HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

# Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 136 • 1st SESSION • 42nd PARLIAMENT

**EVIDENCE**

## Tuesday, February 19, 2019

---

## Chair

**Mr. Bob Zimmer**

# Standing Committee on Access to Information, Privacy and Ethics

**Tuesday, February 19, 2019**

● (1530)

[*English*]

**The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)):** I'll call to order meeting 136 of the Standing Committee on Access to Information, Privacy and Ethics for our study, pursuant to Standing Order 108(3)(h)(vii), of the privacy of digital government services.

Today we have with us Alex Benay, chief information officer of the Government of Canada; Aaron Snow, chief executive officer, Canadian Digital Service; Ruth Naylor, executive director of the information and privacy policy division, chief information officer branch, Treasury Board of Canada; and last but not least, John O'Brien, director, security and reliability engineering, Canadian Digital Service.

It's my understanding that Mr. Benay and Mr. Snow will each speak for 10 minutes, so go ahead, starting with Mr. Benay for 10 minutes.

**Mr. Alex Benay (Chief Information Officer of the Government of Canada, Treasury Board Secretariat):** Great. I will be doing my address in both languages, if you want to connect your headphones right away, and I apologize in advance to the translators: I get quite excited because this topic is very important to me. I will try to make sure I speak slowly.

Thank you, Mr. Chair, for the invitation to appear here before the committee today.

[*Translation*]

As you mentioned, with me today is Ruth Naylor, executive director of the information and privacy policy division.

I will start with some brief remarks, after which, I will be happy to answer the committee's questions.

[*English*]

Mr. Chair, in the age of smart phones, social media and apps that do everything, Canadians have a growing expectation that their government will provide them with services as easily as Expedia, Amazon or Netflix do, which is why the Government of Canada is embracing digital tools to provide Canadians with the reliable, accessible and secure services they expect, while at the same time protecting their privacy.

We believe that better service and privacy are not at odds with each other, thanks to technological improvements that allow these protections to be built in from the concept and development stages.

[*Translation*]

As chief information officer of the Government of Canada, I am responsible for providing strategic direction and leadership in information management, information technology, security, privacy and access to information across the Government of Canada.

Therefore, my office has taken steps to promote digital services and better protect Canadians' personal information.

[*English*]

For example, the Government of Canada recently adopted a set of digital standards that help departments and agencies design better services for Canadians. They ensure that government makes investment decisions that increase security and privacy, builds in accessibility from the start, and allows for more collaboration while working in the open. These standards are being put into action with the next-generation HR and pay initiative, which is to identify options for an alternative HR and pay solution.

Working through our agile process, these digital standards are being used to assess whether vendors can meet government business outcomes, including delivering a solution that is secure and respects the privacy of users. The digital standards allow us to define how the future of government services will be delivered in a digital age, while enabling us to be more agile, open and user-focused at all stages of design.

[*Translation*]

The initiative to develop the next-generation human resources and pay solution is an example of what can be achieved when the standards are applied successfully.

The process will take a few more years yet, and much work lies ahead, but the results to date are promising.

In addition to digital standards, we are developing rules and guidelines based on best practices to help departments and agencies with the digital transition. For instance, in the spring of 2018, the government approved targeted changes to the Policy on Management of Information Technology and the Policy on Information Management.

The targeted changes are meant to address a number of issues. These include improving governance and oversight of information technology, or IT, overall, and strengthening the role of the chief information officer of the Government of Canada and that of departmental chief information officers.

As recently as December 2018, we updated the Directive on Management of Information Technology.

More specifically, as part of our digital exchange strategy, we adopted modern procedures related to application programming interfaces, known as APIs.

[*English*]

I apologize for the technical term.

[*Translation*]

Our changes have made Government of Canada services and data accessible via APIs, promoting the re-use and sharing of data across departments and with Canadians.

The API standards also enable the private sector to streamline services in co-operation with government and ensure Canadians' security and privacy.

In December 2018, we also updated our rules on enterprise architecture, which is the coordination of information, applications, technology, security and personal data.

The changes we've made support open standards and open source programs, “cloud first” principles, as well as ethical data collection and data security principles.

Ultimately, with these changes, staff will be able to work more efficiently government-wide thanks to a better convergence of technology and policies and opportunities for dialogue from the beginning of the procurement process.

These measures are key in order for the Government of Canada to develop a comprehensive digital strategy for the long term.

● (1535)

[*English*]

A key focus of the proposed policy is to integrate security and privacy at the investment and design stage of government services, programs and operations. The proposed digital policy will continue to be developed over the course of this year.

Along with our partners at the Canada School of Public Service, we've also created a public sector digital academy, the first ever in Canada. The academy will be giving our employees the leading edge skills they need to deliver the digital government services Canadians expect. An important part of this curriculum is privacy.

As we move forward on digital service delivery, we're also collaborating with provincial and territorial governments, as well as the private sector, to create rules to commonly accept and trust digital identities.

Canadians don't need to know how government is organized or the intricacies of federal, provincial and territorial jurisdictions when they try to access services.

To improve service delivery, we'll focus on the needs of the user rather than the organization of government, and enable Canadians to conveniently and securely access online services across jurisdictions. For example, we are building a digital identity ecosystem to support the use of trusted digital identities by Canadians to access services across jurisdictions. These jurisdictions include all orders of government, private sector and even international partners.

Specifically, development has begun on an initiative called “Sign In Canada”. Through this common access point, Canadians across the country will be able to access their government services online using their federated trusted digital identity. Sign in Canada will also support the digital service strategy and our efforts to federate identity across the government of Canada.

In addition, we are establishing a digital exchange platform to help enable departments to share their data with each other and the outside world in a modern, secure and unified way. This would be similar to Estonia's X-Road, which you've heard about. Just as Canadians don't need to know how government is organized to access services, citizens expect government not to ask repeatedly for the same information.

[*Translation*]

Furthermore, we've adopted mandatory procedures in relation to enterprise architecture and begun a preliminary conceptual analysis review to ensure alignment. We've also established an enterprise architecture review board, made up business and technology representatives from across government. In managing the information Canadians share with us, we want to ensure their privacy is respected while enhancing interoperability government-wide. This work is still in the early stages.

[*English*]

We are committed to improving service delivery by investigating a "tell us once" user experience. This means that Canadians could possibly provide key information once and not be repeatedly asked for the same information when dealing with different departments and agencies. My staff is currently examining government business processes, policies and legislation to identify any barriers to implementing this service vision. With this in mind, we need to look at the rules around information-sharing and how we could, with the right checks and balances in place, allow more efficient information-sharing across departments and agencies that provide services to Canadians.

My staff is also working closely with the Office of the Privacy Commissioner to benefit from advice on our plans and initiatives to advance digital government. We've heard from the Privacy Commissioner that privacy should not be characterized as a barrier to innovation. We look forward to continuing to work closely with the Privacy Commissioner to rethink how we can best protect the personal information of Canadians.

To meet our privacy obligations, we have to do the hard work of developing digital services that are citizen-centred and protect the personal information of Canadians. To that end, we're collaborating on a number of fronts in order to share best practices and learn from the work of others. To harness the power of technological advances, TBS and PSPC have been working to develop innovative and agile procurement tools to meet the current demands of the public service.

[*Translation*]

We recently worked together to build the first list of AI suppliers. They had to demonstrate that they had the necessary resources and skills and had adopted ethical AI practices. To safeguard privacy, this initiative is aligned with, and builds on, the government's direction and our current policy development work.

This initiative promotes the use of new tools, while providing concrete direction and oversight to limit unintended consequences for Canadians. To develop a meaningful strategy, we worked transparently with international experts, industry leaders and government officials who will oversee its implementation.

● (1540)

[*English*]

This is part of our concerted effort to open up government that was recognized in September when the World Wide Web Foundation's Open Data Barometer ranked Canada first in the world alongside the United Kingdom for its open data leadership. Each of these areas, such as Al, data, cyber and privacy do not exist in silos. They are intertwined with each other and with other sectors to such an extent that it is impossible to know it all.

Technology continues to dissolve traditional boundaries, which is why it's essential that we continue to work as one government, recognizing that all aspects of our businesses are being touched more and more by technological advances.

Success in digital government means providing the seamless, integrated services people have come to expect—services that meet people's needs and expectations of government, and that ensure government stays relevant in people's lives. This obviously includes protecting the privacy of Canadians.

Charting this course for modern digital services, including privacy protections, will keep Canada on the cutting edge of citizen support and engagement.

[*Translation*]

In closing, I want you to know that I look forward to the committee's report and recommendations on this important issue. Thank you.

[*English*]

**The Chair:** Thank you, Mr. Benay.

Next up, for 10 minutes, is Mr. Snow.

**Mr. Aaron Snow (Chief Executive Officer, Canadian Digital Service, Treasury Board Secretariat):** Thank you, Mr. Chair; and thank you to the committee and Alex.

With me is my colleague John O'Brien, director of security and reliability engineering at the Canadian Digital Service. Before CDS, John was with the Communications Security Establishment as a technical lead for malware analysis and automation, or put more simply, John knows how the bad guys operate.

For those of you who are less familiar with CDS, we're a digital consultancy in government, for government. We're part of the Treasury Board Secretariat and we work side by side with Mr. Benay's organization. CDS was established only 18 months ago, with a mandate to help this government improve how it designs and delivers digital services by providing direct, hands-on help to federal departments to make digital services faster, simpler, more accessible and secure. In the process, we help build capacity in those departments to do modern service design and delivery.

For example, we've been working with Veterans Affairs Canada to improve how veterans and their families find and access benefits; with Immigration, Refugees and Citizenship Canada to help newcomers to Canada reschedule their citizenship tests online; with the Royal Canadian Mounted Police to help victims report cybercrime and online fraud; with our colleagues in Mr. Benay's office to make connections to government websites more secure; and with the Canada Revenue Agency to help Canadians with low income file their taxes and access related benefits.

[*Translation*]

I'm American.

[*English*]

Before I arrived in Canada last spring, I had the privilege of leading a similar initiative in the U.S. to bring new tools, practices and approaches into government to better serve the public. In 2013, I was a presidential innovation fellow. We were told on our first day as fellows that it was a bait-and-switch program, and sure enough, many of us who signed up for six-month fellowships stayed for four years.

My colleagues and I went on to create the service delivery unit called 18F in the aftermath of the failed initial launch of healthcare.gov. I served as 18F's first director of delivery and then as executive director. I'm also a former lawyer.

