisdiction. The last thing Canadians want is a one-size-fits-all approach imposed on them by some Big Brother central government.

I know that health care is a provincial responsibility. The approach to treating high-density urban populations is completely different from the approach to treating rural populations. If provinces have something that works for them, should we not be letting them proceed with that, rather than relying on some faceless national entity telling them what to do? That is my concern. Provinces should do what they want to do. However, the biggest fear is that the federal government might want to take this over.

Google, you have had opportunities to deal with major players throughout the world. What would your comments be in this regard?

Mr. Colin McKay: We are making the tools available so that all levels of government can make decisions appropriate to their needs and their priorities. The community mobility reports are designed to give that information at as granular a level as we can at the moment. It's the same thing with the exposure notification API. That's designed for any public health authority that wants to build a contact-tracing solution and wants to have the best possible use of the Bluetooth location technology on an Android phone or an iOS phone.

I don't really have an opinion about the different executions at any level of government, just that we're conscious that we're trying to provide the technological solutions to support public health authorities as they try to find the right path forward.

Mr. Earl Dreeshen: Thank you, Colin.

Like many Canadians, I think the use of contact-tracing technology could well lead us down a slippery slope. I think that is what the folks from Mimik were talking about. In several places where these applications have been developed, there's nothing to indicate how long the applications will be around for, how long any information collected from them will be used or who around the world will be able to use it.

Mimik, I understand you've developed an application that's supposed to address the privacy issue. You've spoken of that. Canada's Privacy Commissioner recently issued a joint statement with regard to contact-tracing applications, and I'll highlight the points it made. It said, “Government should be clear about the basis and the terms applicable to exceptional measures. Canadians should be fully informed about the information to be collected, how it will be used, who will have access to it, where it will be stored, how it will be securely retained and when it will be destroyed.”

Are you aware of any government anywhere in the world that has embraced the principles that Canada's Privacy Commissioner has mentioned? Also, I'm concerned about what happens if there's a breach of one of these applications. Who would be responsible?

Mimik, go ahead.

● (1735)

Ms. Fay Arjomandi: We believe that the best approach is for me, as the end-user, to have control over my data. I should choose whom to share it with, how to share it and also whether the person who uses that data has the right to copy that data. We believe there should be a policy to impose a fine or other measures on anyone who breaches the data right that consumers are demanding. That's what we're enabling with hybrid edge cloud. The information should stay safe on devices, and a key that the user has can provide permission for any application to use it.

Mr. Earl Dreeshen: At the end of April, a privacy expert and fellow at the Berkman Klein Center for Internet and Society at Harvard University told the media that his problem with contact-tracing applications was that "they have absolutely no value". Putting privacy aside, these applications don't accomplish what they've set out to do, from their perspective. Why then should Canadians be putting their privacy at risk if this is unproven technology that may not accomplish as much as people are saying?

Perhaps Eric from IBM could take a run at that.

Mr. Eric Johnson: When he says contact tracing, I'm assuming it's proximity tracing that we're talking about, what Mimik was talking about. I think the position we've taken is that it's very much a consent model, much to what Fay said. You as the end-user should have the decision on your data and on whether you opt in or opt out.

Mr. Earl Dreeshen: Thank you very much.

The Chair: Thank you very much.

Our next round of questions goes to MP Lambropoulos.

You have six minutes.

Ms. Emmanuella Lambropoulos (Saint-Laurent, Lib.): Thank you, Madam Chair.

Thank you to all our witnesses for being here with us to answer our questions.

My first question is for Google Canada. Obviously, protecting Canadians and the privacy of Canadians should be the priority. In a statement that you, alongside Apple, issued earlier this month, you did mention that there are strict guidelines in order to protect the privacy of Canadians. Can you please go into detail about what has been put in place in order to protect the privacy of Canadians?

Mr. Colin McKay: I think that a lot of what I'm about to say will echo what Madame Arjomandi just said.

When we're talking specifically about the exposure notification API, there is on-device collection of information that is not shared without the consent of the user. They first have to take the step to download an app and then give permission for that information to be collected. Importantly, the information that is collected about their location is actually anonymized and randomized. It's not associated with the individual or the device. Rather, it is a reference point for public health authorities if there happens to be a person who has been notified that they're positive for COVID-19. Throughout the process, we're taking specific steps to provide information about the proximity contact of individuals without actually sharing the personal information of those individuals or creating a long-term record about either their travels or their location.

I'd also like to follow up by underlining that we've made an explicit commitment with both the exposure notification API and the community mobility reports to shut those programs down once public health authorities have signalled that the current crisis is under control. Now, it's up to the public health authorities—I don't think we have a definite timeline on that—but we have made that commitment to alleviate any concerns about this being a long-standing complication on your device.

Ms. Emmanuella Lambropoulos: Thank you very much.

From what I understand, there are two phases. Phase one began in May, possibly yesterday, I guess. The application is now available for Canadians to download. It seems that phase two will be more broadly used a few months from now. Can you explain the difference between the two phases and how this may compromise, in some way, the privacy of Canadians?

● (1740)

Mr. Colin McKay: Really, it's a technological progression. The reality that exists right now is that we need an application programming interface so the public health authorities can develop the apps that allow them to build that relationship with the user and request that they allow tracking through Bluetooth.

As a second phase, we're pushing out modifications and improvements to the operating systems on the device itself, so that much of that work is being conducted through the operating system. It's a technological improvement rather than an expansion of the program or its capacities.

Ms. Emmanuella Lambropoulos: Thank you very much.

Do we know if contact tracing has been used before to track diseases and to ensure low infection rates? Do we think this is a good way forward that would actually help slow the progression of this disease?

Google or IBM, I guess, has this ever been used in the past?

Mr. Colin McKay: Speaking from my point of view as a one-time history student, it has been used in the past. I can't give you any judgment on whether or not it's effective and how we contain the virus.

What I'll state is that we, at Google, are certainly an environment where we're recognizing that we need to modify our services and provide tools to public health authorities so that they can explore options. We are recognizing the opportunity and then trying to react to it in a constructive way, while recognizing our obligations to the users.

Ms. Emmanuella Lambropoulos: Thank you very much.

I know that it depends on what the health authorities ask for, and we're trying to protect Canadians as much as possible, but what specific information will these apps allow us to gather?

Mr. Colin McKay: If that's directed to me, I can't speak to the specific apps. What I can speak to is that at Google, what we'll be exchanging is anonymous Bluetooth beacon information that enables the apps to identify and then notify individuals who have been in proximity to each other. As for the apps themselves, it will be up to the public health authorities to decide what sort of information they are going to request from users.

I will note, however, that we've made it a specific requirement of using our exposure notification API that app developers cannot request personal information; they can't associate it with the Bluetooth information. They also cannot request specific location information from the device alongside the exposure notification API.

What that means in practice is that there could be an app that only interacts with the API, then a separate app that does a lot more on behalf of the public health authority. That would be separate from Google services.

Ms. Emmanuella Lambropoulos: The Privacy Commissioner of Canada requested, along with its list of requests, that the app be decommissioned once this crisis is over. Do we know of any plans to do so once the crisis is over?

Mr. Colin McKay: As far as I know, there aren't any apps deployed with the exposure notification API. We're certainly in contact with public health authorities about this. That's something for the app developer to discuss with the privacy commissioner in their jurisdiction.

Ms. Emmanuella Lambropoulos: Thank you very much.

[*Translation*]

The Chair: Mr. Lemire, you have the floor for six minutes.

Mr. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Thank you, Madam Chair.

My question is for Mr. Perron.

How safe can we feel with our telephone? Can we assume that we're under constant electronic surveillance? Is that a myth or a reality?

