HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 142 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, April 4, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, April 4, 2019

● (1530)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): I'll call the meeting to order. This is meeting 142 of the Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3)(h)(vii), we are resuming our study of privacy of digital government services.

The witnesses we have with us are, from the Canadian Bankers Association, Angelina Mason, General Counsel and Vice-President; and Marina Mandal, Vice-President, Banking Transformation and Strategy. From Symcor, Inc., we have Della Shea, Vice-President, Privacy and Data Governance and Chief Privacy Officer.

We'll start off with Marina, for 10 minutes.

Ms. Marina Mandal (Vice-President, Banking Transformation and Strategy, Canadian Bankers Association): Thank you, Mr. Chair, and good afternoon. It's always a pleasure to appear before the committee.

My name is Marina Mandal, and I'm joined today by the CBA's general counsel and vice-president, Angelina Mason. Before I continue my opening remarks, I just want to apologize in advance if my voice drops during my comments. I'm fighting off a cold or flu or something.

The concept of digital government, when we're already living in a digital society, should be welcomed. This is especially true in the area of identification, where establishing who we are and what we're eligible to do is one of the foundational tasks of government. Despite remarkable advances in technology that accelerate with each year, we're still tethered to an analog model that relies on presenting physical documents to establish our identity in multiple daily transactions that we have with public services, businesses and each other. The good news is there's a modern solution to this challenge. The Canadian banking sector is ideally situated to underpin a digital ID system that will revolutionize the way we use personal data to interact with the world.

The current system is deficient in three major ways.

First, it's outdated, especially when it relies on physical documents like driver's licences and utility bills. These documents can be forged or stolen, and used fraudulently. Requiring face-to-face transactions also places the burden on those in remote communities and those with mobility challenges who could be forced to travel long distances to conduct basic business or access essential services.

Second, even today's technology-based approaches are clumsy. The two-factor identification sequence used online—where you enter a username and password—can be easily compromised. It's also a hassle for users who must remember dozens of log-in credentials.

Third, inefficient methods of establishing identity are a drag on economic growth. They slow down the speed of transactions, introduce uncertainty and are prone to costly errors. Countries around the world realize this situation is untenable and are crossing the electronic frontier to explore the benefits of implementing digital identity systems.

When ID goes digital, citizens can verify their identity electronically using a combination of existing systems and newer biometric tools, such as fingerprints or facial recognition. With the growing number of Canadians accessing services and businesses online and the increased use of mobile phones, Canada is in a position to move forward with its own robust digital identity system. Two recent developments have added momentum to this trend.

First, updates made in 2018 to the Bank Act expressly allow banks to provide identification, verification and authentication services beyond the needs of their own operations. This is a contemporary acknowledgement of what has always been true about banks: They know who their customers are, know about their financial status and can attest to both. Historically, banks would write physical letters of introduction for clients to help them in personal or business matters in distant locations. The endorsement of a bank created trust among strangers.

The second development is that the CBA produced a white paper last year that lays out a clear path for making digital ID a reality in Canada. We took into account our country's unique characteristics, advanced institutions and sophisticated infrastructure to develop a framework for what could work here.

We call for a federated model of digital ID because it would align with Canada's political structure. A federated model works by creating linkages between federal and provincial identity management systems. Right now, identity is spread across multiple isolated regimes. For instance, the federal government has social insurance and passport information, but the provinces manage health cards and driver's licences.

The first step in our model envisions maintaining these distinct systems, but connecting the disparate elements in such a way that someone's identity can be authenticated electronically using a combination of attributes. Instantly verifying someone who is using multiple digital reference points is more secure than relying on a plastic licence card that could be a forgery. Because this digital network is connected yet decentralized, the risk of compromising the system is reduced by eliminating honeypots of data that hackers tend to target.

The second step is to harness the power of the private sector. This would enable the creation of a digital ID system without the cost and risk of building complex infrastructure from scratch. Canada's banks already operate across the country and around the world. We have robust, interconnected electronic systems that citizens can access from branches, bank machines, home computers and mobile phones. These networks are up and running 24 hours a day, all year long. More importantly, banks are already held to a high standard when it comes to collecting and safeguarding the personal information of customers. For banks, the privacy of their clients' data and personal information is at the core of what they do. Banks are subject to rigorous oversight to ensure this data is held accurately and securely, from one end of the transaction to the other.

● (1535)

The third step in our federated model involves passing legislation that would allow business and government to accept digital ID. Banks must know their clients as part of Canada's fight against money laundering and terrorist financing. That involves thoroughly gathering and maintaining customer information and financial intelligence subject to strict regulations. lt's true that some client ID requirements under anti-money laundering and anti-terrorist financing legislation have been modified to allow non-face-to-face verification; however, the rules continue to be rooted in physical ID.

Our industry is ready and willing to work with Treasury Board, the Department of Finance, ISED and other departments and agencies to explore ways to accommodate the technologies of the connected age.

The government is already starting to explore other ways to update financial transactions, and blockchain and artificial intelligence are pushing into new frontiers. With these developments, the demand for digital ID will only grow more urgent. Banks stand ready to contribute energy and resources to build a federated model for Canada.

Thank you for your time. I look forward to answering any questions you may have.

The Chair: Thank you once again.

Next up, we have Ms. Shea, with Symcor Incorporated, for 10 minutes.

Ms. Della Shea (Vice-President, Privacy & Data Governance and Chief Privacy Officer, Symcor Inc.): Good afternoon. I would like to thank you, Mr. Chair, and also the members of the committee, for the opportunity to speak with you today on such an important topic and to share perspectives as the government endeavours to understand how to improve services for Canadians while also protecting their privacy and their security.

My name is Della Shea. I am the Chief Privacy and Data Governance Officer at Symcor and I offer my comments this afternoon based on approximately 20 years of experience leading internationally recognized data privacy and security programs at Symcor.

For those of you who may not be familiar with Symcor, we are one of Canada's leading providers of business process outsourcing services to the financial services sector. We offer a diverse portfolio of traditional and also digital services, including payment processing, statement production, document management and also fraud analytics. We also provide services to other organizations in retail, utilities and telecommunication sectors and more recently also to some governments. We have close to 2,000 employees, who work across Canada.

You've asked how government can improve services for Canadians while also protecting their privacy and their security. In addressing this question I'd like to share some of my insights as well as experiences gleaned from actually embedding privacy and security into our services at Symcor.

In this regard, my comments will focus on establishing and maintaining trust, and specifically on three core tenets that underpin trust: first, privacy by design and data stewardship; second, the role of trusted service providers in a digital ecosystem; and third, a consistent legislative framework. I will address these in turn.