As Mr. Benay pointed out, digital isn't just about bringing services online. As our U.K. colleague Tom Loosemore once put it, digital is about "Applying the culture, practices, processes and technologies of the Internet era to respond to people's raised expectations."

Technology is not without its challenges, but it's not usually the hard part. We only half joke at CDS that we're a change management office disguised as a digital service office half the time.

How do we go about designing and developing government digital services that are both easy to use and secure? There are lots of answers to that question, but I want to touch on five important practices that CDS tries to demonstrate in every project we take on, and that historically have been more the exception than the rule in government, but that is changing rapidly.

Those practices are, first, to apply research and design practices that put people first, not rules and processes; second, to deliver and improve continuously; third, to assume there will be failures and to be good at reacting to them; fourth, to work in the open; and finally, to have strong feedback loops between delivery and policy.

In regard to the first, CDS relentlessly focuses on the people who use government services. In practice, this means working with users continuously to find out what they need, not just what government needs from them. We know that among those needs, security and privacy are critical and non-negotiable. To meet those needs, we factor them into how we build and deliver services from the outset, and continuously throughout deployment and development. This allows us to test our assumptions with the people who will use the service. If you've never witnessed user research, it can be eye-opening and profoundly humbling. It lets us develop a mutual understanding about what data is actually necessary to complete a service transaction and provide a first-rate experience.

By engaging with users early on and throughout the design of a service, we're able to develop an ever-improving understanding of their specific needs, concerns and preferences, including what and how much personal data we need to deliver a great service, how long we need to retain that data, and how we can provide assurances about how we will handle it, and when appropriate, delete it.

Talking directly and often to the people we serve is critical to building in privacy and security from the start, which brings me to the second point about how we work.

We develop digital services iteratively, employing practices and tools that enable continuous, incremental improvement. How does this promote more secure systems? The Canadian Centre for Cyber Security publishes a list of the top 10 IT security actions organizations can take to minimize the likelihood and impact of a cyber intrusion, and one of their key messages is to keep your systems patched and up to date, such as the regular updates you make to your phones from Apple, Google or BlackBerry.

This seems simple, but it's an issue for organizations everywhere. To do this well and in a timely way, services need to be built in such a way that frequent improvements are the norm, not the exception. The harder it is to make changes to your system, the longer it will take to create and disseminate fixes when a vulnerability is discovered.

● (1545)

Some government systems in operation today deploy changes only a few times a year, other than urgent patches, and even a simple change request can take more than a year to work its way through the long queue, get coded, and survive a lengthy, manually driven gauntlet of review, compliance tracking, testing, staging, and perhaps a little silent prayer before it goes live.

By contrast, most of the websites that you interact with every day, built by companies like Amazon, Google and Shopify, release dozens or hundreds of changes every day, safely, quickly and painlessly, into the public. This process is commonly referred to as continuous delivery, and it's how we build things at CDS, too. Updating systems to improve reliability, to fix problems, and to adapt to users' changing needs and expectations is easier, faster and more reliable this way. Making this model of continuous delivery and improvement the norm in government is both a problem of technical debt and a problem of delivery practice. Modernizing our systems and how we manage changes to those systems is the single-most effective thing we can do to improve the security posture of those systems.

This brings me to my third point. Continuous delivery enables you to act quickly when something goes wrong—not if, but when. In a perfect world, every system would be 100% secure. Of course, we don't live in that world. Cybersecurity best practice is to make the rational assumption that failures and breaches will happen, and to plan accordingly. Leading organizations make the most of the lessons learned after every such incident, large or small, to improve their resilience. We conduct blameless post-mortems after incidents, creating an environment where staff feel psychologically safe and confident in being fully open and honest about errors and mistakes. We learn more and improve more by acknowledging failures than by hiding them. It's healthier for organizations to encourage discovering and surfacing the root causes of failures than for people to fear being blamed for circumstances outside their control.

Fourth, we've all witnessed the blowback against organizations that stay silent about security incidents or other kinds of project failures for far too long. This is one reason why we work in the open—that is, in full view of the team, and whenever possible, the public. Building our services in the open by default reduces risk. This might seem counterintuitive. It is a stubborn myth that secrecy is good for security. In practice, developing software in the open allows others to contribute to, stress-test and critique our work. It provides more incentives for everyone to get the code right instead of taking shortcuts that might not be exposed in a tightly held environment. It gives us the opportunity to discuss openly the decisions we're making and the potential trade-offs. It allows us to create a culture of learning from mistakes, and it shares our work with others—a perk of which we've been the beneficiary many times already.

The U.K. government encapsulates this in a simple design principle, “Make things open: it makes things better”. The same principle appears in our government's digital standards.

This brings me to my final point about how we go about delivering secure, easy-to-use services to the public. Mike Bracken, who led the U.K.'s government digital service through its first four years, once wrote that “in an analog world policy dictates to delivery, but in a digital world delivery informs policy. This is what agile means for Government and its services”.

Working with and listening to our users, putting working prototypes in front of them as quickly as possible, and continuously improving those services is the best way to not only learn what works for our users, but also learn which policies are working, how others are not, and how we should update them to keep pace with modern expectations. This is somewhat of a shift from traditional policy development, which is often divorced, organizationally, from implementation. Everything is figured out months, maybe even years, before it lands at the people who will be impacted by it, at which point, unsurprisingly, it may sometimes miss the mark.

We believe that the practices CDS employs and promotes every day, practices encouraged by the digital standards, are the best way to meet public expectations for better, more integrated services that are also more secure and more responsive to the privacy needs of Canadians.

Having done this in two countries, I feel certain of this: change is hard, and it doesn't happen overnight. However, we're making headway in meeting the public's expectations for user-friendly, efficient, secure service delivery, and we look forward to making more and greater progress.

Thank you. I'd be happy to answer your questions.

● (1550)

**The Chair:** Thank you both.

First up for questions, for seven minutes, is Mr. Saini.

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

Thank you very much for coming.

I want to start off with you first, Mr. Benay. One of the things we've seen with the systems we have right now is that we have legacy systems and a shortage of technological skills within the government. You've started a concept called the Government of Canada talent cloud because of the ongoing change in our economy, the gig economy. Can you explain to me how that's working out? If you have people coming in temporarily, how do you build a long-lasting talent pool to make sure that you have the requisite talent going forward?

**Mr. Alex Benay:** The talent cloud is an experiment by a select few public servants who thought that we could look at a different model for bringing employees into the Government of Canada. We tend to take a decent amount of time to bring employees in, and the goal is to bring staff and employees into the Government of Canada within about 30 days. It's still the goal. It has not been achieved yet, but we're working towards it.

By using some of the techniques that my colleague Mr. Snow mentioned, they were able in the last year to launch a beta, open-source, very low-cost prototype where we're now hiring people within roughly 40 to 50 days. We're addressing the need to bring people in quickly in government.

The system also looks at the concept of the gig economy that's out there, where people in the technology field are increasingly choosing short-term assignments as opposed to a 35-year career with the public sector, which makes their coming in and out very difficult.

What we're trying to do with the talent cloud, which is still experimental, is to facilitate that trend and give otherwise contract employees the rights to have access to pensions and benefits. They may choose to come to work for six to 12 months at a time with our talent cloud solution, then leave for a few years and come back in. In the technology space, that's extremely useful, because it means that people stay relevant, people work in different sectors, and they're bringing in different perspectives. We're making that concept of a porous public sector increasingly a reality thanks to the work of the talent cloud team.

**Mr. Raj Saini:** Mr. Snow, in your opening comments you talked about iterative learning. With the amount of information that will be collected, there is going to be a lot of pressure to use AI to analyze the data and the public service metrics, obviously to make better decisions and to increase the efficiency of delivery.

How do we convince the public that this is something that will be in their and the government's best interests in the long term?

**Mr. Aaron Snow:** The core principles that you need to stick to to maintain and gain the public's confidence are transparency and acknowledgement.

When we talk about iterative service development, we talk more about user research and understanding these users at a more micro than macro level, which might be more conducive to the use of AI. For any number of veins, when we're talking about using large amounts of data and algorithms that may or may not be perceptible by most of the public, it is core to be as transparent as possible and have an open conversation with private, not-for-profit and public sectors about what constitutes appropriate oversight of AI. That's more in Mr. Benay's wood house than mine.

**Mr. Raj Saini:** I know that the comparator that we use to judge our abilities going forward is Estonia, but Estonia is only 1.3 million people. It has 4 million hectares of land, half of which is forest, so the country is not terribly big, plus it has a unitary form of government.

One thing Norway has done is to start a mailbox for every citizen, with each of them having a designated mailbox where information is delivered to them. My concern is that, in going forward as an advanced country, an advanced economy, you have different government departments that already have legacy systems. How are we going to bring everything together so that the information is accessible in one touch, but also make sure that we are able to communicate in the interim with the public?

● (1555)

**Mr. Alex Benay:** It's a very good question.

Estonia is one example. You've raised some important points of difference. We also have provincial and some pretty significant municipalities across the country. We are not Estonia. It's important both culturally and legally speaking to recognize that. However, there are a lot of things we've learned from the Estonians. We've learned how to share data in a secure way. We've learned that they can deliver digital services and increase privacy at the same time. They've shown the world that this can be done. For us it's a question of scale, and it is a question of technical debt and legacy, to your point.

We've put in place some governance measures over the last year wherein we are asking departments to come and have conversations about their solutions earlier through a mandated enterprise architecture review board where every functional group is represented at the table, from security to privacy to applications to service delivery, to make sure that we're having the right conversations and not doubling down on legacy systems because that's the easier thing to do, and that we're having the conversations on moving to cloud, on protecting citizens' data, on artificial intelligence and on new governance challenges that some of these technologies pose.

We've systematically been bringing the conversation closer to investment decisions, because that's where some of the decisions are made, and we often live with the repercussions.

**Mr. Raj Saini:** I have one final question. This is more of a theoretical question, because as you know, Canada is part of the D9 group that's moving towards digital government.

With the [*Inaudible—Editor*] and looking at some of the countries, we have free trade agreements with a lot of them, and there's obviously going to be information going back and forth as a result. Has there been any discussion of one standard that everyone could abide by for the transmission of information?

If there's an entity here that wants to do business or public procurement in another country, they would be able to do that, knowing there's one system, a certain level of privacy, a certain level of architecture and a certain level of technology. Has there been any discussion on that?

**Mr. Alex Benay:** We took a first step towards that. The short answer is “not yet”.

It is a group that is fairly new, but we did take a first step towards that when Canada led a joint declaration on responsible artificial intelligence usage across all of the countries. That now means we can go back into our respective countries and work with our industry to make sure that we start respecting some of these rules. The next step will be to bring corporations into the D9 conversations and start working together.