Mr. François Perron: Yes. We have some very clear evidence that the telephone can keep a record of conversations and geographic locations. There are also acceleration sensors, which make it possible to better understand what the person is doing. Increasingly, algorithms help identify an action verb associated with what the person is doing.

A telephone can undoubtedly be used to do what you've just described.

● (1745)

Mr. Sébastien Lemire: This week, Radio-Canada published an article stating that Facebook had to pay $9 million for making misleading claims regarding confidentiality. The article quotes Matthew Boswell, the commissioner of competition:

> The Competition Bureau will not hesitate to crack down on any business that makes false or misleading claims to Canadians about how they use personal data, whether they are multinational corporations like Facebook or smaller companies.

Is the current legislation stringent enough for companies?

Mr. François Perron: Again, I must put my response in context.

I'm much more familiar with the part of Quebec's legislation that applies to software used in the health care sector. In this context, the matter involves the use of personal information by public agencies. In these cases, clearly, we must obtain explicit consent for each use or purpose of the personal information provided.

In Quebec, the health legislation is stringent. However, in the private sector, it's a different story.

Mr. Sébastien Lemire: As you said, we can't assume that users will be thoughtful in terms of their own protection. You spoke of a combination of measures. I seem to recall that you spoke of an "ecosystem" earlier. Can this ecosystem help us develop free and informed consent that applies to a specific context, such as the COVID-19 context, of course?

Mr. François Perron: This ecosystem will be spontaneous. We'll see a growing concern. Your question can have two parts. First, the public will take an interest in the issue and will start asking questions. The players in the ecosystem can explain the ins and outs. What issues are being raised and what can we do to protect ourselves? Second, it will depend on how the ecosystem is structured and on how well the ecosystem meets the standards in place. The question touches on very clear concepts of public education and information.

Mr. Sébastien Lemire: In response to COVID-19, a company by the name of Mila has taken an interest in developing a location tracking app that uses Bluetooth.

In a situation where the greater good, in other words, public protection, is at stake, how can we make sure that someone who tests positive isn't automatically recorded in the system if they aren't a consenting user?

Mr. François Perron: That's a very specific question, one that raises the question of second-class citizens. All of a sudden, extra information about these people is available.

Obviously, if a company puts out an app for the public that is deemed to contain people's personal and health information, the technology will be governed by clear legislation, in Quebec's case. Options include asking users for their express consent or ensuring information owners are always the ones deciding who the information goes to and have the ability to withdraw their consent and recover their information. I'm much less familiar with how the law applies in the private realm. On the public side, an app deemed to contain personal information goes through phases of certification. Watchdogs ensure the app is compliant.

Again, the information will have to be categorized to determine whether it constitutes personal information or health information, which isn't at all clear right now. That's one of the questions that will have to be answered in order to classify the app.

Mr. Sébastien Lemire: Canada's federal and provincial privacy commissioners got together and issued a joint statement on May 7. In it, they say, “The choices that our governments make today about how to achieve both public health protection and respect for our fundamental Canadian values, including the right to privacy, will shape the future of our country.”

Is it therefore conceivable that the decisions we make today, even the most minor initiatives, could become permanent?

● (1750)

The Chair: Please keep your answer brief.

Mr. François Perron: In a nutshell, the answer is yes. Everything is moving at a breakneck pace right now. We're communicating by video conference, so where do the data collected by the video conferencing system go? Is anyone making sure that the data stay in Canada?

Questions abound, but we're moving so fast that it's impossible to have all the answers. It's a slippery slope, and problems could arise. I wholeheartedly believe that.

Mr. Sébastien Lemire: Thank you, Mr. Perron.

Mr. François Perron: Thank you.

The Chair: Thank you very much.

[*English*]

Our next round of questions goes to MP Masse.

You have six minutes.

Mr. Brian Masse: Thank you, Madam Chair.

I'll have a question for every witness. There will be a part (a) and a part (b). I'll set it up and then go through the list so that they can answer appropriately.

Back in March 2018, I tabled Canada's first digital bill of rights. It was an attempt to start the process and a discussion on a more formalized updating of our regulations, laws and agencies, with an overall feeling, I guess, that Canadians would be confident that their digital rights would be respected, similar to their physical rights. It was about empowerment and, as well, controls and issues such as net neutrality. There was a series of different things, but the most important is to have a predictable pattern, I guess, so that businesses, not-for-profits, governments and also other institutions from around the world will understand that Canadians are protected in a very specific and very tangible way, empowered by law.

We've seen a number of different issues come up with this COVID response, with everything being discussed, and now, even tracing. Last night, we had interesting testimony with regard to fraud, which was very important. This is part of the question.

I look at some of the issues and at the Competition Bureau, for example, when we talk about online information. They just fined Facebook for $9 million—it's $5 billion in the United States—for misleading Canadians in using third party applicants and allowing private information to be dispersed. The Competition Bureau here is only at a $9-million fine versus $5 billion.

The Privacy Commissioner has already said specifically that they need more resources and money with regard to doing their job in terms of the challenges they face. Look at the CRTC. Even before now, it has taken ages to get an answer or a decision and, also, enforcement on public policy issues related to Internet use, service rates and expansion.

My questions for the guests are: (a) Do you accept, support or reject a digital bill of rights that could be brought forth in some capacity, with everybody involved, to finalize a position and to have at least an understandable sound grounding of what that means for each person and also for the responsibilities of companies? (b) Do government agencies and does the respective legislation need modernization or updating? You don't have to get into the specifics of that, but I'd like to hear about those things.

I'll start with the order of presentation, so perhaps we can start first with CyberQuébec. First, do you accept, reject or support a digital bill of rights? Second, what is your position on whether government agencies need modernization, or are they capable right now?

[*Translation*]

Mr. François Perron: It's hard to give a clear and comprehensive answer. There's no doubt in my mind that the current legislation is incomplete. I alluded to that earlier when I said I wasn't very familiar with the private protection regime. I'm much more familiar with the public protection regime, seeing as I work in certification on the public side.

The legislation needs more teeth. That's my personal opinion. I pay attention to what Europe, in particular, is doing. There, the General Data Protection Regulation is in place. Under the regulation, companies that fail to report privacy breaches involving personal information are fined. I would say it's important to move in that direction.

I missed the nuances of the second part of your question. As I said earlier, the current legislation needs to be strengthened so it has more teeth.

[*English*]

Mr. Brian Masse: That's great. Thank you, Mr. Perron.

Next is Google.

Mr. McKay.

Mr. Colin McKay: Thank you for the question.

Yes, I think I remember your bill and when you tabled it. There are many elements that are complementary to the conversation we've been having, up until this crisis, around reforming Canada's data protection laws.

I want to underline that there's certainly a conversation that we had around PIPEDA, but also around the Privacy Act, especially in the context of the conversation we're having today in regard to modernizing and recognizing, as many of witnesses have reinforced, the need for explicit consent from users, and then, in defined circumstances, for the use and then withdrawal of data that has been shared. So I think my answer to you is yes, and I think we've seen some of those paths begin.

On my answer to your second question, as we can see from the Competition Bureau's decision, there are specific roles, responsibilities and penalties that already exist within our system. You hinted in your question they may not work at the speed and the breadth that some of us may want. Google certainly is working globally around levelling the playing field on data protection, as well as consumer protection, and we're a participant in those conversations. There's certainly space to grow in Canada.

● (1755)

Mr. Brian Masse: Okay, thank you.

Next is Mr. Johnson from IBM.

Mr. Eric Johnson: I would echo Colin's comments. We would obviously support the modernization of it. It's all about trust and transparency, and that's what we have to build. We've seen it in Europe, like you mentioned, with the GDPR. We're supportive of going down that path.

Mr. Brian Masse: Thank you.

Next is Madam Arjomandi, from Mimik.