First, as many of you and members of the privacy community are aware, the concept of privacy by design calls for privacy to be taken into account throughout the planning and service delivery process. In short, privacy must be an organization's default mode of operation. Governmental bodies will have to take a similar approach. My recommendation is to establish controls on the way governments design their systems. The privacy by design framework should be used in order to embed privacy into operations.

A second concept closely related to privacy by design is data stewardship. Data stewardship and being an effective data steward is about actually operationalizing the accountability model that has been set forth under Canadian privacy legislation. As Canada's privacy commissioners have highlighted, it is about the clear acceptance of responsibility for the protection of personal information under their control.

As the government considers its approach to rendering services to Canadians, I would urge the adoption of a data stewardship model. At a very practical level, this means maintaining accountability for protecting Canadians' privacy and security.

Next, I would like to briefly touch on the critical role of a trusted service provider in the digital ecosystem. The shift to platforms and ecosystems has already happened. This represents the future for all organizations, including governments. The new digital ecosystem has brought the opportunity to create new and innovative operating models and new partners, intermediaries and also collaborators.

Under the Canadian private sector privacy legislative framework there is an elegant rule that organizations are responsible for the personal information in their custody and control, including when this information is also transferred to third parties.

It is critical for government to establish a working model that consists of trusted service providers and intermediaries in this digital ecosystem. This will consist of a model whereby organizations are held to a consistent standard to minimize the likelihood of systemic vulnerabilities, but more generally to provide confidence in the digital ecosystem and digital service delivery.

In a similar vein, as a matter of gaining and maintaining public trust, there must be consistent and robust privacy rules for the private sector and the broader public sector for data processing activities, to avoid any gaps in privacy coverage.

In short, all players in the digital landscape, both private sector and public sector, need to be following consistent and robust privacy legislation. The role of government will be fundamental in establishing consistent, robust privacy rules applicable to the digital ecosystem.

● (1540)

This brings me to my conclusion. The data strategy road map for the federal public service published last fall outlines a comprehensive vision to overcome silos and leverage data as a valuable asset. I applaud the government for embarking on this study to consider privacy and security as it undertakes this journey.

I would encourage the government to design a maturity model that will scale to the future, one that not only considers privacy and security at the foundational level of digitizing government services but also contemplates a fully digitized society where everyone and everything is connected to a fluid and ever-expanding ecosystem.

Thank you. I look forward to your questions.

● (1545)

The Chair: Thank you, Ms. Shea.

Next up we have questions, starting with Mr. Saini for seven minutes.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon. Thank you so much for coming.

Ms. Mandal, in your opening comments, you said something that I wanted to dig down a little deeper into, just so I have a better understanding. We know right now that if we're going to do anything in digital government we need private sector involvement. It has to go hand in hand to leverage not only the intelligence in the private sector but also these advanced technologies that they have. We also know right now that information, especially in Canada, is very decentralized, with different levels of government holding information, and even different departments holding different information.

In the white paper you wrote, you talked about the federated approach to the digital ID framework. You mentioned some of that in your opening comments. Can you give us a broader understanding of how that will work in contrast to the Estonian model with X-Road? You said one thing that I think is similar to X-Road, that there are no honeypots. But with X-Road they started from greenfields. We're not going to be able to start from a greenfield. We have more advances to mature, legacy systems. Different departments have different systems.

How could we compare the two? How would the federated approach work as compared to X-Road, which is a different approach in Estonia?

Ms. Marina Mandal: Thank you for the question.

I know that the CBA's white paper, for those of you who have had a chance to review it, does talk about two countries in particular, Estonia and India, which are quite different for a number of reasons from Canada. We thought, as I think this committee did as well, that Estonia is sort of a model example within the specific context and culture of that country. I would say the similarities between the lessons learned from Estonia for Canada is the paramount importance of privacy and data security. My understanding is the federal government's digital exchange project adopts similar technology to what underlies X-Road. Those are two things we can take from Estonia.

I would say that pretty much after that everything is quite different. The federated model works with Canada's governance. We have multiple levels of government. A foundational identity documents it with different levels. Birth certificates sit with provincial governments. Citizen and immigration documents sit with the federal government. The federated model makes sense because of that decentralization. I think when we look at the private sector involvement.... I think in Estonia it was pretty much a government top-down position, as it was in India, whereas in Canada we already have movement. We have things that are in flight right now. I'll talk about a couple of things probably a few more times through my comments today.

The Digital ID & Authentication Council of Canada was created coming out of the task force on payments that was appointed by former finance minister Flaherty, because the task force on payments said that for digital payments to work, you absolutely need digital ID. DIACC has at the table provincial governments, the federal government, telcos, banks and credit unions. They have come together to create a pan-Canadian trust framework that would ideally underlie all players in the digital ecosystem in Canada.

Mr. Raj Saini: Thank you.

Ms. Shea, I want to come back to you. I know you have the private sector experience that's there.

We talk about a process called onboarding. Could you give me a rundown of how onboarding in Canada works? Onboarding in Canada would involve 37 million people. We have people living all across this country. Some people are able to access the Internet. Some people live in areas, unfortunately, where broadband is still not available. You have people who are digitally savvy, and you have some people who may not be that digitally savvy.

How are you going to get everybody on board? There obviously will have to be economies of scale that are involved, and if this system's going to work, everybody has to participate. The onboarding process for me seems like one of the great limiting steps, as we say in science. How would that work?

● (1550)

Ms. Della Shea: I would like to suggest a few things.

In my comments, I had suggested having a maturity model and actually realizing that you can't do everything all at once, so have patience, in terms of how you are going to achieve a goal of having a digital service, having a digital government and ultimately, a digital society. That is the road ahead of us. It's being patient and having a maturity model to clearly articulate how you're going to accommodate individual citizens from all different walks of life.

Dr. Geist, in one of his earlier comments when he appeared before this committee, talked about the universal access issue. I think that's a very important issue to think about and address, especially when you are considering the geographical limitations and challenges of Canada. Being able to provide universal, affordable access is going to be a major challenge for Canada.

Underpinning this is also understanding that not everybody, even if they had access, would have the capability of being able to partake in government services. There's the educational component and it becomes a very important piece of the puzzle.

I would recommend that the government look at a parallel way of implementing the onboarding of individuals and also to be patient. It is going to be a journey. Not everyone is going to have an equal playing field in getting onto that new ecosystem.

Mr. Raj Saini: I have a follow-up question. I'm going to shift tack a little bit. I'm going to ask you this question, specifically because I believe that the organization you represent has a lot of experience with cybercrime and cyber-fraud.

We know that 80% of cybercrime and cyber-fraud is committed by organized criminal activity. We're living in an age now where there are state actors and non-state actors. Although there would be no honeypot, so there would not be one area where all the information resides, we're still going to be prone to that.