The answer is that it's a beginning. It's not necessarily as mature as you would have described.

**Mr. Raj Saini:** Thank you.

**The Chair:** Mr. Snow, do you have something to add?

**Mr. Aaron Snow:** Not on the D9, but Canada is in a treaty with nations in Europe that requires us and all those nations to provide a single source of—

**Mr. Raj Saini:** Do you mean the GDPR? Is that what you're referring to?

**Mr. Aaron Snow:** No.

We're required to provide a single source of procurement opportunities across federal, provincial and local governments, academic and health institutions by, I believe, 2022. This is way outside my wheelhouse. We've been discussing and working on that with PSPC. They would be the right folks to talk to about that.

**The Chair:** Thank you.

Next up, for seven minutes, is Mr. Kent.

**Hon. Peter Kent (Thornhill, CPC):** Thanks, Chair, and thanks to all of you for attending today.

Mr. Benay, I'd like to pick up on your remarks with regard to the differences between Estonia and Canada as a wonderful federation.

There are still some who believe that Estonia's digital government, which was, in effect, created through democratic imposition on a compliant population after the breakup of the Soviet Union, is still a glittering digital city on the hill that Canada should try to emulate. I wonder if you could speak to just how realistic that would be, even if limited only to federal government departments and agencies. How realistic is achieving that, or could it be achieved in Canada in, let's say, a decade?

**Mr. Alex Benay:** I'll answer from a technological perspective, and by that I mean there's a lot we can learn from what the Estonians have done with their X-Road, their data-sharing platform. We brought some of the founders into Canada twice over the last year to start re-creating our own similar platform, but from the Canadian perspective. We have provinces and large municipalities; we are not Estonia. From that perspective, we've learned a lot.

We've also learned a lot around the need to continuously update laws, for example, in the context of a digital age. We've learned the fact that they do data governance very well. They decree that an organization is the holder of that piece of data, and that becomes very rigidly implemented.

There are a lot of things, regardless of scale of countries, values and background, that we should look to and we actually are looking to. We've learned a lot from them.

We've also learned a lot from our other D9 partners. For example, Portugal has a very good digital identification system that might actually be closer to Canadian systems than those in Estonia.

We do look to Estonia on technological leadership, but in some cases, we're seen as leading in values and ethics around ethical AI and responsible AI usage, so they're learning from us. It has been a very good relationship that way.

● (1600)

**Hon. Peter Kent:** Mr. O'Brien, could you speak to that?

**Mr. John O'Brien (Director, Security and Engineering Reliability, Canadian Digital Service, Treasury Board Secretariat):** I'm not super familiar with X-Road, the technology itself.

That said, if you were to approach it from the pure functionality that it offers, the idea of verifiable audit logs is, in itself, a function that I would suggest we'd want to have in any system we put out.

The second factor on that is the concept of having citizens be able to see when government officials access their data. That transparency is the core element we need to build into any system we build in the future.

If we can articulate those things quite clearly to Canadians, it will not be a very difficult thing to sell.

**Hon. Peter Kent:** Mr. Benay, I was gently amused, positively amused, by the following reference in your sentence: “Canadians don't need to know how government is organized or the intricacies of federal, provincial and territorial jurisdictions when they try to access services.” It reminded me generationally of when Réal Caouette, the Quebec politician, tried to justify Social Credit economic policy by saying that you don't have to understand how a carburetor works if when you step on the gas the car goes. It brings me to procurement. You talked about the investment and design stage of government services, programs and operations, and here the Phoenix system comes to mind, where apparently those who were procuring the system decided to cut costs, acquisition costs, by eliminating some of the services the manufacturer, the vendor, was actually recommending to government. We've seen the result of that today.

My question has to do with perhaps how citizens don't have to know the intricacies, but I think we have a shortcoming with those in charge of procurement within government. I wonder if you could comment on that.

**Mr. Alex Benay:** Certainly. I'll comment on both aspects.

The reason that we're trying to design—and this gets back to Mr. Snow's point—this in a way that we don't impose the structures of government on service delivery to citizens is that we just want them to see us as the Government of Canada and to make it as seamless as possible for them to access services. We do have structures, we do have laws, we do have processes within the Government of Canada, but with technology we may actually be able to represent our existence and our delivery of those services in a very different and much more intuitive way to citizens. That's what we mean by those comments: how do we streamline things for citizens? It's not what we think they want, but from talking to them, which goes some of Aaron's points, knowing what they want.

In light of that, what we've been able to do with, for example, the next generation system of Phoenix is to take a good hard look at the lessons learned that were produced by the OAG, by the Goss Gilroy report, by committee reports, and apply those lessons so that we could say they were lessons learned in the replacement of Phoenix.

For example, in the procurement exercise we're currently running, we've had user expos conducted across the entire country where we're putting the actual competing technologies that are going through this process in the hands of users for them to test and give us their comments, putting accessibility experts in a room and testing things. By putting the user at the centre of it, we've been able to change the decision mechanism from a process as Aaron was outlining it, to what the HR administrator or pay administrator, the everyday public servant, will need. We've actually embedded them in the procurement process in a way that's not been done before.

So we are able to show that we can actually move some of these issues on procurement in a very [*Inaudible-Editor*], where we have included everybody in the process from the beginning, including the Parliamentary Budget Officer, who sits in on our meetings once in a while, to unions and heads of bargaining agreement agents. It's been a very inclusive tent; it's been a very large tent. We have “privacy by design” principles being applied to the procurement process as well. And all of our documents, for the most part, as long they don't interfere with the procurement process, are publicly available on a portal so that people can see our transition as we're going through this and feed into the process. We're showing that we can do the thing differently. It's our first step into this space and we'll see how this goes.

● (1605)

**Hon. Peter Kent:** Just to my final part of my question, does the expertise exist in your agency to recognize that if a vendor or supplier of a certain technology says you need the whole package at the full price, because if you buy less there are going to be problems, you have the expertise to accept or analyze what that provider is telling you?

**Mr. Alex Benay:** At this point we do, and if we don't, we go get it, and we recognize when we don't. But, again, the way we've designed this process has been iterating with the vendors. We're talking to them as we're going through the process, which is slightly different from a traditional procurement process, where we talk through binders and responses and 200- and 300-page RFPs. In this case we're working with them as we're designing the process, at every gate, because we've gated our entire process. If we know from talking to them that we have some gaps, we will go get them.

You heard me say in my earlier statement that it's very hard to be an expert in absolutely everything in digital. I think if we start with that premise, we'll make sure we have the right people around the table when we know there's a gap.

**The Chair:** Thank you, Mr. Kent.

Next up for seven minutes, we have Mr. Angus.

Go ahead.

**Mr. Charlie Angus (Timmins—James Bay, NDP):** Thank you so much for your presence today. This is a fascinating discussion. When I was a much younger and much better looking man, I sat on a committee that did government operations, and much of what we're talking about I think is under the purview of government operations. We need to focus on what is the purview of this committee, which is issues of the ethical rights of citizens and privacy rights. Therefore, I'm going to mostly focus on that.

Mr. Snow, Canada has suffered endless numbers of security attacks against government servers, in particular government agencies, over the years. These tended to be by state actors. Are you seeing a change between security threats from state actors or from individual actors and gangs who are trying to access information?

**Mr. Aaron Snow:** CDS works with a limited number of partner departments at a time. We don't have that sort of horizontal data. We aren't privy to the kinds of threats that various departments are seeing in the back-end systems that we don't touch.

That's probably not a question for me.

**Mr. Charlie Angus:** Mr. Benay.

**Mr. Alex Benay:** I don't have the data readily available for state actor versus individual actors. At this point, we're trying to operate with the idea that an attack could come from someone in a basement, all the way to a state actor and everything in-between. We have people who are knocking on the front door of government systems hundreds of thousands of times a day.

We've been able to centralize some of our infrastructure with Shared Services Canada in order to build a moat around this. We've created a new national cybersecurity centre that was launched this year. It's trying to bring the private and public sectors together as well, because an attack on one sector can often bleed into another. Critical infrastructure is an example.

When we're designing our services, we have to bake in security from the beginning. You heard me speak about the architecture review board that we created. The security lens is applied for every major digital project moving forward in the government and over the last 12 months.

**Mr. Charlie Angus:** I remember when the fax machine was cutting-edge technology. Among the first people to use this cutting-edge technology were the scammers running the Nigerian 419 scam. You had to do a lot of work to get all of those faxes out there and you probably didn't get a lot of pickup. Then the Internet came along and the ability to hit millions increased.

When you have one point of contact of information you can only be so successful. When you have two or three points of information about a person you can become very successful.

In my office, I deal—as I'm sure my colleagues do—with people who have been or are being victimized by these scams all the time. These scams are much more sophisticated now as the technological changes happen.

My question is in terms of government, financial and medical information. Protecting that information is vital because that's where the non-government actors are going and what they're looking to use. What assurances do we have that as we put more of our private information into one big system, we're actually being protected?

**Mr. Alex Benay:** I'll start, and you may want to jump in.

Just to be very clear, we're not advocating putting our government information in one big system, one big data lake or one big pool of information.

For example, the Canada Revenue Agency is responsible for the business number in our policies. It doesn't mean that the information is not located in other places as well. We're not advocating for a central system.

I think that—

● (1610)

**Mr. Charlie Angus:** When we have cases of citizens' information being improperly accessed in the Canada Revenue Agency, are you involved in the review of how that goes down, or is that siloed under CRA, saying that those were just a few bad apples in the operation? If we're putting more information out there, do you actually get to be part of these conversations about the misuse of that personal information within government services?

**Mr. Alex Benay:** Yes. For privacy breaches, luckily Ruth's team is responsible for overseeing and being involved in these discussions. On the cyber front, we have another executive director who works closely with Shared Services Canada and with CSEC on major incidents. They do make their way into the office of the CIO on a daily basis.

Ruth, I don't know if you want to comment on privacy breaches and the process.

**Ms. Ruth Naylor (Executive Director, Information and Privacy Policy Division, Chief Information Officer Branch, Treasury Board Secretariat):** Yes, I can speak to that a little bit.

Institutions have a responsibility or an obligation under our Treasury Board policies to report privacy breaches that are material in nature, both to the Office of the Privacy Commissioner and to TBS. We work quite closely with the Office of the Privacy Commissioner to compare notes on those reports.

At TBS, we make a range of tools available to institutions to support them to identify, manage and do the reporting aspect of this. We work with the OPC and follow up with institutions where that's warranted.