Ms. Fay Arjomandi: Absolutely we support it. In fact, in 2017, we published a digital manifesto about personal data, and a few months ago, we published consumer analytics for data robbery, because we believe that data belongs to us. In fact, it should be treated as a form of income for us versus just generating income for others.

Also, we believe that we're facing not only data privacy but data piracy, and consent is not enough. We need to be engaged with our data and give permission for use of our data every—

The Chair: Thank you very much, Madam Arjomandi. Sorry, but that's all the time we have for that round.

The next round of questions goes to MP Rempel Garner.

You have the floor for five minutes.

Hon. Michelle Rempel Garner (Calgary Nose Hill, CPC): Thank you, Madam Chair.

My questions are for Mr. McKay.

I'm looking at YouTube's community guidelines related to the COVID-19 medical misinformation policy. It says that YouTube doesn't allow content that spreads medical misinformation or contradicts the advice of the World Health Organization or local health authorities. Does this mean that Google and YouTube are now taking responsibility as a platform for determining truth about public health information during a pandemic?

Mr. Colin McKay: No, we're looking to public health authorities, who have the experience and the expertise to provide guidance on what they consider authoritative information.

Hon. Michelle Rempel Garner: If you're not looking to take responsibility, then why do it?

Mr. Colin McKay: Sorry. Do you mean why apply the guidelines and battle misinformation on YouTube?

Hon. Michelle Rempel Garner: Yes. I guess I would contextualize the question.

In January, the World Health Organization said there was no evidence of human-to-human transmission of the coronavirus. Would YouTube have removed a video questioning that at that point in time under this policy?

Mr. Colin McKay: I'm sorry. I can't speak to possibilities. I can only speak to the practical experience we've had.

Hon. Michelle Rempel Garner: Sure.

In that practical experience, would that community guideline have applied to videos or users talking about using masks to prevent the transmission of COVID-19 when the WHO was quiet on that issue?

Mr. Colin McKay: The policy itself is applied to instances where there's an explicit threat to personal safety or health and where there's the possibility of personal injury. In the case that you're describing on the use or non-use of masks, we would still turn to the WHO and public health authorities to give us guidance.

Hon. Michelle Rempel Garner: I'm reading directly from the policy, and it says the policy would remove:

> content that contradicts WHO or local health authorities' guidance on:
>
> - Treatment
>
> - Prevention
>
> - Diagnostic [and]
>
> - Transmission

So I think it's a little broader than that.

Would this policy have applied to, let's say, someone who posted a video saying that border security measures do work when the WHO was saying that they don't work?

● (1800)

Mr. Colin McKay: We try to apply the policy as broadly and effectively as possible. The reality is that we're facing circumstances from day to day where we're dealing with misinformation on a much more significant scale. What you're describing here would sound in our conversation as something that would need to be deliberated, but at the time—

Hon. Michelle Rempel Garner: Just as legislators.... I'm just wondering if this opens your company up to legal responsibility for determining what is the truth in a pandemic situation. I'm just curious why you're taking this position as opposed to just acting as a platform.

Mr. Colin McKay: We are acting as a platform, but we're looking to informed sources to give us the information so that we can ensure that authoritative information is going to our users. We also take steps—

Hon. Michelle Rempel Garner: What about in a situation where the "informed source" is wrong, as the WHO has been?

Mr. Colin McKay: I think one of the advantages of our platform is that there is ongoing debate and opposing points of view in the content that is made available by our users.

Hon. Michelle Rempel Garner: But your platform community guidelines say it would remove content that would have an opposing viewpoint to the WHO.

Mr. Colin McKay: I think in practice, when we're dealing with issues of particular notoriety and severity, we're acting quickly and we're following those guidelines.

Hon. Michelle Rempel Garner: Again, there seems to be some ambiguity here on the purpose of this policy. Would you say that it's less about misinformation and more about perhaps upholding existing political dogma on a certain topic?

Mr. Colin McKay: No. I would say it's wholly about providing authoritative and reliable information to the user.

Hon. Michelle Rempel Garner: I'm curious. If I post this clip to my YouTube channel, will it meet community guidelines?

Mr. Colin McKay: Sorry, I don't see how it wouldn't. It's being broadcast right now, and we're having a straightforward conversation with an obvious difference of opinion.

Hon. Michelle Rempel Garner: Thanks. I'll end my comments there.

The Chair: Thank you very much.

Our next round of questions goes to MP Ehsassi.

You have five minutes.

Mr. Ali Ehsassi (Willowdale, Lib.): Thank you very much, Madam Chair.

Thank you very much to each one of the witnesses.

I've found today's testimony incredibly helpful. I say that because there's been a flurry of activity in different jurisdictions and contact tracing is obviously of great interest. However, to step back from the technical details, I want to ask each of you a very short question.

For contact tracing to work, in each one of your estimations, what percentage of the population of a jurisdiction has to participate or has to be part of that process? Could you provide me with numbers?

Mr. Perron.

Mr. François Perron: I have not researched this question, so I will defer comment.

Mr. Ali Ehsassi: You have no estimates.

Mr. François Perron: No.

Mr. Ali Ehsassi: No, okay.

Mr. McKay.

Mr. Colin McKay: I'm afraid I don't have an estimate for you.

Mr. Ali Ehsassi: Nothing? No rough estimate?

Mr. Colin McKay: No.

However, I'll say that the reason Apple and Google are working together is a recognition that we need collaboration across platforms so there is the greatest possibility for public health authorities to make that option available to our users.

Mr. Ali Ehsassi: Thank you.

Mr. Johnson, roughly what percentage of the population of a jurisdiction has to participate to make it an effective tool?

Mr. Eric Johnson: I can tell you what I'm hearing from other countries and from experts. I can't give a position myself.

The general percentages I'm hearing are that it's between 60% and 80% to get an effective coverage. That, I think, is what seems to be in the public.

Mr. Ali Ehsassi: Thank you, Mr. Johnson.

Ms. Arjomandi.

Ms. Fay Arjomandi: Yes, I've heard the same data. It's about 60% to 70% of the population.

The only way, in my opinion, to get that going is to give trust to users, that they have their own data and they are in control of it. Nothing goes to the cloud to get anonymized post. Everything is basically managed on the edge device, calculated on the edge device, and it's in their control.

That's the whole architecture we've been following, to basically inhibit the data even going to the cloud. Everything is getting processed and calculated on the device, and it's across device, across operating system, across network and cloud.

● (1805)

Mr. Ali Ehsassi: That being said, you were referring to a triple A rating for privacy. I understand that Google had the opportunity to elaborate on what their privacy safeguards were, but we didn't have a chance to hear from you specifically on that issue.

Could you elaborate on what the privacy features are in your app?

Ms. Fay Arjomandi: Again, with the hybrid cloud edge platform, the data resides on the device itself. It gets calculated on the device. We don't send location information to the cloud. We measure proximity on the device level, and we do proximity mapping using hybrid cloud edge. I would know two devices were close to each other, but I wouldn't know who that device belongs to and where the device has been. That's the most important thing. We provide visibility to the end user to decide which data at which point they want to share with which health care provider.

They have the control to say whether the health care provider can copy or keep the data or if they want to only have access to and view that data. These are the only ways that I as a citizen would use an application like this. I would recommend it to my parents, my sibling, my loved ones. Otherwise, I as a technologist would be the first one to avoid using such technology.

Once I have the contact tracing, there should be an action, an incentivization to share some data. Incentivization should not be with advertising, but should be, for instance, for health care services offering something that I receive in care and support in case I get sick that I would now be willing to share some information with the right person and the right point of contact.

Mr. Ali Ehsassi: Thank you.

To step out from the contact tracing issues, Mr. Johnson, as part of the IBM global task force you have a bird's eye view as to what's taking place in various jurisdictions.