One of the things about privacy is that domestically, you have a robust system, but internationally, when we have potential attacks, potential cybercrime and maybe attacks on a certain part of the system which may contain more information than another, how do we protect ourselves from that? The reason I ask this is that you have a lot of non-state actors now that are extremely well resourced and well financed. How do we deal with that?

Ms. Della Shea: I would like to suggest the importance of shared intelligence. I think that, going into a digital transformation for the government, you will have cyber-attacks. There will be threats. I think that's a given, so it's ensuring that you have designed security into the systems at the very beginning and not looking at it as one type of control, but rather a multi-layered set of controls.

At Symcor, as an example, our strategy is really about having a multi-layered approach to security, so right from the data layer to the application layer and in the infrastructure and network. It's really about having that layered approach.

I think we also have to think about the importance of shared intelligence and having a framework. From a legislative and policy perspective, this is going to require some thought to enable data sharing across entities for the purpose of getting ahead of those potential bad actors that are attacking the system.

Mr. Raj Saini: Thank you very much.

The Chair: Thank you, Mr. Saini.

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

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

Thank you, all, for appearing today.

It's been interesting to follow, particularly with regard to the banking association, the interest expressed and the vision tested by your president, Mr. Parmenter, at a speech in January.

In your opening remarks, Ms. Mandal, you mentioned three challenges: the clumsiness, the outdatedness and the drag on economic growth. Which of these did the commercial banks address first or do you believe it is possible for the public service, as opposed to the private sector, to address all of these at the same time?

Ms. Marina Mandal: I think that fundamentally, it absolutely has to be a public-private partnership in Canada. As I indicated in my earlier response, government owns the foundational documents proving identity, so I don't see stand-alone solutions, at least none that are in flight in the market right now.

One solution that is a private sector solution done in partnership with the banks is SecureKey Concierge. I know that you heard from SecureKey a couple of weeks ago.

In terms of your question, SecureKey's product addresses all three of those things, I would say, but not so much the economic growth one, just because it's a limited use case right now. It allows access to more than 80 government services. It gets rid of the users who may only access the CRA once or twice a year but may access their bank online every week or two. It really takes away from the proliferation of user names and passwords. They only have to remember the one to log in to their account.

Then there's the question of outdatedness. Again, you're getting rid of the physical need to tie in to the CRA and other government services.

As to the economic growth one, digital ID is a pretty nascent market in Canada from both a public sector and a private sector perspective. As we see the market develop at both levels, public and private, I think we'll see more use cases that address the economic growth point.

● (1555)

Hon. Peter Kent: In terms of the outdated aspect, we had testimony a couple of months ago that suggested using something like the NEXUS card, the use of biometrics across the board, as it's used for travel security at the moment.

Have the commercial banks looked at implementing biometrics in place of the old standard identification?

Ms. Marina Mandal: I think that biometrics would be somewhat challenged, from a legislative barrier perspective, on the email front. There are no commercial bank initiatives around digital ID and authentication that rely on biometrics, to my knowledge, not in Canada for sure, but even—I'm trying to think—globally.

The one example of biometrics being used in digital ID that I can think of is the project currently being developed in Ontario in support of the Ontario effort towards digital ID, which I believe is called eID-Me. It was done in partnership with a financial technology company and would have your identifier, for Ontario government purposes only, on your phone. It would be password linked and biometric—either thumbprint or facial recognition. Globally and in Canada, it would be, I'd say, the major one that attempts to go the biometrics route rather than the bank log-in credentials route..

Hon. Peter Kent: Ms. Shea, do you have thoughts from the commercial sector on the use of something like the NEXUS card for secure digital ID?

Ms. Della Shea: Again, the private sector is different because of the legislative requirements. I think the key for considering having a biometric type of device is, similar to the NEXUS model, that it's really a consent-based model. That would be pivotal, because requiring a biometric of all Canadians, I think, would be a very challenging path to go down.

Hon. Peter Kent: In terms of travel security, it's not a problem, because the benefit outweighs whatever concerns might exist.

Ms. Della Shea: Exactly.

Hon. Peter Kent: Might there not be the same attraction in other realms?

Ms. Della Shea: It's a really good point, making sure that you have that risk-benefit paradigm and giving people the option, making it transparent.

Certainly, if it is an option for citizens and they are adopting it as part of making their lives more convenient, I think it would be something worth exploring. Pivotal to it, though, is having really robust security and having governance around the security process—

Hon. Peter Kent: —which would require change in the law.

Ms. Della Shea: Yes.

Hon. Peter Kent: As we've seen in the public service with the Phoenix pay system, one problem is that when governments approach a vendor, the vendor provides a suggested product and the purchaser, the procurer, decides to eliminate some of the recommended security safety aspects, and we then see the disaster that we have today. We see the same thing with the Boeing 737 and the safety additions that required extra payment, extra training and so forth.

How do you overcome this in private sector partnerships with government at all different levels? How do you ensure that government political decision-making doesn't interfere with success?

Ms. Della Shea: Everything is going to be a cost-benefit analysis. First of all, there's no such thing as absolute, perfect security. To achieve even close to perfect security will impact not only the financial aspect but also the utility of a service, so you have to really take a balanced approach.

Canada Health Infoway is an example I would urge the government to look to in terms of the way it established a process for vendors to present a solution for health care services. There is oversight and there is governance around the vendors who become certified through that process. That, then, would be a model the government could look to as a potential way of framing how you certify a vendor or a service provider to engage with government services.

Having minimum standards would be absolutely critical, in addition to having an assessment process to assess the various vendors wanting to become part of that ecosystem and then having ongoing monitoring. To speak to your example about airplanes, it is really about having oversight. It doesn't just happen once. It's no longer just about a project; it's now about a product and about a process and having a governance framework around it. Having it be ongoing is really critical.

● (1600)

Hon. Peter Kent: Not rushing to get a program into place before it's ready.

Ms. Della Shea: Absolutely.

Hon. Peter Kent: Ms. Mandal, what are your thoughts in this area?

The Chair: We're at time, but if you have a quick—

Hon. Peter Kent: Oh, I'm sorry. I'll come back.

The Chair: That's fine. I'm trying to be nice.

Next up, for seven minutes—

Mr. Charlie Angus (Timmins—James Bay, NDP): I see a little bit extra. Don't I always say what a good chair you are?

I'm not going to challenge the chair today.

The Chair: Go ahead, Mr. Angus.

Mr. Charlie Angus: Thank you, Chair.

Thank you for this presentation.

I deal with fraud all the time now in my offices. As they started out, you'd have had to be very naive to fall for the 419 scams, but they have become increasingly sophisticated. I've been shocked at how many people—in fact, many people probably never come forward—have been victims of these scams.