**Mr. Charlie Angus:** I find that very impressive.

I studied privacy breaches in the previous Parliament when that was my beat. My concern is how often departments decided not to tell the Privacy Commissioner. Maybe 10% of the time they came forward, and they said that they didn't think it was big or that it was a problem.

People don't want to make it look like they really blew it. When you have hundreds of breaches, it doesn't look good for the department.

How do we know that all the breaches are being reported? That was the Privacy Commissioner's frustration before. It should be the Privacy Commissioner who decides whether or not the breach is significant, not the department.

**Mr. Alex Benay:** Yes, from a cultural perspective you heard my colleague Aaron mention the fact that we have to get to a place where escalating issues are not necessarily seen as a negative, but a positive. There have been some good steps taken toward that throughout the public service. We've had a lot of support from senior government officials on the transparency required to raise some of these issues, and we're seeing deputy ministers, ADMs, and DGs asking for an update on the red status of either projects or breaches.

Culturally speaking it's going to continue to be a work in progress. There's some good momentum on that side in the public service from a transparency perspective, but Ruth probably has some details on the two-year action plan we're developing in partnership with the departments and the Privacy Commissioner's office.

**Ms. Ruth Naylor:** We had the benefit of some recommendations from the Privacy Commissioner in his last annual report on exactly this issue and that office's concerns about the varying numbers of breaches reported. Often, the institutions up that decision about what to do and what not to do. I think institutions are working in good faith on that, but we want to be doing some work over the next two years.

We're developing a two-year action plan. We've shared it with the Office of the Privacy Commissioner, because we want their input before it's finalized, and we'll be working in partnership with them to deploy it.

It will be focusing on increasing awareness about the nature of personal information, what a breach is and how to report a breach. Also, at the recommendation of the Office of the Privacy Commissioner, we're focusing a lot of those efforts on the IT and security community, because they are the people on the front lines when there could be a compromise or information could be lost. Therefore, we want to make sure they have the instinct to say that personal information was involved in this.

We have a small team working on this in partnership with government institutions. We're hoping we'll be able to make a difference on that front over the course of the next two years.

Thank you.

**The Chair:** Thank you, Mr. Angus.

Next up for seven minutes is Mr. Erskine-Smith.

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

Thank you all for being here.

While I don't think Estonia is a perfect solution, there are some perfect solutions within Estonia that we have to learn from.

Digital ID, I think, is a critical aspect of moving toward more digital government. X-Road is another aspect, and I'm glad you're doing work on that front. Then there's obviously a transparency component where, in their law, when a public official accesses personal information, it's transparent to the citizen.

I want to walk through the first two pieces, at the very least, which are more under your purview.

You mentioned with respect to digital ID, Mr. Benay, that there is Sign In Canada. Maybe you could give me a bit more background on when that started, where we are at with it and what we are looking at doing moving forward.

● (1615)

**Mr. Alex Benay:** Yes. Sign In Canada itself is in its infancy. In the last few years we have been focused on the rules framework underneath it instead of the technology.

We have been working on the pan-Canadian trust framework with the provinces, NGOs, non-profits and the corporate sector as well. It's essentially a set of rules that we all agree to abide by to respect each other's identities.

If a province abides by the pan-Canadian trust framework, it should be good enough for the federal government and for a bank. It's more of a federated model. It matches the governance framework of the country more.

**Mr. Nathaniel Erskine-Smith:** If I'm a citizen and I want to log into the CRA or EI or to renew my driver's licence at the provincial level, I don't want all of these passwords. I don't want to have to remember that my CRA password and my user name are different. Then I have to store them in a separate password folder. I want simplicity as a citizen. What does it look like from a citizen perspective?

**Mr. Alex Benay:** I fall victim to them myself as well, and I have a vested interest in ensuring that these things don't happen.

Sign In Canada will essentially permit you to choose the “no wrong door” approach to services, accessing federal services from a province or a territory, or vice versa, and possibly from your bank as well. We do have the security regime to put this in place, but we didn't have the rules framework in place.

Sign In Canada means that you could have access to ESDC services from CRA. Also, we are in active discussions on possible pilots and projects with the provinces, where we would give federal services through the provincial ID system as well.

It's very different from the Estonian model, which is a singular approach to it. We are taking more of a “no wrong door” approach to services, as long as a rules-based approach is followed.

**Mr. Nathaniel Erskine-Smith:** Does your office, in consultation with the OPC, have a list of potential privacy concerns and how to address them?

**Mr. Alex Benay:** Yes. As part of the new governance that we put in place roughly 18 months ago when we changed the Financial Administration Act to create standards, we changed the governance process around the architecture review board. It means that any one of these kinds of major projects has to go through this review board, where privacy is looked at.

Another part of this may possibly be legislative impediments as far as data-sharing is concerned, which is another tombstone piece of work that we have to do. We have been in conversations with the Privacy Commissioner's office on those, for example, as well.

I suspect that the dialogue will continue to increase as we do more and more digital services between my office and the Office of the Privacy Commissioner.

**Mr. Nathaniel Erskine-Smith:** Is there any written analysis that can be shared with this committee with respect to any privacy implications of digital ID?

**Mr. Alex Benay:** We can certainly make any of that documentation available. We've also started a legislative review process, so we can look into—

**Mr. Nathaniel Erskine-Smith:** That would be appreciated. It would certainly be helpful, I think, for our committee's work.

You mentioned X-Road and said that we're moving down that path as well. Presumably, that's in its infancy, too, but maybe you could give me an update as to where we are and what the road ahead looks like.

**Mr. Alex Benay:** In this case, it's a little further ahead than the identification piece. Our Canadian digital exchange platform—DXP for short—is a series of tools, from a messaging service where we can share the data to an open-source API store where federal government services will be able to create an API for third parties to gain access to unclassified data for now. We're walking before we're running. As we're designing this, I'd say that we've completed about 50% of the build. The challenges are in finding real “live-use” cases that have minimal risk and in ensuring that we are using unclassified data first, rather than citizen data. We will make sure that we walk before we run. In this case, we brought in the Estonians who had designed X-Road, and we started redesigning X-Road in the context of Canada's laws, regulations and other things.

The beauty with this system, if it proceeds down this road, is that we will be able to bake in accessibility, privacy and security. We'll also be able to determine how we move data around in the Government of Canada, based on a core set of principles.

**Mr. Nathaniel Erskine-Smith:** When you say you're going to walk before you run, running in government is perhaps optimistic. However, in terms of the first steps, when I look at Estonia and at first steps, it strikes me that the basic information in the population register, which is constant information that is drawn on by other departments—it's my name, my email address, my home address, my phone number...I keep telling the government this and I don't want to do that over and over again, wasting my time and presumably someone else's time at the department. Is that the kind of walking we're talking about, this basic information, or is that not where we're at? Are we even earlier on?

**Mr. Alex Benay:** I would say the theory you've described is accurate. Where we choose to apply it may not be with personal information first. For example, the business number is something that we've agreed on. There is a central registry for a business number, so we may want to start there. We may want to start with unclassified...well, no, I promise you we will also start with unclassified information first. We could crawl before walking.

● (1620)

**Mr. Nathaniel Erskine-Smith:** I was going to say that it sounds like crawling, not walking.

You've both laid out the paths you're proceeding on, and it seems like a lot of good work is being done quite quickly. Are there specific recommendations that either of you think we ought to make to the government with respect to improving digital government services and respecting Canadians' privacy?

**Mr. Alex Benay:** I think there are a few things. I do think that we are gradually—and possibly not quickly enough—applying the lessons we've learned from some of our major failures. You heard me speak to the NextGen process. I think that the culture shift is going to be the big change, and it's not necessarily the culture of the public sector. It's simply the fact that things are changing so quickly. In some cases, things are happening, and it's not necessarily in our control or something that we didn't see happen, because the pace of change in the outside world is very quick. That could mean companies automating themselves, with our not necessarily having a say in it and all of a sudden it's a service that we use. That is a major risk.

I think our biggest challenge, or at least the thing that we have to keep an eye on, is the pace of change, and therefore our laws and some of our regulations. The dialogue is there at a technical level across all levels of government. The biggest challenge.... Some of the countries that are doing quite well are the ones that are adjusting some of their frameworks more rapidly, as rapidly as the change in technology itself.

We're learning from that. We have a good opportunity with the digital line to see how some of these smaller countries are being a bit more nimble. We are also seeing how we could apply that in Canada. That is probably one of the biggest lessons we've learned up to now. Whether that means protecting privacy or developing regulations for economic growth, we're seeing that those countries that are able to react faster are getting a lot of benefit, both from a citizen protection perspective and from an economic growth perspective.

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

Next up, we have monsieur Gourde for five minutes.

[*Translation*]

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

Thank you to the witnesses for being here today.

I'd like to know what Canada's ideal digital system would look like, in your eyes. I'm sure you have to work within certain parameters, but if you could do things your way, taking into account your expertise, what would be the ideal system you would deliver to Canadians if you could?

**Mr. Alex Benay:** What we would like to deliver is a system without any closed doors, so to speak, a system that provides digital services to Canadians on the IT platform of their choice or in person at a Service Canada office. They would be able to obtain a service at a Service Canada desk or through their Apple or Samsung smart watch, for instance. Canadians would have a multitude of choices enabled by a system developed with their help. The system would be designed so that all privacy and data protection requirements and access to information standards were built in from the outset. All too often, these fundamental principles are unfortunately overlooked or relegated to the end of the implementation process. Every Canadian would have access to the services they need via their preferred gateway. Finally, the ideal system would support interoperability across different levels of government, in contrast with a single system that would have to be tested in 43 federal departments and some 20 provincial ministries.

[*English*]

**Mr. Aaron Snow:** There are two points I would be looking for.

Number one is that in my ideal digital world, the system is fully transparent. You understand how the service is being delivered and what the steps are. When government asks for your information and when government provides you with the benefit, there is a clear, plain-language map of how it all works.

The second point I would make, to Mr. Benay's point on the previous question, is that systems that are flexible and adaptable are the systems that will keep up with whatever changes. It was only 11 and a half or 12 years ago that the first iPhone appeared. Twelve years from now, the way we want to interact with digital services and with government will be something that we are not imagining yet.

As a systems nerd, I want to know that my government is ready to adapt to whatever comes next.

● (1625)

[*Translation*]

**Mr. Jacques Gourde:** Are we behind our neighbours to the south when it comes to providing digital services to citizens, or do we fare well?