Are we as a country doing a good job leveraging our digital infrastructure to be ready not just for COVID but for future pandemics as well?

The Chair: Very quickly.

Mr. Eric Johnson: Very quickly, yes, Canada is doing a great job. It's easy to be critical and it's important to be critical because we can improve very much. We can do more on the cloud. We can do a lot of digitization. A lot of countries are envious of the position we're in and how we've handled it. You can see it in the media from our public health leaders.

The Chair: Thank you very much.

Our next round of questions goes to MP Gray. You have five minutes.

Mrs. Tracy Gray (Kelowna—Lake Country, CPC): Thank you, Madam Chair.

Mr. McKay, since the beginning of the pandemic, Google Canada has been sharing community mobility reports, publicly displaying changes in location trends. For example, in your May 13 report tracking your users' movements, retail and recreation visits are down 38%, transit stations are down 58% and parks are up 48%.

What apps does Google use to track people on these community mobility reports? Is it just Google Maps?

Mr. Colin McKay: The community mobility reports are generated using aggregated and anonymized data from Google users who have opted in to location history. They've explicitly decided to share their location history with us on their mobile device. We've taken that and anonymized and aggregated it, as I said, to identify these five separate geographies or types of behaviour that give us insight and trends that are useful to public health authorities.

What's useful to notice about location history is that you're able to go into your location history and turn it off temporarily or delete it completely or delete areas you visited. You're also able to set an automatic setting that deletes it after a certain period of time.

Mrs. Tracy Gray: Okay. A variety of apps can be used. For example, Google owns YouTube, so if people are keeping their YouTube open while they're out and about, is their mobility being tracked?

Mr. Colin McKay: Those two are not connected. If you're using your phone with location history enabled, that is one function within your phone and YouTube is another.

● (1810)

Mrs. Tracy Gray: Okay.

Did Google Canada notify its users that their data would be used to produce these community mobility reports prior to the information becoming public?

Mr. Colin McKay: We made the decision to both anonymize and aggregate so there isn't any personal information or any identifiable information related to a user. In this case, we didn't make any notifications because it is general trends, and they have analysis over a very broad subset of users.

When you look at the reports, some reports have omissions or complete gaps. That's because there wasn't enough information to do that anonymization accurately and properly.

Mrs. Tracy Gray: Some have criticized Google for their lack of transparency when it comes to consent around location data collection. Wouldn't you agree that notifying users would have helped with this criticism?

Mr. Colin McKay: We took an explicit step in using only the data collected by users that had opted into location history because they had gone through a very specific consent flow on their device that explained both the information being collected, as well as the controls they have over that information on their device. We felt that was the most appropriate constituency of our users from which to draw these insights.

Mrs. Tracy Gray: So those reports aren't necessarily a full representation but a slice or a cross-section of people.

Some of the phones have settings allowing a location only to be shared during the time of using an app, such as with Google Maps. In that scenario, would Google be including an individual's data in their community mobility reports when authorization may only be to track, say, for example, their location when Google Maps is being used?

Mr. Colin McKay: In this case it was when they were opted into the location history, which is a continuing record of their movements that is shared only with Google within very specific conditions. In fact, the setting you've noted is actually one way that we've taken extra steps to give our users the information and the mechanism to signal that they don't in fact want their location tracked except when they're using an app. That one-time use only, when you're using an app only in this instance, is a way for us to provide additional control to the user.

Mrs. Tracy Gray: Okay.

Mr. McKay, do you also share these community mobility reports with governments?

Mr. Colin McKay: We share them inasmuch as we make them public to whoever would like to see them.

Mrs. Tracy Gray: There are the public reports. Would governments receive additional reports other than the ones that you're making public? Would they receive reports that would have more details than the public reports that you're posting?

Mr. Colin McKay: No, they receive exactly the same reports that you can see on the website.

Mrs. Tracy Gray: Okay.

Some have questioned the data accuracy of the location sharing use, pointing out that if locations are tracked through cellphone signal instead of through GPS data, that location could be inaccurate. Would you agree with that assessment?

Mr. Colin McKay: There are certainly levels of granularity associated with what data you're using. We explicitly went with these five regions so that it was a broad category that didn't provide for—

The Chair: Thank you very much.

Our next round of questions goes to MP Erskine-Smith.

You have five minutes.

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

If Conservative MP Ms. Rempel puts up this video, you won't take it down, Mr. McKay. If I went to the corner of Woodbine and Queen and I made a video saying, “Everyone should drink bleach to cure COVID-19”, would you keep that video up?

Mr. Colin McKay: That violates the guidelines and it should come down.

Mr. Nathaniel Erskine-Smith: That seems sensible to me. Some level of science ought to play a role in your decision-making, surely.

Mr. Colin McKay: Yes, that's why we look to public health authorities for guidance and it's also why we have explicit definitions for our guidelines, so that people can interpret them.

Mr. Nathaniel Erskine-Smith: In terms of transparency, if a video is taken down or downgraded in some fashion and it is a more debatable decision—it isn't so obviously objectionable as drinking bleach—what is the appeal process?

Mr. Colin McKay: I think you hinted in your question that there are various levels in which YouTube videos are affected by a violation of our community guidelines. In some cases they're demonetized so you can't make advertising revenue from them. In other cases, they're rendered private so you can continue to share them but they're not surfaced in the search. Finally, there's a takedown. They receive notification by email that there's been a violation of the community guidelines and there's an opportunity to explain why that should be reversed.

Mr. Nathaniel Erskine-Smith: It's fair to say I've given you a hard time in the past, wouldn't you say, Mr. McKay?

● (1815)

Mr. Colin McKay: We've had engaged conversations.

Mr. Nathaniel Erskine-Smith: Let me be the first to then credit YouTube and Google for emphasizing science and not sensationalism when it comes to saving lives.

Mr. Johnson, you indicated you have seen research that a 60% to 80% adoption rate is critical for the efficacy of a proximity tracing application. I've seen the same research. Do you think we can plausibly get there with an app that is opt-in?

Mr. Eric Johnson: That is a really good question.

I can give you my personal perspective. It's just to give you some statistics out of the U.K. In the U.K., 80% of people have a phone. If you have to get to 80%, it's very, very difficult. I'm optimistic because I think the more contact tracing we can do...the openness that's been discussed and the consent.... As long as people are comfortable that they're not being tracked and their data is safe, I think there's hope, but it's a tough road, in my opinion.

Mr. Nathaniel Erskine-Smith: If it is a matter of public health in relation to ensuring we are free from deadly viruses, is it inappropriate to have more mandatory rules?

Mr. Eric Johnson: Is that for me again?

That's a philosophical question. Certainly IBM doesn't have a position. I think we have to look to our health leaders. I can say that in British Columbia we all do what Dr. Bonnie Henry tells us to do. We're in. We're all in.

Mr. Nathaniel Erskine-Smith: Maybe I'll put the same question to Mr. Perron in that case.

Mr. François Perron: Sorry, I have to rearrange the microphone.

[*Translation*]

Are you asking about the percentage of people who use a cell phone and the efficacy of an app? I'm sorry, but I missed that part of the question.

[*English*]

Mr. Nathaniel Erskine-Smith: It's not the percentage. I have a minute left, so let me put it this way.

I don't know what it's like in Quebec, but in Ontario, children are required to have a vaccine for a number of different diseases to attend school. It seems odd that we wouldn't take a similar approach to saving lives in relation to a pandemic for an application on our phones so long as it is privacy preserving in every other possible way. For the DP3T standard except for voluntariness, it would mean having a data governance framework and data would be deleted at the end of this pandemic.

I wonder why, if a vaccine is not voluntary for kids attending school in Ontario, we are talking about voluntariness to such a great degree with respect to an application that could potentially save lives.

[*Translation*]

Mr. François Perron: Again, that's a very intriguing question.