The only way it seems that we're stopping them is literally when the bank teller says no. People transferring funds to relatives who are in jail someplace, people transferring money to someone they want to marry who doesn't exist, people transferring funds because they're afraid the CRA is going to arrest them—they are becoming increasingly sophisticated.

Their power comes from this. If you have one point of information on someone, it's a long shot; if you you have two points, you're getting very good; if you have three points of information on someone, you're getting very dead-eye accurate. With AI, with the ability to glean stuff off the net, more and more of this fraud is going to take place. It seems to me, in the work that I do in my MP's office, that often the only thing that stops it is a bank teller saying, “I think you're a victim of fraud here.”

What mechanisms are there in the industry to start to deal with the growing sophistication of targeting people for fraud?

Ms. Angelina Mason (General Counsel and Vice-President, Canadian Bankers Association): I would say a significant part of it is education. We educate and let consumers know the risks out there. Also, it's a sharing of information to find technological ways to block certain types of communications.

With the recent launch of the Canadian Centre for Cyber Security, Scott Jones, who was recently at our cyber security summit, was chatting with us about ways in which we could from a technology perspective block those types of communications. It would require some sophisticated analyses and some sharing about how our systems work within industry, but we are very eager to participate in those types of discussions to see whether we can take even more proactive steps to address that concern.

Mr. Charlie Angus: Last year, 90,000 Simplii Financial and BMO customers were affected by a breach of personal financial information. Customers reported that they received conflicting answers about the timing and the scope of the breach, which was worrying. Was that breach by a malevolent outside actor? What was the nature of the fraud that citizens were affected by?

Ms. Angelina Mason: I can't speak to the specifics of the breach. What I can say is that we have been leaders in the cyber security space. We have had an excellent record. It was a rare incident, and I can assure you that banks took measures to ensure that their customers were whole financially and to provide other assistance to them.

We always continue to fight the fight. We are always looking at ways to detect these breaches. It's a daily thing. We are constantly finding ways to address attacks. We continue to look at it from both the perspective of sharing of information and understanding what new types of attacks could be coming at us. We invest heavily in this space and we continue to make it a priority.

● (1605)

Mr. Charlie Angus: I must confess, I don't keep my money in the bank. I'm in a caisse populaire, but I've been the victim of a few fraud instances, and I'm amazed when they contact me immediately and say that something happened on my card. That level of speed is very interesting.

Is that part of this whole move towards increasing the technological ability to intervene to stop fraud?

Ms. Angelina Mason: Yes. There are different layers. There are cybersecurity types of measures, which are really to address if someone's actually trying to get into our systems and get access to information. There are other types of compromises that can happen on fraud that aren't really cyber-related. Your credentials have been shared or your card has been compromised because they found out the numbers and the PIN.

In addition to addressing cyber, we do all sorts of monitoring so we can detect if there's unusual activity, identify different types of compromises and address them immediately.

Mr. Charlie Angus: RBC was named—I think it was in the New York Times—in one of the Facebook app issues. Because of their app, they were given preferred access, which gave them the ability to read private messages on Facebook. RBC said they never had that access. Facebook said they did. The Privacy Commissioner is investigating.

Does the Canadian Bankers Association look into these issues to be able to reassure customers that this kind of undue personal information is not being accessed by a bank?

Ms. Angelina Mason: We would not be part of that.

Ms. Marina Mandal: No.

Mr. Charlie Angus: All right.

Part of our work here is about protecting the privacy rights of citizens and private data. I note that, I think, CIBC and RBC at least have noted in their privacy policies that data can be transferred, processed or stored outside of Canada. That raises questions for our committee in terms of trying to ensure the protection of financial data.

Do you have a policy on trying to ensure the data is kept in Canada, where at least with our privacy laws and national standards we would know that the private information will be kept private?

Ms. Angelina Mason: Having data outside Canada and internationally is common not just across the financial institutions, but across a full range of companies. The Privacy Commissioner has addressed this in guidance.

It's so commonplace that you deal with it in a variety of ways. First of all, our federal privacy legislation requires that if data is to be housed outside of Canada, it must, through contractual and other measures, be kept as secure as if it were in Canada. There's also a requirement to provide notice to consumers so they're aware of that.

Mr. Charlie Angus: In the U.S., does that data come under the Patriot Act?

Ms. Angelina Mason: If you're talking about the potential for that data to be accessed in a lawful manner, it could be accessed through it, but that would of course require a warrant approach.

Mr. Charlie Angus: Yes, I've dealt with a number of citizens who were born in the U.S., and there was the whole tax issue in the United States, which was demanding that they pay taxes. We had citizens who had lived here for 40 or 50 years and were concerned. Are they made aware that their data may be held in the United States under the Patriot Act when they sign up for an account?

Ms. Angelina Mason: Yes, we provide disclosure where that data may be outside of Canada, and we explain the implications of that.

Mr. Charlie Angus: Thank you very much.

The Chair: Thank you, Mr. Angus.

Next up, for seven minutes, is Monsieur Picard.

Mr. Michel Picard (Montarville, Lib.): Thank you.

I have a three-part question. What is your understanding of open banking systems? What is your take on this from a security standpoint? Would that be a model, if it's good, that could be followed in the case of government?

Ms. Marina Mandal: As I'm sure you know, the government issued its first formal consultation paper on open banking in January. We put in a submission, along with other stakeholders, in February. I'll get into that in a second.

Since the deadline in February, we've been in conversations. I would say it's very early days on open banking. The way we approached our comments was really to think through the risks that we think are posed. Those were aligned with what the government identified in its consultation paper: concerns around consumer protection, privacy, financial crime and financial stability. We focused primarily on the first three, and we talked about potential risk mitigation strategies, both from a regulator perspective and from a more industry-led solutions perspective.

That's how we have framed our thinking on open banking. It's really early days, and we're continuing to have discussions with the government when it asks us to provide some views. However, yes, it's early days and there's still a lot to come.

● (1610)

Mr. Michel Picard: The fact that—

Ms. Della Shea: Sorry, do you mind if I add to that?

Mr. Michel Picard: Please do. You're the expert. I'm not.

Ms. Della Shea: Symcor provided a submission to that call for papers as well.

Our recommendations really came down to what I had outlined earlier this afternoon in terms of recommendations primarily around privacy by design and security by design. As well, we had a framework to assess all actors in that ecosystem, with the concern potentially being vulnerabilities, essentially the weakest link vulnerabilities, so having an appropriate assessment process to ensure everyone in that ecosystem was maintaining at least a minimum level of privacy and security.

Essentially, what we recommended was ensuring that privacy and security was really cherished above all—so we were thinking about the utility, the convenience of open banking—and also that protecting Canadians was really paramount.

I think that, again, as Marina mentioned, it's early days. It is an important mandate for the government to be considering and looking at, especially with developments internationally. I also believe that it's an opportunity to look at international standards. Again, it's a little bit of go slow to go fast, potentially.