[*English*]

**Mr. Aaron Snow:** I think the U.S. government shares many of the same obstacles that this government and other governments at this scale face. There are many sides to that question. I'm sure that in some places the U.S. government is a little further ahead and in some a little further behind.

**Mr. Alex Benay:** I am happy to jump in.

[*Translation*]

A few weeks ago, in Washington, I met with my American counterpart, Suzette Kent.

I'll repeat what Mr. Snow said. The Americans have a better grasp of certain elements, particularly cloud computing, an area where they do business with U.S. companies, and that may give them a data protection advantage.

We, however, have a leg-up when it comes to AI governance. We are in the midst of developing multiple directives on an open basis, directives other countries are using in their approaches to AI governance. Given all the interest this has generated, our two countries have been in constant communication over the past 12 months.

**Mr. Jacques Gourde:** What percentage of Canadians do not want to receive services digitally? We aren't able to convince everyone; probably 10% to 20% of the population is still somewhat resistant to the idea. The in-person service delivery model people are used to is being replaced. Robots and AI are being used to deliver an increasing number of services in the digital age. How are we going to deliver those services to resistant Canadians?

**Mr. Alex Benay:** Our strategy is to make sure that every Canadian is able to access services. We recognize that it's perfectly acceptable if someone opts for in-person service at a Service Canada office. I should point out that TBS has begun gauging public opinion on digital service delivery. We've learned that two out of three Canadians are comfortable with federal government departments sharing their personal information to improve service quality.

As you mentioned, the number of people who want access to digital services is on the rise, but I don't see us doing away with in-person delivery for important services. As I see it, our service strategy must adhere to a fundamental principle: no one should fall through the cracks. Trust will likely play a role as well. We'll have to show people that we can meet our commitments and that they can have confidence in the system—hence the importance of being transparent about the services we will provide and the policies we develop.

**Mr. Jacques Gourde:** I have one last question for you.

Will MPs' offices be integrated into the digital service delivery model? We are on the front line of service to Canadians, after all. When constituents encounter problems, they call our office, so we reach out to departments to see how we can help the person get the service they need. It adds to the workload of office staff, and MPs don't always have the resources for that.

Even when they're advised to contact Service Canada, people prefer to call their MP's office for help, rather than contact the department in question. It's a double-edged sword for us, being on the front lines of service delivery to constituents.

Do you intend to build MPs' offices into your digital service solution so we can help one another?

[*English*]

**The Chair:** Give just a very short answer.

[*Translation*]

**Mr. Alex Benay:** That's a question I would have to put to Service Canada. We'll take it under advisement, as we would any feedback from Canadians and MPs' offices. We want to make sure our services better target the right people to prevent those kinds of situations.

[*English*]

**The Chair:** Thank you.

We're way past time.

[*Translation*]

**Mr. Jacques Gourde:** Someone else will give you a chance to answer.

[*English*]

**The Chair:** Maybe you can answer later on. We have a fair amount of time.

Next up, for five minutes, is Ms. Vandenbeld.

**Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.):** I want to pick up first of all on something that you said, Mr. Benay. It struck me. You said that Canada is leading on ethical AI.

Can you explain what you mean by that?

**Mr. Alex Benay:** Yes. For the past 14 months we've been working on direction and policy for the way government departments use automated services, moving forward, because this is something we're seeing increase.

You heard me say that PSPC has done a procurement action for creating an AI vendors catalogue. We now have 74 companies that have been registered in this vendors catalogue for the the last few weeks. We've been providing policy direction, working fully in the open, putting our policy instruments and our documents and our directives on GitHub and Google Docs for the world to see. We've collaborated with MIT and Oxford and other universities.

It's been a very open and transparent process in creating a tool set that is called an algorithmic impact assessment. You would be familiar with something called a privacy impact assessment, when we're looking at privacy; we're looking to develop something similar, as a prevention tool, for algorithms that will identify to the departments the level of risk. Automating a chatbot that tells you through the NCC website whether the skating rink is open is probably a lower-risk step than automating our borders, for example, or our immigration systems.

We've been developing this tool fully in the open. We've had countries such as Mexico start to use the algorithmic impact assessment already, and we have other countries, such as Portugal and others we're working together with—the “digital nine”—use some of the tools we've been developing. This creates an international body of knowledge that up until now just did not exist.

● (1630)

**Ms. Anita Vandenbeld:** One thing I wanted to go into a little bit is the differing expectations that various Canadians have. Obviously there are elderly Canadians who are less comfortable with going online, and then there are others who, as you mentioned, expect that it's going to be just as easy to deal with government as it is to deal with Amazon or any other app they might be downloading.

When you look at those different expectations, you also find a huge difference in terms of how comfortable people are in giving their information. I still know people who won't do online banking because they don't trust it.

How do you develop an all-of-government approach when you have completely different expectations among different parts of the public?

**Mr. Aaron Snow:** I'd say that in part—and this is actually part of the answer to the previous question as well—fear or confidence in a system is in part a function of how easy it is to use and understand and how transparent the system is about how it is dealing with you and with your information.

We understand that digital is, generally speaking, a good, efficient means to provide services at scale at a lower cost. As Mr. Benay noted, we would never want to close out other forms of service; we want to make sure that we remain multi-channel. But the extent to which adoption and digital happens or does not happen has everything to do with the type of experience people have, which is why it is so important to be working with those people at every step of the process.

**Mr. Alex Benay:** Let me add as well a few statistics.

According to Statistics Canada, in the 65-plus age group about 80% of homes are Internet-connected, which is not a great but not a bad statistic. I think the question is—and this will relate to what Aaron was saying—if we can make the service seamless, transparent and easy to use, we'll go a long way in shifting the behaviour of the teams and the service model that they choose and want.

We've seen in countries such as Uruguay who have committed to having 100% of their services become 100% digital for 100% of their citizens by the end of this calendar year that they make an effort to educate the population as well, both from a data privacy perspective but also from a service delivery perspective on how to engage with government.

Those are things we'll have to do to make sure that we don't leave anyone behind.

**Ms. Anita Vandenbeld:** Going to the people who will be implementing this, the public servants, both of you have spoken about things like culture change.

Mr. Snow, I think you said that this is more about change management than it is about technology.

I noted that you said there's a public sector digital academy. You have mechanisms such as this talent cloud to bring talent in for short periods. In terms of the culture shift that is going to be required by the public service, how are you making sure that it is in place, not just the technology but the people?

**Mr. Aaron Snow:** CDS's answer to that question is one partner-department at a time. Culture change is not usually something that happens effectively with a single directive that everybody should just start behaving and thinking differently all at once.

There are pretty clear models of how adoption of new technologies in the public culture occurs. It looks like a bell curve or a Rogers curve. Early adopters will try anything and get started. If they're comfortable, their friends and their networks start to hear about it and more people take it up. Then, at the very end, after mass adoption, there are a few folks like my father who took 15 years to start using email.

It is slow. One of the ways we measure the success of a project that we do with partner departments is that as we're wrapping up or are in the midst of that project, we see if the department is starting to use some of the same methods, practices and tools that we brought in, possibly for the first time there, on other unrelated projects. If we see that, we know that we're succeeding because those notions are starting to take root and spread in the department.

● (1635)

**The Chair:** The time's up.

Next up for five minutes is Mr. Kent.

**Hon. Peter Kent:** Thanks, Chair.

I have a question for Mr. O'Brien to start off with.

We know that federal government departments have been hacked successfully, deeply penetrated any number of times, in the last decade by certain foreign players. I think the cybersecurity of the various repositories in a digital government like the Estonian model —interconnected but separate repositories of information—would be essential to assure Canadians of the security of their privacy.

Last month in a speech, Neil Parmenter, the president of the Canadian Bankers Association, talked about all of the banks' interest in developing digital ID across the country, in every sector, to enable the banks to better provide services to their customers. He also suggested that because of the way banks today protect access to client security, they should perhaps play an integral role in any future Canadian digital government. What would your thoughts be on that?

**Mr. John O'Brien:** I guess I'll start by saying, I did work for CSE for about 12 years. I was in the cyber defence branch, so I was likely involved in these intrusions you spoke about, in some respect. That said, I no longer work for CSE and I don't want to speak on their behalf, but I'll kind of wave my hand a little bit.

You're right. There are actors around the world, both at a nation-state level and from a script kiddie—people just trying to break things—who are constantly attacking systems around the world. We're not really special—well, maybe we are special—but I think one of the challenges that a lot of organizations have is that when they get compromised, they don't really want to go and tell people because that creates negative press for them.

Essentially, what happens is that everyone ends up suffering in silence. Part of the work I did before I left CSE was to take one of the security tools that we built and open-source it, to release it to the security community so that we could actually bring up that security bar across the industry. From a transparency perspective, that's where we sit in terms of the security space.

To kind of pivot on to your question about the banks, I guess the point to that would be, I don't actually know how banks secure their systems. For me to say that I think they are in the best position to protect Canadian security would be kind of out of place. I would love it if they would be more open and honest about that, just like I would love it if Google and Facebook and all these companies would be very open and honest about how they do security things. At that point, we could all collectively bring up our security postures, and I think Canadian citizens would be a lot more trusting of all of the parts.

**Hon. Peter Kent:** Mr. Benay, have you had any interaction with the Canadian Bankers Association? They talk about the multiple levels of protection they have to protect clients' personal data. They seem to think that they would be in the forefront of those in the private sector who may offer to participate in government digital services.

**Mr. Alex Benay:** I haven't had any interaction directly with the bankers' association, but I can say that the banks have been engaged in the pan-Canadian trust framework, for example, so this isn't something that is necessarily new to them.

We have architecture conversations with the banks fairly regularly on some of their investments, including their sign-in protocols, and ours, and making sure that we're working together. We also have, I would suspect increasingly, at least the objective of the new Canadian Centre for Cyber Security, to continue interacting cross-sector, because often an attack on a bank could lead to something happening in the CRA and other places. I can tell you that the focus on cross-sector collaboration is something that Public Safety Canada is examining and CSEC and other colleagues, as we're going through this new era of cybercrime, frankly.

**Hon. Peter Kent:** Thank you.

**The Chair:** Next up for five minutes is Madam Fortier, and then it will be Mr. Angus.

[*Translation*]

**Mrs. Mona Fortier (Ottawa—Vanier, Lib.):** Thank you, Mr. Chair.

Good afternoon everyone.

I'd like to thank the witnesses for being with us today. Many of my questions have already been asked, but I still have a few left.

Earlier, we talked about the Privacy Act and other legislation that protects people's personal information. I realize that the legislation will require some amending as society embarks on the digital path and the government adopts digital service delivery. I've been an MP for two years, so I understand that that type of legislative review takes a long time.