As I see it, the current problem is that making the app mandatory would contravene a number of laws, specifically in relation to consent. Use of an application usually requires people's consent. What you're proposing, however, would require people to share their personal information. That strikes me as very difficult to do in a country like Canada.

In terms of how Quebec law pertains to public organizations, consent poses a problem there as well. As someone who's not a public health expert, I have a much harder time understanding how something like that could work.

The Chair: Thank you very much, Mr. Perron.

Ms. Gaudreau will start off the next round.

Ms. Gaudreau, you have two and a half minutes. Please go ahead.

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Thank you, Madam Chair.

A lot of things need to be considered. I'm pleased with the progress we've made since the last meeting.

We've heard that our data is more or less protected. The Privacy Commissioner of Canada reports that 30 million of 37 million Canadians have been the victims of a data breach. How is that possible?

Do we need to pull back quickly to make sure we, as lawmakers, are protecting the public? Do we need to rise above partisanship, put people first and save lives, by moving swiftly to change outdated laws to help our citizens?

I'd like to know your thoughts on that. I heard Mr. Perron comment at length on the subject.

● (1820)

Mr. François Perron: Would you like me to say more?

Ms. Marie-Hélène Gaudreau: Go ahead, Mr. Perron.

Mr. François Perron: I think it's important to make clear that it's very hard to see any teeth in the existing legislation as it applies to the private sector, keeping in mind that I'm much more familiar with the framework for public institutions.

As things stand, it's very hard to assert the right to privacy, to be 100% sure that an individual will be notified if their personal information has been leaked or disclosed illegally. Many—

Ms. Marie-Hélène Gaudreau: Thank you, Mr. Perron. I have another question.

We are realizing that legislation doesn't keep pace with technology, and it's on us, as lawmakers, to correct that. You've appealed to us to act, so I thank you for that.

Actually, we know exactly what we have to do. First, we need to deal with legislation to give it more bite and assist you in your efforts. Then, we can turn swiftly to the matter of location tracking.

Am I wrong, Mr. Perron?

Mr. François Perron: It seems obvious to me that a clear legal framework is a must.

As you can tell, I'm fumbling a bit, but as long as that part isn't dealt with, having the right discussion around technology will be tough. That's a no-brainer.

Ms. Marie-Hélène Gaudreau: Since I have a bit of time, I'd like to ask you about identity. The Standing Committee on Access to Information, Privacy and Ethics talked about decorrelating the social insurance number to make it a digital identifier.

Where do you stand on that? Perhaps someone else could jump in quickly.

Mr. François Perron: If no one's going to answer, I will. One of the problems with a unique identifier issued by a single entity is that if that identity or identifier is revealed, made known or disclosed, the secret behind the information doesn't work anymore and you end up with the same problem you started with.

I don't think changing the nature of the social insurance number to make it some other type of number is a good idea. It would have absolutely no benefit.

The Chair: Thank you very much.

Thank you, Ms. Gaudreau.

It is now Mr. Masse's turn.

[*English*]

You have two and a half minutes.

Mr. Brian Masse: Thank you.

Mr. McKay, I know the bleach example may seem a little radical, but how do you deal with, for example, President Trump, who says that you should take hydroxychloroquine? The FDA has said you shouldn't. What do you do in a circumstance like that? It's happening right now.

Mr. Colin McKay: It's a very difficult conversation to have because, obviously, in working as a platform we need to respect that there are authorities and elected leaders who are giving specific points of view.

What we try to do and what you will see on YouTube is that, if a video is dealing specifically with COVID-19, there will be an information panel below that video. In the case of Canada, it will point directly to Health Canada's site on COVID-19, where you'll see specific advice about treatments, social patterns and behaviours.

We are always in this push and pull where we need to recognize that there are leaders, and they have a right to communicate with their citizens.

Mr. Brian Masse: Okay. You'll be happy to know that I did google that while I was waiting for my turn here.

I want to follow up with something from yesterday which I thought was important. It was from the Canadian Internet Registration Authority. I do want your opinion on this.

What I found interesting about the testimony last night from Mr. Holland, which was good, was it showed that it considers itself—and probably is—the gold seal or standard of registering Internet sites using the .ca brand. I'm fairly naive in the sense that I thought that the Government of Canada.... When I hear ".ca" I think it really has some standards, but there is no follow up to the authenticity of the activity of those who actually have that brand later on. I wonder if you have any thoughts on that.

To me, part of cleaning up fraud, attacking fraud and preventing fraud is the preventative work. I just find it odd that you could then use a platform like yours later on to perhaps be the sounding board or the morphing of something that may be very real and true at first into fraud later on. Is there any involvement of Google with regard to screening any of that?

Mr. Colin McKay: I am parsing what you just said. In terms of domain registry and actual geographic location, that process involves CIRA in the first step, and then ICANN, the international registry, secondarily.

For most websites, I think what you first turn to is actual criminal law enforcement, especially in cases of fraud, physical harm or misrepresentation.

● (1825)

Mr. Brian Masse: If I could just interrupt, they are overwhelmed right now.

I know you are going to get cut off, and my point is that we're overwhelmed and might need a more comprehensive solution, but thank you.

Thanks, Madam Chair.

The Chair: Thank you very much.

We are now moving into the third round. The next round of questions goes to MP Patzer.

You have five minutes.

Mr. Jeremy Patzer (Cypress Hills—Grasslands, CPC): Thank you very much, Madam Chair.

I'm going to begin with IBM. In your opening remarks, you referenced a single source of truth. I'm wondering if you could elaborate on whose truth that is.

Mr. Eric Johnson: That's an excellent question.

When you're pulling data together, you want to have one source. The problem is if you have multiple.... For instance, suppose you implement multiple contact tracing solutions, and you're pulling data into multiple databases. When you're asked a question, you could get three answers, right? It's okay to have multiple solutions. You just want to make sure that the data at a provincial level is coming in and it is a single source of truth.

From that, you can then do systems of insight. You can build predictive modelling tools, but at least you have the confidence that the data you have is in one single place.

Mr. Jeremy Patzer: Right, so if it's a single source of truth, would all three answers, per se, still be available, though?

Mr. Eric Johnson: For sure. It's integrating it so that you know you're drawing it from only one source and you're not drawing it from multiple sources that might contradict one another or you might not get a full answer, that sort of thing. You want it all in one place.

Mr. Jeremy Patzer: Right. Thank you.

I'm going to switch to Mr. McKay from Google.

We've heard here tonight that 60% to 80% is required for tracing apps to be effective. In the U.S., the adoption rate appears to be quite low. NBC recently reported that the highest usage is at around 2%, in South Dakota. Why do you think it is so low, and, how can you make the case to Canadians that these apps will be effective and useful as well as respectful of their privacy?

Mr. Colin McKay: In response to your first question, I think we're at only the initial stages of the rollout of either the API or the apps.

To the second part of your question, I think it's up to the public health authorities and the governments to make the case to their citizens that there's a need and an obligation to use these applications for the greater public health. We're simply providing the tool that enables them to make those apps more effective and more productive.

Mr. Jeremy Patzer: You talked earlier about updates being put through with tracing built in or to make its operation more app-friendly. How easy would it be for, say, Android or iOS or an Apple platform to force an update onto a device without the end-user knowing that he or she had received that update?

Mr. Colin McKay: I can speak only to the Android platform, on which you receive notifications when there are updates to either an app or the operating system itself, which give you a description of what is happening and why it's taking place. Then once again, even after the implementation of the updates, you can make the decision within the permissions to deny access to Bluetooth and to deny access to location information. So even if there is the functionality, you can still turn it off on your device.

Mr. Jeremy Patzer: Reuters reports that 23 countries have expressed interest in your technology. Are any of these countries problematic in terms of their human rights record, and would you make this technology available to such governments?