Mr. Michel Picard: Actually the system managed, duplicated data everywhere, and the open banking system concept proposes that we have just one place where the data is, and the exchange of information where the different data needs to be combined and used.... If you have a unique system where you have unique data—at least unique sources—the apparent beauty of it is that you don't look everywhere. It's just in one place. You need a very sophisticated security system to avoid a breach, because if you are breached, you lose everything. Is it a calculated risk?

Ms. Marina Mandal: I think you've hit on, absolutely, what our key concerns were as the Canadian Bankers Association around cybersecurity and financial crime more broadly in the context of open banking, where, as you know, the customer consents to have their personal and financial information transferred to another provider, whether it's a bank or perhaps a fintech that's not as stringently regulated as banks.

Once that happens, and if that information then goes further down the line, the third party provider provides it to another party, we worry about both the increased connectivity and the proliferation of entities having access to the data. That definitely makes it harder in the case of a cyber-attack to determine your points of vulnerability, number one and number two. Again, not all third party providers will be regulated the same way.

We were pleased to see in the budget this year the announcement of the cybersecurity legislation forthcoming, but we worry about entities that might not be subject to comprehensive regulatory oversight on both privacy and on cyber.

Mr. Michel Picard: Ms. Shea, in your opening remarks you mentioned the word “trusted” many times. What are the criteria for someone to be a trusted supplier? In business, there's no such thing as trust—

Ms. Della Shea: So—

Mr. Michel Picard: —and in politics, I guess.

Ms. Della Shea: The term “trusted provider” to me is really that you have a commitment to what your values and standards are right from the get-go, and that you have support from the top of the organization all the way to every layer.

Essentially, that's necessary to actually do what you promise to do. It's not enough to just have a statement or a policy saying you're going to protect privacy. You really need to have the infrastructure, the communication, the buy-in across everybody who is involved in delivering a service. They need to understand, number one, what their goals and obligations are, and number two, that they have the tools to be able to execute on those things. That really requires a commitment. It requires understanding across the entire organization, and understanding really comes down to making things simple and easy for anyone to be able to understand what they have to do to achieve that trust or to achieve that commitment. In this case, we're talking about privacy, so what does that mean? It means making everyone understand.

At Symcor, we did this by implementing a set of data values. We have a set of data values that stand for privacy, accountability, compliance and trust, and we leverage these values to be able to communicate to everyone. It's not just a bunch of things that are buried in a policy. These are the things that you commit to doing every day. That communication is enforced through a lot of interesting and fun activities. We host an annual data privacy day, where we have quizzes and games. We have training. Our data values are actually represented by a little mascot, which is actually an owl. He's quite popular across the organization. People look forward to his little notes and messages.

It's about doing what you say you're going to do, and then standing behind it with the commitment, whether it be a financial commitment, because it does require that level of commitment as well—

● (1615)

Mr. Michel Picard: Thank you.

The Chair: Thank you, Monsieur Picard.

Next up, for five minutes, is Monsieur Gourde.

[*Translation*]

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

I'd like to thank the witnesses for being here today.

In this digital ID universe, I think Canadians not only deserve, but also have the right, to know that their personal information will be kept confidential. I'm concerned about digital data being stored outside Canada, where the data would be subject to foreign laws, not Canada's.

Do you think Canadians' digital data should be stored in Canada so we can more easily address problems that arise in the future, or can we assume foreign laws are comparable to Canada's and thus we have nothing to worry about?

[*English*]

Ms. Angelina Mason: I'll have Ms. Mandal speak to the actual data component of digital data, but in regard to the requirement that information be kept secure, as I said earlier, our privacy framework enables us to have data in Canada and outside Canada provided we have appropriate contractual and other measures to ensure the same level of safety.

Ms. Marina Mandal: On the data point as it ties into digital ID, I want to make sure we understand. I know you've heard from SecureKey, and I'm using SecureKey as an example because they are a live, private-public sector partnership that is in market.

The triple-blind authentication they talked about means no one has actually seen data. Let's say I go to the bank, or I use my bank credentials to log in to the CRA. The bank doesn't know that; the CRA doesn't know who my bank is, and SecureKey doesn't see any of that. The way the technology works is that no one is seeing anything. It's all done in such a way that, obviously, I am opting in, I am consenting, or I am proactively using the product. Digital ID isn't that flow of data back and forth; it's not the open banking situation. It's really just the authentication and attribute validation components of it.

[*Translation*]

Mr. Jacques Gourde: Earlier, you recommended that these new technologies be implemented within an appropriate time frame to make sure they are useful and work well. By time frame, do you mean one to three years, three to five years or 10 years?

[*English*]

Ms. Della Shea: I just want to make sure I understand the question. It's about the horizon to implement technologies in a safe way.

I believe it's an ongoing process, so I don't necessarily believe there's a specific time element tied to this. Technologies are not all on an equal playing field right now. Some are much more mature than others. If you look at large players that have invested significant amounts of time, energy and funding into those technologies where there is history, those are things that could be more readily adopted.

I would caution, however, as new technologies come to market, that we need to have an effective way to do proper assessment to ensure that those technologies are achieving the actual goal. That goes beyond just privacy and security to ensuring that the utility and functionality are doing what was originally intended. I believe it's not one size fits all. There could be a tiered approach to doing an assessment of technologies in terms of established technology in the marketplace versus ones that are emerging.

● (1620)

[*Translation*]

Mr. Jacques Gourde: In terms of conducting effective assessments, should these new technologies be deployed gradually, starting with a single sector, city, region or province, say, as opposed to the entire country, so as to avoid the kinds of problems that arose with other services?

[*English*]

Ms. Della Shea: That's an excellent recommendation. Essentially, if you assess once, you can apply it multiple times, and that's an important efficiency play. As I mentioned earlier, Canada Health Infoway has a structure whereby they certify a technology. This essentially enables others to leverage that technology within the health care industry without having to do the same assessment over and over again.

Ms. Marina Mandal: I can add to that. I completely agree that is a great idea. It's a way to iteratively test without putting customer information at risk. To flag a couple of places where it's happening, in New Brunswick the government has rolled out digital IDs—I'm specifically talking about the technology around digital ID—only on a pilot project basis. In British Columbia, I believe that's the intent as well.

Illinois is using digital ID specifically for tracking who's licensed to be a doctor, so there's that kind of use case as well. Maybe the need is very high there for whatever reason. There are use cases based on the technology used, as well as those based on the type of identification authentication problem you're trying to solve for.

[*Translation*]

Mr. Jacques Gourde: Thank you.

[*English*]

The Chair: Thank you, Mr. Gourde.

Next up, for five minutes, is Mr. Erskine-Smith.