Given our legislative framework, what do you do when you realize that certain amendments are necessary in order to protect Canadians?

● (1640)

**Mr. Alex Benay:** You raise some very good points. The current Privacy Act has been in force since 1983, well before the Internet era. The discussion we're having today attests to the big changes on the way that will affect society. The act applies to 265 institutions. I mention that not to make excuses, but simply to highlight how colossal the undertaking is.

When we encounter an issue, we work closely with the Department of Justice. TBS is responsible for building an inventory of situations that arise, and our discussions with the Department of Justice and other stakeholders are ongoing. The enterprise architecture review board began cataloguing issues and key points that have come to our attention.

Naturally, it takes time. Take, for example, Europe. The EU General Data Protection Regulation, or GDPR, wasn't developed in a few years. It takes time to come up with those kinds of rules, which will likely require regular review, as Mr. Snow pointed out. Many of our private sector partners are currently putting new services in place. Obviously, it's an ever-evolving challenge. We also have to work closely with our partners at Innovation, Science and Economic Development Canada, since they are the ones in charge of enforcing the Personal Information Protection and Electronic Documents Act, or PIPEDA, in the private sector.

There is no doubt that the digital ecosystem is quite complex, so we want to be sure we take the time we need to analyze all of the issues reported to us. The next step will be to engage with Canadians about their private data.

**Mrs. Mona Fortier:** As you go down this critical path, have you identified any measures we should take a closer look at now, in light of what's coming? When or how often should we expect the eventual reviews?

**Mr. Alex Benay:** In the timetable we gave ourselves, we set aside two years to review certain legislation that might hinder information sharing. We wanted to ascertain whether an issue was real or merely just a rumour, so after examining 11 departments, we identified 187 amendments to legislation that could affect the sharing of information.

What I just said is also based on the premise that information sharing is a problem, real or imagined, but we wanted to validate it. With some of the technologies we talked about earlier, namely X-Road in Estonia, we'll be able to validate some of the notions we have. We'll continue working with our partners at Justice Canada and Innovation, Science and Economic Development Canada to make sure we have the complete picture. Right now, we are thinking it all through.

**Mrs. Mona Fortier:** Did you have something to add, Mr. Snow?

[*English*]

**Mr. Aaron Snow:** I can refer to my experience in the United States. Legislation, being the slowest and most encumbered of all routes to the solutions, can often result in unintended consequences. We saw that happen in several cases, so I would exhort all of us to look for the smallest and fastest unit of governance when possible to avoid going into the process of creating and amending laws.

[*Translation*]

**Mrs. Mona Fortier:** Thank you.

[*English*]

Do I still have time?

**The Chair:** Thirty seconds.

[*Translation*]

**Mrs. Mona Fortier:** If you think we should look to models adopted in other countries—we talked about Estonia, among others—we'd be curious to know which ones so we could consider other best practices in the course of our study.

**Mr. Alex Benay:** It's important not to dissociate issues related to data protection, AI and automation. For instance, we're doing a lot of work with France right now on issues around ethics, data management, privacy and automation, so I encourage you to explore those elements.

● (1645)

**Mrs. Mona Fortier:** Thank you.

[*English*]

**The Chair:** Mr. Angus, for three minutes.

**Mr. Charlie Angus:** I find the more I stay in politics the more of a digital atheist I become. I used to be a digital believer in the peaceable kingdom that we were going to create.

I represent a rural riding that's bigger than Great Britain. Many of my communities have no roads, and where the Trans-Canada Highway goes through my riding, I have businesses that can't get Internet services on the Trans-Canada Highway. In my little communities, the libraries are full of kids after school, not because they are reading books but because they don't have Internet at home.

To follow-up on my colleague, we are the face of government for them, because they get told to go online, but what they are dealing with is a world that is increasingly like Kafka in a world of smart phones, because what government expects from people—your child tax benefits, your EI, your disability claims—are becoming increasingly complicated. Having a new interface doesn't change that. In fact, it disenfranchises people, because they become more frustrated, so they end up in our offices all the time, and we're having to go through and do the forms.

It's not your responsibility to deal with the inanity of government, the paper and the evidence, but when you talk about making it easier for people, what I see as the question is that it's great you have all the bells and whistles on the service, but if they can't access a way to get through that, then they become even more disenfranchised than if they were just told to mail it.

**Mr. Aaron Snow:** Rare is the project we work on that does not delve into service design, and not just digital design. In fact, in every product team we have, in addition to our research and design, and our engineers, there's a member of our policy team on that team as well for exactly this reason. Service design spans across. To communities like yours where connectivity is at issue and where complexity is to grow, we design with those users in mind. We go to those people.

For instance, this isn't necessarily an example about disconnected users, but the work we did for citizenship exam rescheduling for folks who were trying to change citizenship, we knew that some subset of the people who would need to reschedule citizenship exams would be doing so from their phones, because it's the only Internet access they had. Those connections might be intermittent, so that particular service was designed to work even when their connection goes in and out. It was designed to work on a phone, computer, gaming console, on any access they had, so that whatever level of access they had, it was going to be an experience they were not going to suffer through.

Every service is different. Every service has different requirements, different needs based on who's consuming the services, but that's why it's so important and why it's the first of the digital standards to put your users at the centre of the design experience, not just digitally but for the entire service design.

**The Chair:** Thank you, everybody.

How many people still have questions?

We're going to have rounds of seven minutes for each party, and if there are further questions we'll take them too. Just let me know. We'll start with the Liberals.

Nathaniel, you have seven minutes.

Then we have the Conservatives and then the NDP each for seven minutes. Go ahead.

**Mr. Nathaniel Erskine-Smith:** Yes, but Charlie Angus with one question takes at least seven.

**Some hon. members:** Oh, oh!

**Mr. Nathaniel Erskine-Smith:** Before getting into some additional questions, just to clarify this so it's clear to me what we will get back in response to what I asked previously. With the federated, trusted digital ID there's a privacy analysis and whatever you have with respect to a privacy analysis, the committee will get.

In answer to my last question and recommendations you would make, Mr. Benay, you suggested that the biggest challenge you face is the need to adjust frameworks rapidly. Mr. Snow, you were nodding your head when Mr. Benay said that. You used the word "nimble". You acknowledged in your opening remarks that the Office of the Privacy Commissioner has mentioned reticence with respect to using privacy as a barrier in comparing the two. Privacy obviously might stand in the way of doing some of the work you want to do, but for good reason. In other cases, maybe bureaucrats are flagging privacy as a concern, but it's not a real concern or it can be met through other means and it shouldn't be a barrier as it goes.

Has work been done in your office to analyze legislative things—you don't want to call them barriers—that might in your view, or your office's view, need to be addressed to do more digital innovation?

● (1650)

**Mr. Alex Benay:** We've committed to doing a two-year study within TBS on legislative reviews for digital service delivery. We did an assessment of 11 departments, and I believe we found well over 150 possible—and I do want to highlight "possible"—legislative impediments.

We also found a lot of existing data-sharing agreements among the departments. Now we have to sift through those as well. Work with the Privacy Commissioner's office has started in sharing the plan. We do have some form of assessment of that.

**Mr. Nathaniel Erskine-Smith:** Let's start there. You have 11—

**Mr. Alex Benay:** Eleven core service departments. It's a front-line set-up.

**Mr. Nathaniel Erskine-Smith:** Okay, great. And you said 150 potential—

**Mr. Alex Benay:** I believe the number is 187, but we'll confirm that.

**Mr. Nathaniel Erskine-Smith:** Okay. Has that list been shared with the OPC?

**Mr. Alex Benay:** I will validate that, but I do not believe the list has been shared, but the project intent itself has been shared, yes. We've not finished the work. We're at year one of two right now.

**Mr. Nathaniel Erskine-Smith:** Okay. Would you be able to share that list so I have a better understanding of what—

**Mr. Alex Benay:** Absolutely.

**Mr. Nathaniel Erskine-Smith:** You can share that list with us. I would encourage you all to share with the OPC. That would be very helpful.

Mr. Snow. I park in the city of Toronto. I don't know if you've ever parked in the city of Toronto. I think a lot of people have come before us and have said that a lot of the questions with respect to digital government, about building trust and getting Canadians or citizens to trust us—I think a big part of the answer is not a politician selling it, as far as it goes, but building services that work for citizens, such that they want to keep using them. I like parking in the city of Toronto. It's easy to do. I understand the app for this was developed by a San Francisco company. The app is then licensed by the city of Toronto. I even like getting a ticket in the city of Toronto, because it's so easy to dispute the ticket, as I can do so online from the comfort of my own home.

As a citizen, the way I park in the city of Toronto and how I dispute a ticket in the city of Toronto, I want that at all levels of government. I trust in the system, as far as it goes, with respect to parking in Toronto.

CDS, you've listed a few projects. Is there a project that I can walk up and down the street, saying this is just like parking in Toronto.

**Mr. Aaron Snow:** Not quite yet.

CDS, being fairly young, is also walking before it runs. The citizenship examining schedule is the closest to that. The process before was that you would get a letter in the mail that looked like a summons. It was scary and it was written in “policy-eese”, and somewhere near the bottom in small print was some instruction about where to send a letter if you wanted to reschedule. The team that worked on the project talked to people who were caught between taking their citizenship exam or attending their daughter's graduation. People would try to make it. We're going to the place where now.... The the first thing the team did had very little to do with technology, but to simplify the letter. The the first words at the top of the letter were changed to, “Congratulations, you're one step away from becoming a citizen of Canada”. Just that content design change was enough to change the experience for lots of people. Then, here's the URL, you go there, you go online, you pick other dates that you're available on, you hit submit, you receive a confirmation soon thereafter. The experience is considerably—

**Mr. Nathaniel Erskine-Smith:** Is there an open call—we've got a Minister of Digital Government. That minister presumably tells her colleagues that, if they have a problem and they want digital services or service standards to be improved, they should come to her office or to CDS and they'll try to tackle the issue for them.

Does that happen?

**Mr. Aaron Snow:** I haven't spoken with Minister Philpott about that particular approach. Over the last 18 months, CDS has literally had hundreds of conversations with offices in departments and agencies all over government. We listen to a lot of requests, many of which are not necessarily in our wheelhouse, but we try to redirect and help folks in other ways.

We have a set of criteria that we use to evaluate the opportunities and figure out where we can have the most impact and do the most reusable work.