Mr. Colin McKay: I'd say that we provide this technology to public health authorities in the pursuit of public health. I can't speak to what countries those might be and what conditions there may be. We're still in the early days and we're still in the process of actually rolling out the API.

Mr. Jeremy Patzer: Right, but if YouTube is willing to shut down users because they contradict a world health order, if we have countries in which health authorities are in gross violations of human rights, would you deny them access to the platform?

Mr. Colin McKay: I think we're still in the hypothetical when we're talking about the particular Apple-Google project.

Mr. Jeremy Patzer: Right, but there are lots of countries that are predominant in the world, and they have their own health authorities, but they also have gross human rights violations that have been covered up through misinformation and different scenarios. Would you prevent them from utilizing this technology?

● (1830)

Mr. Colin McKay: Once we roll out the API, there's a process engagement between Google and the government and the public health authority for the implementation. We need to make sure that they respect our terms and conditions and the terms of service around the API use before it's actually rolled out to their app.

Mr. Jeremy Patzer: Thank you.

Last, would you allow information sharing between countries if they were using the same app? Again, if you had multiple countries with bad human rights records, would you allow them to share records with one another?

Mr. Colin McKay: The way we've structured the app is that it's on device storage, and then it's uploading to public health authorities. It's meant to be binary that way, and any information sharing would be between the health authorities separate from our API or our OS movements.

Mr. Jeremy Patzer: Thank you.

The Chair: Our next round of questions goes to MP Longfield.

You have five minutes.

Mr. Lloyd Longfield (Guelph, Lib.): Thank you.

I'm going to continue along the path that Mr. Patzer was on with Mr. Erskine-Smith.

I want to explore first of all with Mr. Johnson from IBM, and then go over to Mr. McKay.

It's great to see you again. I know you helped to guide us through Washington when INDU visited there last Parliament. A lot of what we do relies on co-operation and coordination with the United States. We are working on our digital strategy and including the digital charter looking at increased penalties and enforcement powers. I know we have worked with organizations like IBM on some of our strategy in terms of managing data and anonymizing and aggregating it, working with Statistics Canada.

When we're working with the United States, we have some data treaties, and IBM is obviously on both sides of the border, in fact across a lot of borders, which gives us some international exposure to opportunities for data sharing in the right ways. Could you maybe comment on the work that IBM is doing in terms of large-data management and storage?

Mr. Eric Johnson: I can comment at a high level. I'm not an expert in this space, but I can tell you that, for instance, when we are implementing a system in Canada in particular that is going to deal with public health information, PHI, we have to abide by the provinces' rules and the federal rules. It has to reside in Canada. It can't cross the border or anything like that. We adhere to that.

We have a set of data-specific legal counsel that guides us, and we interact with local, typically provincial, lawyers or federal lawyers, if that's the case, but that's generally.... Because of that, we can give a perspective from Europe or from whatever jurisdiction we need to talk to. That's pretty high level, but that's what I've been involved in.

Mr. Lloyd Longfield: That's good.

I know at the University of Guelph, IBM is a partner looking at data around crop production, crop tracing and tracing of disease within crops. This would be something similar, only on human health.

Mr. Eric Johnson: Yes. Again, the type of data is very important in how it's shared. You may want support or people working on your data or working on your project, but they're not within Canada. Then they have to abide by all the privacy and security legislation. We have to make sure they're not seeing that data. There are all sorts of anonymization tools, and I'm sure other colleagues could comment on it, but that's something we do as well.

Mr. Lloyd Longfield: It's those things that the general public, in terms of the rules around anonymization and aggregation to make sure public privacy is protected.... People distrust government and people distrust big companies. You're one; we're another.

Mr. Eric Johnson: Yes.

Mr. Lloyd Longfield: Building public trust in order to get people to return back to work is a real challenge, so that's one that fits into Google and what is going on with Google and Apple.

I'll go over to Mr. McKay maybe to comment on the Privacy Commissioner of Canada's saying that if this isn't effective, we will destroy the information that we've collected, and that there will be management.

Google gives us, again, worldwide opportunity that, if somebody is coming from another country, let's say the United States.... We have a lot of visitors from the States, not so much right now, but at some point we will have that again. How do we protect ourselves against Americans who are coming into our country and bringing COVID with them?

● (1835)

Mr. Colin McKay: I think you're talking about general public health protections and border restrictions.

From the point of view of the exposure notification API, you've noted an important element of how contact tracing must roll out and must be negotiated between public health authorities in different jurisdictions, which is how exactly they share information or they correlate information so that they can provide exposure notifications outside their own jurisdiction.

That is one of the more complicated elements of the conversation we're having around privacy because of the intersection between public sector data privacy rules and private sector data privacy rules that needs extreme focus and debate.

Mr. Lloyd Longfield: That also brings into the discussion the World Health Organization and the need for an international body.

I'm out of time.

Thank you very much.

The Chair: Our next round of questions goes to MP Rempel Garner.

You have five minutes.

Hon. Michelle Rempel Garner: Thank you, Madam Chair.

I'm just going to build on some of the questions that my colleague MP Patzer was asking.

I will go back to the sharing of information with an app or the utilization of the API.

I'll go to Google. You talked about how there would be a binary between the app and, let's say, a public health authority. What about in a situation where the public health authority is part of what Western democracies would consider to be a malicious state actor with human rights violations? Is your company concerned about potentially aiding and abetting potential human rights violations in that situation?

Mr. Colin McKay: In the context of the exposure notification API, we've explicitly engineered it so that there is only the exchange of information about Bluetooth localization, and it isn't identifiable information for the public health authority. We would be communicating information about mobile phones that had been near each other within the constraints identified by the public health authority. They would have—

Hon. Michelle Rempel Garner: Okay.

So then, going on to that, I know that Bluetooth technology in and of itself is certainly not impervious to security issues. I know that there are two common vulnerabilities. There's “Bluesnarfing”, which is unauthorized access from a Bluetooth connection, or “Bluejacking”, which is sending unsolicited messages to a nearby Bluetooth device.

What work has your organization done to prevent a situation where, for instance, a hacker falsifies the spread of COVID? Let's say a malicious actor does that and then that information is spread. Let's say I had my phone on and I'm all well and good, or my family is all well and good, but somebody wants me to be in quarantine for two weeks. I have no idea who would want me to do that, but let's say somebody hacks my phone and sends a false positive on that. What liability would your company have, or how would you be preventing that from happening?

Mr. Colin McKay: It sounds like you're describing two separate things.

In terms of Bluetooth security, I can certainly follow up with what we've been doing to create a secure environment on Android phones.

In the other context, particularly the one you have identified around false positives, that's actually a system that would be controlled at the public health authority. They would be taking the results of COVID-19 testing and then using the API to notify people who had been in close proximity to the person identified as being diagnosed positive. So you—

Hon. Michelle Rempel Garner: Sorry, but just to clarify, I was asking this: What if I were falsely identified as being near that person?

Mr. Colin McKay: Well, that verification would be up to the public health authority who's using that information to then request proximity data from the API in order to notify people that they've been close by. The next step from that is then to move to testing. The way the API would work is that you would be notified that you had been in close proximity to someone who had been identified as infected. Then you would move to testing to verify whether or not you, in fact, had been infected by the virus.

Hon. Michelle Rempel Garner: Right. I mean, we're sort of having this conversation in the context of a western democracy, but what about...?

Things have changed here even, to a certain extent, one could argue, but again, I just don't understand that security aspect. What if I were falsely identified through hacking or misinformation or something using this Bluetooth API? I would be subject to a whole range of measures that I or somebody else wouldn't need to be. Has this been identified as an issue? How would you address this?

I guess what I'm saying is that contact tracing through API could be spoofed, right? How would we address that as legislators?