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

I have some questions about digital ID, but my first question is more privacy focused.

On October 24, I made a purchase at the Ontario Cannabis Store, and it took weeks for the purchase to be delivered because the Ontario provincial Conservative government can't even sell weed right. Eventually it arrived, and it was recorded on my credit card statement. That's fine. I'm a Canadian citizen. It's legal to purchase cannabis online, as it ought to be. It's not legal in the United States though, so we hear stories about Canadians crossing the border and being asked if they have consumed cannabis in their lifetime, because it remains a crime in most places in the United States.

What assurance do I have as a Canadian that the credit card statement that acknowledges my transaction of a licit purchase in Canada but an illicit activity in the United States is protected and secure, and that my privacy is safe?

Ms. Angelina Mason: On that point, if you're talking about where that transactional data information is housed—let's say for example it is housed in the U.S.—the only way that data could be accessed for the purpose of seeing whether or not you are meeting this question would be through a formalized warrant process under the Patriot Act.

I don't anticipate that as being something that would be a real problem. I don't think it would be applied that way. That legislation's really intended to address cases of national importance, not an individual's particular use of a substance. I don't see that being something that would be of concern.

Mr. Nathaniel Erskine-Smith: Have banks turned their minds to the question, when Canadians are engaged in legal activities here that are illegal where we would commonly travel, like the United States, of ensuring that the records of those activities are not liable to be accessed by American authorities in any way?

Ms. Angelina Mason: Just to clarify that, we would have contractual protections to ensure they're not shared, although there would be the possibility that you could have a proper warrant served in that country. However, I can't anticipate that a warrant would be served in that context, because if it were something so significant as to come under the Patriot Act, I would imagine it to be something in the nature of a national crime, not an individual, one-on-one use.

Mr. Nathaniel Erskine-Smith: I'm less worrisome, in all probability.

With respect to digital ID, in your opening comments I noted you are ready and willing to help the Government of Canada. We had Alex Benay in front of us and he spoke about federated digital ID as well, and some steps they've taken toward that. From the perspective of the Canadian Bankers Association, what are the next steps that have to be taken to get us closer to this federated digital ID?

● (1625)

Ms. Marina Mandal: What's extremely important is the work being done by DIACC on the pan-Canadian trust framework, PCTF. For a lot of the questions that have been asked so far by this committee and the things we have spoken to—privacy, data security, standards that operate across borders, transparency of governance, open standards—the intent is to have them be worked out and put in place through the pan-Canadian trust framework.

In terms of timeline, the anticipated completion of the trust framework is next year. There are discussion drafts that are being produced right now for public comment, so targeted for 2020.

That's a crucial first step. The standards include privacy by design, so there are 10 principles underlying a digital ID ecosystem.

The other great thing about the DIACC pan-Canadian trust framework process is that you have different levels of government at the table, different private sector players at the table, and technology companies that could help build a solution from a tech perspective. That creates the interoperability.

On principle, the federal government is in the process of developing, or is intending to develop, with, I think it's Sign-in Canada, its own digital ID solution, but you have SecureKey's digital ID solution, which also is intended to meet what the PCTF will look like. That allows the federal government, for instance, or a provincial government, to say that you can use either. If you go to New Brunswick right now, where they're running pilot projects on digital ID, you can log in to the New Brunswick pilot project by entering either your New Brunswick government-issued digital ID or your SecureKey Concierge digital ID.

To me, that is the immediate next step. Another broader part of it, where the Canadian Bankers Association has been playing a role, is just socializing the concept, ensuring, as one of the MPs just said, that Canadians feel safe. They need to understand the product, because Canadians hear about cyber breaches all the time. That's also the educational and promotional part of digital ID.

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

Next up for five minutes is Mr. Kent.

Hon. Peter Kent: I'd like to continue on that point. One of the challenges in Canada, unlike Estonia, is public skepticism about the protection of on one hand their health records and on the other hand their financial records. That's with regard to the CRA, not necessarily with banks, although as Mr. Angus said, certainly fraud is an increasing problem and there are any number of ways. Although the banks have countered it quite effectively, I too have had credit card breaches where the bank has notified me within minutes of an attempted use of a card and its number.

Would the private sector recommend pilot projects on a fairly limited, even a semi-regional basis, given the fact that generationally we have Canadians who do not use digital devices to any great extent at all, even with regard to still insisting that there be a human teller at their bank and that their transactions be conducted on paper? Would you recommend a scaled-down, fairly narrow pilot project, unlike New Brunswick, but perhaps urban centres first, in a certain reduced way?

We've seen in Ontario, for example, in Toronto, an inability to implement the digital exchange of medical information between GPs, specialists, hospitals, clinics and so forth. They've been talking about that for 20 years now, and it's still an incomplete, imperfect project. Would you suggest pilot projects in one particular area? It could be health care or CRA-related, but again, on a very limited scale, could developing a success model give confidence to more resistant demographics to embrace and to engage?

● (1630)

Ms. Della Shea: I believe doing a pilot makes practical sense for a number of reasons. Just the sheer scale of trying to onboard folks and communicate and educate individuals about what this means would be untenable.

In terms of conducting a pilot, however, I would urge that it be on an opt-in basis, for the purpose of developing something with the intention of iterating, so ensuring that you're not trying to bite off everything and be perfect, but just beginning that engagement.

It would also be a really practical way to start introducing the concept, especially if it's set out so it's an optional activity where the folks in charge of developing the solutions would take that information. Having that public engagement would be an interesting model, but certainly knowing and understanding going in that it would be an iterative process would be important.

I believe that's really what privacy by design principles are really about. It's about understanding what the requirements are up front, then all along the way it's going back and checking whether we met those initial requirements and met that intent. Then it's taking that feedback and iterating again and again.

Ms. Marina Mandal: Thank you.

I want to underscore that on the public skepticism point, I agree one hundred per cent. We talk a lot about innovation these days, definitely in the banking industry, and obviously this committee has been looking at digital transformation in the government context. Crucial to consumer trust is knowing that primarily, the privacy data security will be protected.

That's our starting point. Part of building that, as I referenced earlier, is this public education role that I think the public sector and the private sector have. It is explaining to people that digital ID isn't a company you just heard of, SecureKey, handing over all your data. They are not actually seeing it, right? Going through that explanation process using as plain language as possible is very helpful.

Then, we need to ask whether the people in the ecosystem are abiding by the standards and principles. Can everyone agree on them, and are they at a high enough level?

There's a difference between having a bank, or a telecommunications company or a provincial or federal government authenticate you online versus Facebook or any other social media company, solely because those are self-created identities. There's no fundamental, government-issued identity underlying that.

When you talk about digital ID and parsing out public appetite, it's just going to be public appetite as well, based on who you're bringing to the ecosystem, what kind of products they are offering, and the optionality and convenience for the consumer.