● (1655)

**Mr. Nathaniel Erskine-Smith:** In a previous report of ours on the Privacy Act, we recommended a standard of collection and retention of personal information based on necessity and with proportionality. That may be a very large question for you to answer in the limited time I have, but I would appreciate a more fulsome answer—in writing if you don't have a full answer now. Is that a problem in your view? If so, why? And if it isn't a problem, then that makes my life a lot easier.

**Ms. Ruth Naylor:** To speak to the Privacy Act review, I know that the Minister of Justice, in her response to this committee, acknowledged that the government was going to undertake a review of the act. It is a complex endeavour, so an issue like that is something that's still under consideration. That work's ongoing.

**Mr. Nathaniel Erskine-Smith:** Less so about government efforts to undertake a review, but if you've got 187 barriers, as far as it goes or whatever word we want to use to describe it, would necessity and proportionality as a standard get in the way of what we want to do?

Here's a way of thinking about it. Ann Cavoukian was before us and said that privacy and security and privacy and services can go hand in hand. They don't have to be at odds with each another, but sometimes actually they are when we talk about data minimization, because sometimes we want to collect more information to provide better services, but if we have less information, we can't provide the same level of services.

Therefore, it's a question of necessity for the government service, and that question of necessity might mean data minimization, which might actually mean that we don't provide the full suite of services that we may want to in providing the best services we can.

**Mr. Alex Benay:** We'll get back to you officially with an answer in writing.

The immediate reaction I would have for you is that we would take that kind of an issue to our architecture review board, as we're designing the services and as we go through, so that as we see a trend, we then apply a standard. That has not necessarily gone through the architecture review board, at this point and at that level of granularity, but we'll look to it and get back to you with a written answer.

**The Chair:** Thank you, Mr. Erskine-Smith. We're at time.

I'll go to Mr. Kent for seven minutes.

Oh, Monsieur Gourde, go ahead, please.

[*Translation*]

**Mr. Jacques Gourde:** Thank you, Mr. Chair.

I'd like to give Mr. Snow an opportunity to answer my earlier question about the 15% to 20% of Canadians who don't really use digital services. I'm curious as to how we could educate them on the issue, even encourage them to use the services more.

[*English*]

**Mr. Aaron Snow:** The easier to use and, obviously, the more secure those services are, the more folks will use them, I believe.

In some ways, this is also due to how long it takes to do this kind of work, a question of—if I may borrow a Canadian expression—skating to where the puck is going and not to where it is. Availability of connectivity and so on is only getting better, not getting worse. Again, services will always be multi-channel, for as long as there are people who can only access services—even countries with incredibly high rates of digital adoption for their government interactions, like Denmark, which is at 90% plus, they still continue to provide services through alternative channels when people cannot or will not participate. However, you can incentivize the use of digital services and thereby move more people into that experience, if they find it acceptable, but it has to be usable.

[*Translation*]

**Mr. Jacques Gourde:** You raised an interesting point when you mentioned the security of digital services We talked about the ideal situation, but there is a dark side as well. We can't forget that cyber-attacks are on the rise. Just yesterday, I received yet another fake alert. I got a message on my phone that was supposedly from my bank asking me to provide my personal information, and yet, I've been dealing with the same bank for 45 years. As Canadians' digital footprints inevitably grow, we'll see more and more people trying to use that information to scam Canadians and get money out of them.

Will we see stronger safeguards? Although we want to streamline the process and make it easier for people to access services, we may also be making it easier for scammers to take advantage of Canadians.

**Mr. Alex Benay:** To be direct, I would say that we're looking at every facet of the issue, together with the enterprise architecture review board. We want to make services easier to access, yes, but we also have to ensure people's information is secure. I can tell you the problem is the subject of intense discussion among the members of our governance team, which we set up 12 months ago.

I'll let my colleagues at the Communications Security Establishment field some of the more technological questions.

I will say, though, that the scale of public education initiatives is growing. Countries like Uruguay have literally brought iPads into people's homes to educate them, show them how to interact with the government and explain what to do and what not to do—if their mobile device is hacked, for instance.

As society moves farther down the digital path, initiatives will have to include an educational component. That's already happening all over the country, both provincially and municipally.

● (1700)

**Mr. Jacques Gourde:** Mr. Snow, did you have something to add?

[*English*]

**Mr. Aaron Snow:** It is incumbent upon any service that handles personally identifiable information or other sensitive information to provide the basic tools for a confidence-inspiring level of security. It's a common best practice.

For instance, today we use what is called "two-factor authentication". You enter not only a password, but also, after doing so, you need to be able to either get a code on your phone or carry around a physical key. I don't have mine on me; it's in my bag. It provides a belt-and-suspenders solution. The systems that provide that are providing an order of magnitude more security and confidence in the systems, and they are much more difficult to scam.

[*Translation*]

**Mr. Jacques Gourde:** Will the new digital solutions make departments so interconnected that they will be able to search for Canadians' information without their knowledge, or will individuals still have to consent?

Say the Canada Revenue Agency conducts an audit on someone, will the agency be able to turn to the Department of Finance for information on the individual? Could the agency obtain the source of a person's income, access to their banking data and other such information unbeknownst to the individual?

**Mr. Alex Benay:** Current laws prohibit us from doing that. They tend to be structured vertically within an institution.

[*English*]

Our Privacy Act also says that information is collected and used for the purpose for which it was collected.

[*Translation*]

Legally speaking, it would be very difficult to do what you just described without notifying Canadians.

When an enterprise service becomes a reality, or if we ever achieve a state of—let's call it—Utopia, where all services are available to Canadians on a single portal, we'll certainly have to consider those kinds of questions.

Currently, however, things are structured more vertically, as I said, preventing that type of data sharing and analysis.

**Mr. Jacques Gourde:** Thank you.

[*English*]

**The Chair:** You have about a minute.

[*Translation*]

**Mr. Jacques Gourde:** Thank you. That's it for me.

[*English*]

**The Chair:** You're good. Okay.

Next up, for seven minutes, is Mr. Angus.

**Mr. Charlie Angus:** I'm interested in the question of AI. I see that it gets promoted a lot in smart governance. We can use AI to help fight climate change. I'm not making that up; I saw that. We can use AI, and it will help to mitigate natural disasters.

No offence to my colleagues on the government side, but governments love things with all the bells and whistles, and that are magic and seem to offer miracle cures.

I'm interested in the disenfranchisement of citizens through the use of AI, and the way that some end up as winners and losers in the digital and social realms. The ideas that are used in the modelling of AI will have social impacts.

How do we, in our work in committee, ensure that when we're talking about AI, there's an ethical lens that is transparent and makes sure that people are not being targeted or disenfranchised because they don't fit the algorithm?

**Mr. Alex Benay:** That's one of the burning questions we have in the digital service space writ large, not just in Canada, but frankly around the world. It is a question of values. Different countries will automate different things according to their values framework. We want to make sure that Canada automates some of its services based on our values framework. It is a continuous conversation.

Currently, the directives that we're putting in place are looking at certain elements, for example, making sure that we don't have a black box making a decision on behalf of a human. We know that the decision pattern of the algorithms as they change is an important factor, because how do we authenticate the fact that the Government of Canada is responsible for this service if it's an algorithm?

We also have directives in there where, according to the level of severity, you may have to have an internal peer review of the automation that you're working on. That's something we're considering, as well, in putting in some of these directives. It's all part of the algorithmic impact assessment tool that we talked about previously, which we've developed collaboratively around the world.

Those are some of the examples.

I would also point to data. We could have the most unbiased code ever and have bad and biased data. We've seen examples in the private sector, from recruitment tools at Amazon to other things, where the data was biased and therefore the service and algorithm became biased.

It's not just a question of the technology; it's actually a question of the data holdings that we currently have as well. Those are all things that we're looking at.

It's not a perfect solution, but it's something that's going to have to iterate quite frequently.

● (1705)

**Mr. Charlie Angus:** I'm very interested in the black box issue. Corporations and vendors who want to deliver services are going to see that as proprietary technology. Is the black box going to be open to review by bureaucrats, or is it going to be an open source so that the public can see the calculations that are going into deciding how the algorithms work?

**Mr. Alex Benay:** That discussion is happening literally as we speak, so I can't answer that definitively one way or another. It is something that we want to take into consideration. There are pros and cons to both sides of this thing. We want to make sure that we have the best technology available, but at the same time, we have to respect certain values and ethics that are important in the country.

We do have instances where we have private sector code that is being held in case there is an emergency. Those are the things that we're looking at as well.

To be very transparent, this is a new space. Governing algorithms is a new space. Canada is one of the countries actually taking the lead on some of these things. The key for us will be to work iteratively with our global partners who share the same values.

**Mr. Charlie Angus:** Something happened today in the House of Commons that I think shocked all of us was an accusation of racial profiling of young black activists who came to Parliament Hill. I have been 15 years in Parliament. I'm a white guy with white hair, and I think Parliament is very open and inclusive—the police are excellent—but we had a case of people being profiled because of their colour.

My point is that when we're looking at profiling and the black box technology—and the bureaucracy might be the ones who can best see that—the latter will be challenged by people who are being victimized by the profiling that is done. That's my question: How do we ensure that there is that kind of public input and public challenge to make sure that the algorithms do reflect the values of our society in a way is moving everyone forward?

**Mr. Alex Benay:** We have a few existing mechanisms. For example, the architecture review board, which I mentioned a few times, will be looking at automation projects as these are identified in investment plans, departments and other things. From concept, we will be looking at applying our values throughout, from procurement to deployment. The architecture review board will look at that. I think the level of transparency of our services will be very important as we move forward. Some of our directors were looking at the facts we must disclose, such as that you are talking to a robot and not a person on the other side of the chat, for example—which will be good—and that we are expecting citizens to report issues back. The dialogue will increase and become very active as we start automating. It is a pace-of-change discussion as much as it is a values discussion.

**Mr. Charlie Angus:** Thank you for that. As a musician, I know what a polyrhythm is. I don't really know what an algorithm is, but I think it's really important. I just want to know that other people have an opportunity to give their input.

**Mr. Aaron Snow:** Perhaps I'll just note that we're used to talking about computer code as something that we understand in terms of how that code functions. We don't generally treat each other that way. Increasingly, as the code gets more complex and harder for us to comprehend ourselves, it may become more important to focus on, in addition to how the code operates, the outcomes that are actually occurring. If the outcomes are going in the wrong direction, then hold the systems responsible for the output and not just for the nature of the decision-making itself.