● (1840)

Mr. Colin McKay: I mean, we're speaking about a hypothetical. The data that we're talking—

Hon. Michelle Rempel Garner: An important hypothetical.

Mr. Colin McKay: Yes, but the data that is on an Android or iOS device is simply a list of exposures that you've had to other nearby devices over a defined period of time.

If someone was going to spoof your test results or was going to try to trigger—

Hon. Michelle Rempel Garner: I'm not saying spoof my test results; I'm saying spoof me being near somebody who had a positive.

Mr. Colin McKay: I'm just processing this.... In the context of the data that's available on the phones, that would be extraordinarily difficult, because the Bluetooth records themselves are randomized and anonymized.

Hon. Michelle Rempel Garner: Thank you.

The Chair: Our next round of questions goes to MP Jowhari.

You have five minutes.

Mr. Majid Jowhari (Richmond Hill, Lib.): Thank you, Madam Chair.

Welcome to all the witnesses. This is quite informative.

We're going into a lot of depth in the technology and also in privacy. One of the areas that I continue to struggle with still is one of the elements that was highlighted as part of the Triple A rating of Madam Arjomandi, specifically the adoption.

Let me tell you what I'm struggling with and put it into perspective. Canada has around roughly 35 million people. If we try to adopt even the lower end of the scale, which is about 60%, we would need about 21.5 million people participating in this. Assuming that we look at anyone above 15, this is probably about 100% of our adult population. In Ontario, we have about 14.5 million people, which puts it at about nine million people who should participate. Bringing it even one level lower, in York region, we have 1.2 million people, which means that about three-quarters of a million people should be participating. In Richmond Hill, we have about 200,000 plus, which means that 120,000 people should be participating.

Now, almost 20% of our population lives in the rural and remote areas. That's roughly eight million. Therefore, using that 60%, 4.5 million people should participate in that. Forget about the digital divide and the challenges that we have on being able to actually get the platform going.

I know that most of you opted out of answering this question, but I want to go back to where MP Erskine-Smith left off. Why should we not consider, in circumstances such as a pandemic, an opt-out model? Make it mandatory by the government and health organizations to adopt and use the application.

We could start with Ms. Arjomandi.

Ms. Fay Arjomandi: An opt-in or opt-out model won't work, because I can turn off my phone and not use it, or I can use a different phone. Why do that when there's a solution? Again, the solution is that you create a trust between end-users and government that here is a solution that you have, it's in your control and it is available. There is no digital divide in the solution that we're proposing. It's available on both Android and iOS. On the data, again, the data remains on your own device.

Let me give you a very different analogy here. Imagine that all your digital assets are kept in your home. Nobody has the right to come into your home unless it's with a warrant because you're accused of an illegal breach, right? If that's the way I think about my data, then that's the way I would try to utilize the app. I would use the application, because it benefits me as well—

● (1845)

Mr. Majid Jowhari: Yes. I anticipated that probably you'd answer. I did a quick check. In 2019, when we had the federal election, out of 33.5 million people, 25 million were eligible to vote, and 66% participated knowing that their votes and their participation would stay confidential. That's about 17 million. That's still way short of the 21.5 million for us, based on the number being discussed. We can talk about the U.S., with 2% adoption, or Calgary, which is now into the 4% adoption rate.

If in our most sacred civil duty we get 66%, or 17 million, how are we going to ensure that we can get to 21.5 million?

Ms. Fay Arjomandi: Because it's my health and it's important for me. Also, it's about being suspicious about existing systems. We all know that on the Internet no data gets deleted. I buy something from Amazon shopping and I come to YouTube and see the video of what I was looking for, so we know that nothing is getting deleted. We know that every intimate moment of our lives is being captured and utilized for advertising.

This is about health. We are worried. We are scared for ourselves and for our loved ones. We would use a solution if we knew that our data was—

[*Translation*]

The Chair: Thank you very much.

Now we'll start the next round.

Mr. Savard-Tremblay, you may go ahead. You have two and a half minutes.

Mr. Simon-Pierre Savard-Tremblay (Saint-Hyacinthe—Bagot, BQ): Thank you, Madam Chair.

I have a question for Mr. McKay from Google Canada. In recent years, Google has entered the health domain, partnering with hospitals and health groups. There were two stories in the news where it was revealed that patients didn't know their information had been collected.

From what I understand, that's not at all how this works. It's something the person agrees to voluntarily, so there's no risk of someone's information being collected without their consent. Is that true, yes or no?

Please keep your answer brief because I have another question for you.

[*English*]

Mr. Colin McKay: In the case of the API, you are getting consent because you have to download an app from the public health authority in order to enable that functionality.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: That's great. Thank you.

That brings me to my other question. As we know, whenever a user installs an application, they are asked to provide their consent. Between you and I, there's no denying that most people don't read the fine print and hastily tick “I agree”. I know that's not your fault, and that it's every person's responsibility. That said, those conditions and requirements that the user has to accept never explain what happens to the data after they tick “I agree”. I'd like you to shed some light on that for us.

What happens to my data after I tick “I agree”?

[*English*]

Mr. Colin McKay: In the case of Android, what you can see when you're downloading an app is there are very granular specifications of what data they're looking for. You can click on each type of data to see an explanation of why they are looking for it. Furthermore, you can deny the app access to that data. In some cases that means the app won't work, but in most cases you can be very specific about what data it has access to and when it has access to it.

In relation to your question about privacy policies and terms of service, we've also taken steps to make sure that those are more clear-cut and understandable, especially on mobile devices.

[*Translation*]

Mr. Simon-Pierre Savard-Tremblay: Thank you.

The Chair: Thank you very much.

[*English*]

Mr. Masse, you have two and a half minutes.

Mr. Brian Masse: Thank you, Madam Chair.

I'll leave this question open to any of the witnesses who want to jump in.

With regard to the methodology of contact tracing and the public resources to gear us towards it, we know that turning on and off the devices will skew results. There is also the reliability of the data itself through the actual processing.

I don't know whether there are strong feelings out there about this, but I've always worried about how much public policy we do through contact tracing in the general sense, because it is anonymous or is supposed to be anonymous. It's also optional, and we don't have the other variables in there.

Are there any thoughts on that? I'll put that out on the floor, if somebody would like to jump in.

● (1850)

Ms. Fay Arjomandi: If I understood the question correctly, it's about adoption. How do we ensure adoption for the user? I believe it's about ensuring that data remain private.

Mr. Brian Masse: It's also about the quality of the data that influences public policy. If I turn off all of my data tracking, that's not going to provide any balance in terms of.... It's about a participation rate. It's similar to the census. It's skewed. If it's about location definition, we don't know what the skew is at any particular point in time.

Ms. Fay Arjomandi: I believe that can be addressed by incentivizing users, providing them the right service and giving them options to decide what type of data they want to share with the health authority and with other central authorities. I believe that's the only way. If I have control over....

Again, this is not consent, because consent is quite ambiguous. This is about being able to pick and choose whether you want this data to be accessible by this entity for this period of time so that they have the right to copy it or they don't, or have the right to view it or they don't.

Mr. Brian Masse: Okay. Well, I appreciate it. I know my time is—

Ms. Fay Arjomandi: [*Inaudible—Editor*] and to have usage and to basically achieve the best of both worlds.

Mr. Brian Masse: I'm just very skeptical of the statistics and how meaningful they are.

The Chair: Thank you very much.

That completes our third round. We do have a bit of time left, so we can start some slots on the fourth round.

With that, we'll give the first five-minute round to MP Gray.

Mrs. Tracy Gray: Thank you, Madam Chair.

My questions are for Mr. McKay again, please.

You have the mobility reports that you've been working on. Would you recommend that governments use these mobility reports for any kind of policy decision?