Hon. Peter Kent: In the case of the New Brunswick parallel projects, the two approaches, is there any early evidence that would give a taste of the user satisfaction?

Ms. Marina Mandal: I couldn't find much information on it. It seems to be a fairly closed pilot project that's just beta testing the technology on both sides: the New Brunswick government's technology as well as the SecureKey Concierge, which has been in place for a while.

I'm sorry. I didn't quite respond to the pilot project point.

It's interesting. You have heard from both me and Ms. Shea today about the importance of pilot projects in use cases, but if you take something like SecureKey Concierge, about seven million to eight million users are now signed up to the system. It started in 2012, so in seven years that's a significant part of the Canadian population. You never know with a pilot project how it might take off and really demonstrate a broader social desire for something that, frankly, makes Canadians' lives easier.

Hon. Peter Kent: Again, though, it's selling the cost-benefit concept.

Ms. Marina Mandal: Exactly.

The Chair: Thank you, Mr. Kent.

Next up is Ms. Vandenbeld, for five minutes.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you very much for sharing your expertise with us today.

I think it was you, Ms. Shea, who talked about the fact that there will be cyber-attacks, and that one of the best ways to get around that is by sharing intelligence.

Who did you mean in terms of sharing intelligence?

Ms. Della Shea: I believe the concept of sharing intelligence is going to be increasingly important, and sharing intelligence across sectors is going to be something that will be very important to consider.

Within various industry sectors there are limitations in terms of information being shared. At Symcor we have a limited use case around providing the capability for our clients to do limited information sharing for the purpose of detecting fraud, not cyber-attacks—that's something we'd like to get to—but fraud. The intention is really to have a locked-down, controlled process that is very focused on the intent of that use case, which is to get ahead of those bad actors before the event, or the effect of that event, actually happens.

Certainly public-private partnerships are an area of discussion south of the border. Having a framework to be able to share that intelligence with that purpose will be increasingly important.

Overlaying that, however, is having strong privacy governance and oversight, because often there is this tension between security.... We need as much information as possible for the purpose of getting ahead of the bad actors quickly, but I think there is definitely a point in the middle that can be met. It's about enabling increased data sharing, but under a privacy governance umbrella.

● (1635)

Ms. Anita Vandenbeld: Moving from the private sector to government, how would that work? As you've indicated, sharing anything, even between departments, let alone between government and the private sector, could raise a lot of privacy concerns. How do you ensure that you're sharing information for the purposes of keeping out or learning what the bad actors are doing, so that you can secure your systems, without creating those access points to share information?

Ms. Della Shea: It definitely requires a layered approach from the infrastructure to be able to do this. Having security privacy embedded into that design is really critical. Certainly in the Estonian model there is discussion around the use of blockchain as being a potential opportunity to enable that. Dr. Cavoukian has discussed the importance of having privacy by design embedded into that, and not assuming that would take place.

The other layer is also around the legislative framework and being able to enable that sharing, but again, it's very use case specific. I must stress that trust will underpin everything, and having a legitimate, purposeful, reasonable reason to do this data sharing is going to be absolutely critical. The implementation is really going to be about the standard people, process and technology in ensuring that you have that ongoing process to keep it working.

Ms. Anita Vandenbeld: Do you want to respond to that at all?

Ms. Angelina Mason: There can be sharing that doesn't involve personal information. The banking industry has had a number of public-private partnerships over the years whereby we shared threat intelligence, so you can actually share the types of cyber-threats we're seeing.

With the introduction of the Canadian Centre for Cyber Security, we see that as the hub that will then build on these types of initial partnerships and make them much broader, so sharing between the private sector and the government. Then, also, there is the added benefit of sharing internationally.

We are very much looking forward to participating in that hub.

Ms. Anita Vandenbeld: How would emerging technologies impact this? I'm thinking in particular of artificial intelligence. Is this an area where artificial intelligence could be applied in order to be able to detect those types of threats?

Ms. Angelina Mason: Absolutely. This is all about connecting the dots, so the more you can harness artificial intelligence to do the analytics to make those connections, the better.

Ms. Della Shea: I totally agree with Ms. Mason. Artificial intelligence and machine learning are technologies that can actually enhance privacy, because they take out that human element.

I also would like to reiterate the importance of having that use case and staying very true to the use case. There isn't going to be a one-size-fits-all opportunity, so you need to ensure that you have a framework, and that for each and every use case you want to undertake, you have a way to guide it from beginning to end.

The Chair: We're out of time. We just crossed the line.

We have three questioners left. We have Mr. Angus for three minutes, and Mr. Fortier and Mr. Baylis after that. That's all I have on my slate as of now.

Mr. Angus.

Mr. Charlie Angus: Thank you.

Canadians have enormous respect for Statistics Canada, but when Statistics Canada decided to share financial data to get better information, there was a huge blowback, which suggests Canadians are very particular about this kind of integration of financial information with government.

Where do you stand on that? Are you sensitive to the fact that people don't want that kind of deep integration between their personal financial information and government, even if it's anonymized?

● (1640)

Ms. Angelina Mason: Yes, we are very sensitized to it. I would note, first of all, that when Statistics Canada moved to compel the banks, we were not aware that was happening. When it did take place, we obviously had serious concerns.

First of all, I want to clarify that no personal financial transaction data has been provided to Statistics Canada. We were very concerned about the protection of the privacy and security of our customers' information, and obviously, very encouraged to see the Privacy Commissioner conducting an investigation in that regard.

There is a sensitivity, for sure, about that level of data. The banking industry has had a long relationship with Statistics Canada, providing them with information that's helpful, but it's always been at an aggregated level, such as mortgage default rates. We had significant concerns with the nature of the request. We thought our discussions were at the exploratory stage, where we were raising all of these flags, and we were obviously very surprised that it went the way it did.

Mr. Charlie Angus: Thank you. It's actually very reassuring to hear that, because we certainly heard from many citizens who were deeply concerned.

I just want to end with what I began the conversation on, which was the issue of fraud. We've been studying here the danger and the power of AI, which is going to start to transform all manner of online life. There are deep fakes, and the ability to target better and better by getting more and more personal information, which is why breaches of personal information are so dangerous in this age.

I'm interested in training. If you're at a bank and someone makes a lot of inappropriate transactions because they have a gambling addiction, that's not necessarily illegal, but someone else may come in and want to make all kinds of withdrawals in order to pay for someone who doesn't exist who's running a criminal gang in eastern Europe, because they're being suckered. Someone may have a deep fake video that's saying they need this money, but they're in Europe.

There are all manner of new elements that we haven't dealt with before. In terms of training your staff, because it's your front line that's going to deal with a lot of this, how is that being done? Are tellers being trained? Are you monitoring at the teller gate?