**Mr. Charlie Angus:** Thank you very much.

**The Chair:** We'll go to Mr. Saini for one question.

**Mr. Raj Saini:** Two.

**The Chair:** I thought you said one.

**Mr. Raj Saini:** They are two small ones.

**The Chair:** Take your time. Go ahead.

**Mr. Raj Saini:** I just want to talk about technology, but since Mr. Angus raised the point about AI, I'll address it this way. If we look at the advancement of AI right now, there is some speculation that in 15 to 20 years, 40% of the current job market will be displaceable. You can see how fast the private sector is moving here. In terms of the government sector—because there are going to be points, when you have a digital government architecture, where you will also need touchpoints for the private sector—how will you make sure that the technology will remain so that both systems are somewhat equal?

**Mr. Alex Benay:** That's a very good question. I would answer with a few things.

First, I think artificial intelligence and automation, like any new technology.... My colleague, Mr. Snow, spoke to a hype cycle. It's actually a thing in our sector where we see where that technology sits on the hype cycle. I still think that artificial intelligence and the concept of job replacement is, frankly, something that is very debated. It has gone from “the machines will take our jobs” to our increasingly seeing coexistence of humans and machines, and how that will actually augment the work as opposed to replace the work.

I can't speak definitively on the strategy because I still think it's very early in the hype cycle. We're seeing that the countries that do this well are the ones that not only make the investments in these technologies, but also bring a multidisciplinary lens to this discussion.

It's not only an economic growth issue; it's a service to Canadians issue, writ large. It's also how the private sector serves citizens as well. I think it will be important for us to keep an eye on the developments. Often things are done so quickly.... A service provider from a company without necessarily.... It happens so quickly we don't see it. For example, translation services are increasingly becoming very efficient on social media platforms, and it's only for the last eight months that you've actually seen an efficiency curve really spike. So, all of a sudden, that's a different conversation than we were having six months ago.

I think the key will be multidisciplinary, making sure that we don't bring departments to an issue, but bring a horizontal sort of lens to the issues and just continue that narrative and the dialogue.

● (1710)

**Mr. Raj Saini:** I have a final question. As I'm sure you're well aware, in 2007 Estonia faced a cyber-attack, and one of the responses to that cyber-attack was to have scalable blockchain technology, which they found to be secure and had a strong amount of integrity for the system. Are there any thoughts about employing that here?

**Mr. Alex Benay:** I would say that we are increasingly mature on the artificial intelligence path. We're a little less mature on blockchain in the Government of Canada. It doesn't mean that we don't have places that are experimenting. We are looking at ID pilot, digital identification pilots with provinces, for example, using blockchain. We're looking at grants and contributions, I believe, at the National Research Council, using blockchain. It is probably the next area that we need to look at. I would like to say we're more mature in that space, but we're actually not.

We invested heavily in the AI space to match the investment that the government's made in AI across the country, to make sure we were ready to ingest those services. I would suspect blockchain and a few other concepts will probably be next on our radar.

**Mr. Raj Saini:** Okay. Thank you.

**The Chair:** I just have one last question.

Mr. Benay, you talked about using Google Docs as part of the interaction, I guess, with our citizens. It's ease of interaction, too, is key to it all. But one thing our committee's been concerned about is the state of collection and the huge data companies that they are, whether Amazon, Google, Facebook, etc. We see this marriage happening: It might be that we eventually go to vote on Facebook. Maybe there's an app that we use. Maybe that's a subjective thing to think about, but a concern to a lot of us in this room.

As you're part of our bureaucracy that's making this system for government, what recommendations, regulatory-wise, would you make on some of these big-data platforms? You've established the fence around our data, as Canadian citizens.

Maybe this is more for Mr. O'Brien. What regulations would you, in your personal opinion, apply to these big-data companies?

**Mr. John O'Brien:** I think that in terms of regulation, I would completely pass that over to Alex.

I'm going to go back to my earlier point that—

**The Chair:** Let me ask it as a citizen, though. You're ones who use these. You use Google, I'm sure, and all the rest of them.

**Mr. John O'Brien:** I think transparency is the key in that. I'm not going to speak ill of any companies, but there are some companies that are very good about being transparent in how they do security of their cloud services, for example. Google, Microsoft, Amazon all publish very good security white papers about what they do to protect the information in their systems. They also tend to try to be as transparent as they can on the data they're collecting. In a lot of cases, I think sometimes people just don't understand the things they're agreeing to. I think those are some of the things that have been done in the U.K. and in the EU with GDPR in getting more informed consent. I would leave it at that, but I think Alex probably has certain things to say.

**Mr. Alex Benay:** Yes, it's maybe a three-part answer. I think we need to get better at understanding that there are certain pieces of data that are okay to be on some of these platforms, and there are other pieces of data that are not. Personal information, I would say, is too unclear at this point, but it doesn't mean that we can't look at the discussions with these vendors and suppliers around the values that we want to bring in how we manage personal information, the requirements around security.

Some of the work we do on policy, for example, should be completely transparent and open when we're talking about algorithmic impact assessments, because these things will impact a citizen directly. Putting that on Google Docs and, frankly, 10 other platforms, is not necessarily an issue. That's the first part.

On the other part, I would like to just bring standards into the conversation versus regulation. I think there is an opportunity to start with better standard-setting across the country. During my time in the private sector, and when I was at OpenText, I would often run into other countries that had set standards for themselves that, frankly, possibly would put their own organizations or enterprises into advantageous positions. I think we need to look at standards as both offensive and defensive mechanisms, and find ways to actually start looking at these standards as a first step.

With regulations, the problem is that they could stifle innovation —you'll hear that a lot from the private sector and some of my former colleagues—but they're possibly a step. There are probably some other steps you could look at before diving directly into regulations, because they are a double-edged sword.

● (1715)

**The Chair:** Okay.

Mr. Snow.

**Mr. Aaron Snow:** Obviously the policies and whether those vendors are encrypting at rest, whether they're encrypting in transit, whether they're taking various steps to protect data are part of the equation. The other part of the equation is, how are we protecting our own account management? Making sure that we are using password managers, making sure that we are using that second-factor authentication that is available on many of these systems at this point—and increasingly will probably start to become required—are steps that government can also encourage and help explain. So there's a role there as well.

**The Chair:** Ms. Naylor, do you have any response as well?

**Ms. Ruth Naylor:** No, I don't have a response on that issue.

**The Chair:** Okay.

Are there any further questions?

Go ahead, Mr. Angus.

**Mr. Charlie Angus:** Before we rise, I just want to bring to the committee's attention my view that we should have a discussion on the minister's announcement that she's going to have the procedure and House affairs committee look at the potential threat of Facebook to the electoral system. We've done this work. I find it surprising. All the work that we've done has been recognized internationally. A few months out from the election, our committee is being completely sidelined. Our report has been sidelined. We've heard nothing back. I think we should raise a concern with the minister. If she wants to know about the threat posed by Facebook, and undermining the platform, we have done all of this work.

**The Chair:** Is there any response?

**Mr. Nathaniel Erskine-Smith:** I understood that Minister Gould was on our list.

**Hon. Peter Kent:** Yes, we passed that motion.

**Mr. Nathaniel Erskine-Smith:** Right. I would say it is fair game to ask her all sorts of questions, including about this. It would make no sense for PROC to undertake a study that we've already pursued and completed.

**The Chair:** I can write them a letter to explain what we've actually done, and send the report along with it, if that would help.

**Mr. Charlie Angus:** Yes, that's what I would suggest, Chair, that we send it to her, and the committee as well, to say that this work has been done. We spent a year on it, and we did travel internationally.

**The Chair:** Would you like to move a motion to have the minister appear?

**Mr. Charlie Angus:** I would like to move a motion that you write a letter. Certainly, I think the minister should appear, but we should also write a formal letter to the chair of PROC and to the minister saying that we've done this work. It seems absolutely crazy to start from scratch.

**Mr. Nathaniel Erskine-Smith:** I did not see the appearance, but my expectation was that she was asked questions and that this was an off-the-cuff remark. I have no idea, though. Obviously, she's aware that we conducted a study. I wouldn't spend your time writing letters. When is she scheduled to appear?

**The Chair:** I'm not sure. Our current clerk is under the weather today. We'll find out when he comes back.

**Mr. Nathaniel Erskine-Smith:** Oh, I see. Okay.

I think this is a fair conversation to have, to impress upon her the work that we've done and to ask her why she thinks PROC is the appropriate place instead of our committee, and whether she has additional questions that she thinks the committee should perhaps pursue. The committee that is already well briefed and versed should be pursuing it. We've already got her. If you want to write letters, feel free, but I think she's coming.

**Mr. Charlie Angus:** My only concern is that if that committee has been given instructions to start, our conversation with her will be irrelevant. I think they should be made aware as well that we've done this work. We'd be more than willing to advise them.

**Mr. Nathaniel Erskine-Smith:** Sure, write a letter to PROC.

**Mr. Charlie Angus:** Otherwise, by the time they finish with their witnesses list, the next election will be over, and meanwhile, our report is sitting on a shelf.

**Mr. Nathaniel Erskine-Smith:** By all means, send the chair a copy of the report.

**Mr. Charlie Angus:** I've been in Parliament too many years to see parliamentary reports. People love them the day they come out, and the only people who remember them the day after are the committees that did them. Nobody pays attention. I'm going to fight for this one.

● (1720)

**The Chair:** I'll write the letter and send it.

I will raise one last thing. The International Grand Committee has been proceeding. We're going to do a press release, I believe tomorrow.

I thought it was clear already, but I've been asked by our current clerk as well about doing releases and giving permission as chair to do the release. Is that still the case? I thought we already approved that.

**Mr. Nathaniel Erskine-Smith:** We're good to go.

**Mr. Charlie Angus:** I find the statements in the U.K. report to be devastating. I think we really have to be focused on Facebook when we talk. If they were referring to Facebook as international “digital gangsters”, our committee needs to be—

**Mr. Nathaniel Erskine-Smith:** When I read that, I thought—

**Mr. Charlie Angus:** Like, why didn't we come up with that?

**Mr. Nathaniel Erskine-Smith:**—this has Charlie all over it.

**Mr. Charlie Angus:** Yes, I know. Goddamn Brits.

I think we have to be talking about what the international community does in response to the report. The U.K. committee should give us their report and we should be talking internationally about what steps we need to take.

**The Chair:** Yes. They released it on Monday, I believe, and I challenge all of us here to read it. There is an acknowledgement of our presence there too, on the International Grand Committee. That's a nice tip of the hat to us.

Thank you.

Thank you again to the presenters for coming. We have a lot of information and a lot of stuff to deal with. Have a great day.

The meeting is adjourned.