Mr. Colin McKay: What we've seen since the mobility reports have been rolled out is that public health authorities are using them as one data point in assessing whether or not their public health orders around social isolation and broad-based community behaviour are, in fact, working. That was our intent: to provide that trend-based analysis so that they would have an impression of whether or not society is changing as a result of their guidance.

Mrs. Tracy Gray: If the governments are utilizing this information when they're having their discussions and if the public is also seeing this information—because we've seen some of these reports as headlines in the news, where people are moving to.... I just want to draw your attention to the bottom of the mobility report. You do have a disclaimer that states that people have to be opted in as users, that the data represents a sample of users, that this may or may not represent the exact behaviour of a wider population. That's at the bottom of your 10-page report.

With that type of a disclaimer, how much of a representation is it truly? What percentage of the population is it actually representing? Is it 0.01% of the population? Is it 90% of the population? These are headlines. The governments are actually talking about these numbers. What does it actually represent?

Mr. Colin McKay: We haven't disclosed the actual representation. You're right. It is a subset—opted-in users—of a subset—Android phone users and Google account users. What is useful from the information is the way that it provides a comparison with a baseline before COVID-19 hit, which is from early January to early February, which is relevant for most of the world. It provides that comparator, which is a data point that's useful as people try to assess whether or not they're seeing behaviour change.

● (1855)

Mrs. Tracy Gray: Okay. Has Google Canada been approached by any governments with regard to expanding the scope of the data to include more data being disclosed in these community mobility reports?

Mr. Colin McKay: The government and public health authorities are interested, as everyone is, in seeing whether or not trends are changing or are relevant in their own communities. We are rolling that out gradually and globally. In the United States, you can see data down to the county level. That would be the next iteration of the report for Canada if we roll it out.

That isn't specifically a request from the government or public health authorities. Rather, it's the way that we're developing the report and providing the information as we can process it.

Mrs. Tracy Gray: You've gone in to my next question, around breaking it down more closely. Right now when we look at the reports, you have them by province or territory. Do you have plans to break this down further, such as by municipality or region, and to share that data with governments?

Mr. Colin McKay: We've already done that in some jurisdictions. The intent is to roll out that next level of data—whether it's at the municipal, county or regional level—and to make that public just as we have the reports themselves right now.

Mrs. Tracy Gray: When you say that you've already done that for some jurisdictions, does that include within Canada, or—

Mr. Colin McKay: No.

Mrs. Tracy Gray: You've done that in other parts of the world, and now you're going to be considering breaking it down further within jurisdictions and municipalities in Canada. What would be the smallest subset that you're considering? Would it be geographic? Would it be based on town? Would it be based on population? Would it be based on users? How small would you go for that reporting?

Mr. Colin McKay: The variable here is the hierarchy of data that we have available to us in our Google Maps product and how it's classified. It's an interesting conversation because we divide differently those areas that you just described, depending on the province. Some are regional municipalities. Some are united counties. Others are cities. That's part of the process that we're going through right now to identify how we can make that information available.

Mrs. Tracy Gray: If you go down much smaller, how accurate is it? Then you have a much smaller user base and people are much closer.

Mr. Colin McKay: The existing reports reflect that data gap. Some of the classifications for the territories have major gaps in the trend lines because enough information isn't available to us to anonymize and aggregate to a level that meets our expectations around privacy.

The Chair: Thank you very much.

Our next round of questions goes to MP Ehsassi. You have five minutes.

Mr. Ali Ehsassi: Thank you, Madam Chair.

I'll be sharing my time with Mr. Erskine-Smith.

I have a quick question for Mr. McKay and Ms. Arjomandi. Mr. McKay, as you've noted, it's going to be challenging to get meaningful participation from enough people in a jurisdiction. Another thing I've been following is that in the U.K. a lot of people had a hard time registering if they had old Android phones; they were not compatible and they couldn't participate. How do you intend to get around that particular challenge?

Mr. Colin McKay: We're working hard to make sure that the vast majority of Android phones are able to take advantage of exposure notification, and then the subsequent OS improvements. It will be a case where it's more than a significant majority through most of our operating systems.

Mr. Ali Ehsassi: Thank you.

Ms. Arjomandi, I know Mimik has a very strong record behind it. I know that your company has had its eyes on the ball and has been beavering away, if you will, for the last couple of months. What has your experience been in Canada? How come you haven't launched an application to date?

Ms. Fay Arjomandi: For the solutions to be adopted and distributed, we need government and our health authorities to build experience with it. With regard to the policy we were just discussing here, the question is how to configure and provide confidence to the users that their data is getting protected and it's in their control.

I'm doing contact tracing for me. If I do that contact tracing for me and for my own well-being, with the assurance that I can share data where I need it to help me, then I will do it. That's why we have engagement with large enterprises, but for the direct-to-consumer solution we would like to have some engagement from governments. We have reached out to so many federal and provincial government entities and health organizations, but so far, I guess everybody's busy. We're hoping to get heard for the direct-to-consumer solution.

● (1900)

Mr. Ali Ehsassi: Thank you.

Over to Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Thanks, Ali.

Mr. McKay, has anyone from the Government of Canada been in touch with Google to work together on a proximity tracing application?

Mr. Colin McKay: We're in conversations with the federal government and the provincial governments about the possible use of the encounter notifications API.

Mr. Nathaniel Erskine-Smith: Is the same true of the provincial government here in Ontario?

Mr. Colin McKay: Yes.

Mr. Nathaniel Erskine-Smith: What happens in a few months when you roll out the secondary plan for the public health applications? Are they rendered moot in some fashion?

Mr. Colin McKay: No. It's an improvement to the technology. Rather than relying on an API the OS itself is improved so the app can continue in the same process.

Mr. Nathaniel Erskine-Smith: We've had a conversation tonight about opt-in versus opt-out. Is it technologically possible, in your view, to have an opt-out system?

Mr. Colin McKay: It's technologically possible. Do you mean by forced download?

Mr. Nathaniel Erskine-Smith: Right.

Mr. Colin McKay: If you're thinking about a forced download process—

Mr. Nathaniel Erskine-Smith: Or updating the OS, yes, exactly.

Mr. Colin McKay: Yes, in our case we require the user to consent to the download of an application.

Mr. Nathaniel Erskine-Smith: No, I know. Of course, I understand that Apple-Google's current system is very strongly supportive of opt-in. I completely get it, but I'm just talking about technical feasibility. Would it be technically possible to have an opt-out system, if I automatically updated an OS?

Mr. Colin McKay: At the moment, when an update is sent to a phone you have the ability as the phone user to not consent to the update. That exists for the app and the OS.

Mr. Nathaniel Erskine-Smith: Mr. Johnson, to my understanding, every province uses Panorama. Does every province maximize its use of Panorama in the same way?

Mr. Eric Johnson: No, and in fact, every province doesn't use it. Seven provinces and one territory currently use it. The immunization and vaccine inventory is in seven provinces, plus one territory, which is about 86% of our population of Canada having their immunization data in the database. However, outbreak management is only in a few of the provinces, five provinces.

Mr. Nathaniel Erskine-Smith: Which province best uses Panorama?

Mr. Eric Johnson: Which one best uses it? For the most extensive use, I would have said British Columbia and they do it in a whole bunch of different ways; the health authorities all implement it quite a bit differently. However, Saskatchewan and Manitoba have outbreak management, as does Nova Scotia. New Brunswick is in the process; they're almost there.

Those provinces are all using it extensively.

Mr. Nathaniel Erskine-Smith: However, not Ontario and Quebec.

Thanks.

The Chair: Unfortunately, that's all the time we have for this evening. I thank the witnesses for their time, and everyone who is supporting us in this endeavour. We have had excellent questions and excellent testimony again this evening.

With that, I will call this meeting adjourned and I will see you on Monday.