Ms. Angelina Mason: Yes, there's a meeting of bank personnel to identify what we call the flags, where something is unusual. There are also electronic triggers. When you see unusual transactions within an account, they will be pulled out. It's both by human factor and electronic monitoring.

The Chair: Thank you, Mr. Angus.

The last person up today is Ms. Fortier.

[*Translation*]

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

My apologies for being late. Something unexpected came up in my riding.

Ladies, I missed your presentations unfortunately, so I've based my two questions on the notes you provided. I hope I don't make you repeat anything you've already said.

Ms. Shea, my questions are for you.

However, should Ms. Mason and Ms. Mandal wish to comment, please do so.

Ms. Shea, in your presentation, you indicated that “as the government considers its approach to rendering services to Canadians,” you would urge it to adopt “a data stewardship model.” Could you list two or three advantages of such a model for the government, as well as the risks involved?

[*English*]

Ms. Della Shea: Are you referring to the risks of adopting a consistent approach?

[*Translation*]

Mrs. Mona Fortier: Yes. Does the approach pose any risks?

[*English*]

Ms. Della Shea: Just so I understand, was the question about implementing systems and what are the risks?

Mrs. Mona Fortier: This says that you want to adopt a model of management of data. Are there risks that we should be taking into account if we choose to adopt that type of model?

● (1645)

Ms. Della Shea: That's a good question. I can't think of any risks in terms of adopting a model around sound data governance and sound data management. I believe that by having these controls and these methodologies and processes, you're really setting the government up for a win-win scenario.

As Mr. Angus discussed, around the issue with Statistics Canada, that's an example in terms of where the potential legitimate purpose of processing was not considered. A lot of issues potentially could have been handled better by having, first and foremost, a legitimate purpose and having purposeful and reasonable requests for information, and then having a sound governance process to ensure that, again, for whatever is stated is going to be the use, you have the consistency and you actually act on that.

[*Translation*]

Mrs. Mona Fortier: I will now ask my second question. Given your experience with Symcor's transition from print to digital and the expertise you gained, what should a change management strategy take into account as we move towards digital government services?

[*English*]

Ms. Della Shea: Thank you for that question. It is actually an excellent question, as the importance of change management should not be underestimated as you go from having a traditional service to a digital service. You fundamentally are introducing many new things to an existing set of stakeholders who aren't necessarily aware of how these technologies work, why they should use them and how it is going to impact their lives.

Understanding this up front and having a change management program and mandate to ensure that you engage all the stakeholders within your enterprise, or, in this case, government services, and to ensure appropriate training and awareness are going to become very critical. Also, that training and awareness have to be constantly reiterated, and at a level that's very basic, for everyone to understand.

It's also important to recognize that the speed of adoption is not going to be consistent. There are going to be early adopters and there are going to be laggards, and having a mechanism to bring everyone along that journey is going to be critical.

[*Translation*]

Mrs. Mona Fortier: Ms. Mason or Ms. Mandal, do you have anything to add on change management?

[*English*]

Ms. Marina Mandal: I think the CBA agrees with the thoughts that Ms. Shea has laid out.

We do a lot of work within our association on financial literacy. Arguably, there's some need for similar education on data and digital literacy, just so Canadians understand what is happening when they're handing over information, whether it's personal financial information or health information, etc.

The literacy component—and Ms. Shea spoke to this with her references to training and awareness—I think is really crucial. We just keep going back to how innovations will not be adopted if they do not gain the trust of Canadians. I would just confirm agreement.

[*Translation*]

Mrs. Mona Fortier: Thank you very much.

[*English*]

The Chair: Thank you, Ms. Fortier.

Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: I had given notice of this on Tuesday. While we still have time here, I want to move a motion to invite senior representatives of YouTube to explain the company's decision not to run political ads in the upcoming federal election and their refusal to comply with Bill C-76.

The Chair: Is there any discussion?

Mr. Angus.

Mr. Charlie Angus: I think it's an excellent motion. I'm interested in having YouTube here on a number of issues. I'm wondering if we can have it say "and issues relating to YouTube" so that we're not strictly—

Mr. Nathaniel Erskine-Smith: I'm fine with that.

Mr. Charlie Angus: There may be other issues that we may want to ask about.

Mr. Nathaniel Erskine-Smith: Sure.

The Chair: Do you have an amended motion or do you want to work that into your initial one?

Mr. Nathaniel Erskine-Smith: Sure. I'll just say "invite senior representatives of YouTube to explain the company's decision not to run political ads in the upcoming federal election, their refusal to comply with Bill C-76 and any other issues relevant to this committee".

● (1650)

The Chair: Mr. Kent, do you have any comments?

Hon. Peter Kent: Yes, I'd certainly agree. I would certainly support this motion, but as I think I mentioned in the last meeting, we also need to get the Chief Electoral Officer and the Privacy Commissioner here to explain their interpretation of what Bill C-76 is going to require parties and individual politicians to do with regard to data protection. That could be a follow-on from YouTube.

The Chair: To me, that would be a separate motion. Would you propose a separate motion?

Hon. Peter Kent: Well, I think there's a series of witnesses that are all related in this case. It would be relevant, I think, as a follow-on. I don't know, could it be a friendly amendment?

Mr. Nathaniel Erskine-Smith: Why don't we start with this and then we can talk amongst ourselves about how it develops.

Hon. Peter Kent: The intention to continue with this...yes.

The Chair: Okay.

Mr. Angus.

Mr. Charlie Angus: Yes, I think it's easiest to go with this. The door is open. We don't need to establish it like a full-out study.

Hon. Peter Kent: Yes, I agree.

Mr. Charlie Angus: The door may take us to a number of places. Let's go with this and then we'll see where we go.

The Chair: Is that fair, Mr. Kent? If not, another motion can be forthcoming.

Hon. Peter Kent: On the basis of the traditional collegiality of this committee, yes.

The Chair: We will vote on the motion before us.

(Motion agreed to [*See Minutes of Proceedings*])

Mr. Nathaniel Erskine-Smith: I have one final thing.

The Canadian Bankers Association, in their white paper, suggested a few specific recommendations, including legislative amendments that will allow us to move closer to a digital ID. I recognize that the pan-Canadian trust framework is the next step, but to the extent that there are specific recommendations that were not in your opening statement and that you did not get to in answering the questions, similar to that recommendation with respect to legislative amendments, it would be helpful, as we make recommendations to the government, if you would follow up in writing if there are any specific recommendations that you think this committee should be making to the government. That would be one example, and perhaps there are others, but I would appreciate it.

Ms. Angelina Mason: I will, absolutely.

The Chair: Is that it, folks?

Thanks, everybody. Have a good weekend.

The meeting is adjourned.