HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 139 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, February 28, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 28, 2019

● (1530)

[*English*]

The Vice-Chair (Mr. Charlie Angus (Timmins—James Bay, NDP)): Good afternoon. We're going to begin.

[*Translation*]

I would like to make an announcement first. There has been an uprising and I am the new captain of this committee. The anarchists have arrived.

An hon. member: Temporarily.

[*English*]

The Vice-Chair (Mr. Charlie Angus): Welcome, my friends, to the Standing Committee on Access to Information, Privacy and Ethics. This is meeting 139, pursuant to Standing Order 108(3)(h)(vii), for the study of the privacy of digital government services.

Today, we have two groups of witnesses. We have, from the Herjavec Group, Matthew Anthony, the vice-president, incident response and threat analysis, and Ira Goldstein, senior vice-president of corporate development. We also have, from SecureKey Technologies Inc., Andre Boysen, chief information officer, and Rene McIver, chief security officer.

Each group will have 10 minutes to present. We are pretty reasonable here, but when you get close to the 10 minutes, I will start to jump up and down very loudly, not to distract you, but just to let you know. Then our first round of questions will go for seven minutes and then we will go to a five-minute round.

Is the Herjavec Group ready to begin?

Mr. Ira Goldstein (Senior Vice-President, Corporate Development, Herjavec Group): Good afternoon. My thanks to the chair and vice-chairs and the members of the committee for the opportunity to speak today.

My name is Ira Goldstein. I'm the senior vice-president of corporate development at the Herjavec Group. I've spent the last decade working in information security to help companies and governments secure their most critical digital assets.

I'm joined by Matt Anthony, our vice-president of security remediation services at Herjavec Group, whose remarks will follow mine.

Herjavec Group was founded in 2003 by Robert Herjavec, who immigrated to Canada with his parents from eastern Europe. A dynamic entrepreneur, Robert has built Herjavec Group to be one of the largest privately held cybersecurity firms in the world. Our experience includes working with private and public sector organizations in complex multi-technology environments to ensure their data security and privacy.

We are honoured to address the committee today on behalf of Robert, Herjavec Group and our fellow Canadians.

Our statement will address two subject areas related to the committee's study. First, I will outline why digital identity is a key building block in the transformation of government services. I will then outline steps to manage, govern and secure our digital identities.

My recommendation is for the government to tread lightly on the broader transformation path to ensure that privacy and security are top priorities. In parallel, the government should move quickly on a pilot project to expand the existing success of Canada's digital presence.

Digital government services must be built on a foundation of good identity governance. If our identities are to be digitized and managed by government, citizens expect a system that ensures security and privacy. Our identity attributes are assumed to be protected by the issuer, our federal government. In any system, physical or digital, fraud is a risk that must be mitigated through effective and ongoing assessment.

These concepts are not far from realization. When a baby is born or a new immigrant arrives, individuals may request their identity documentation online. Ultimately, physical artifacts are issued as proof of identity, but the fact that we have an online portal today to provision identification means that we have the foundation to leverage that data for use in digital government services.

Several government services are already online. One of the most critical functions of government, tax collection, is digitized through Canada Revenue Agency's EFILE system. Presumably the push to EFILE was supported by efficiency outcomes and stands as a successful case of digital transformation.

Any further steps to digitize citizen identity must consider the perception of the impact on individual privacy. Individuals may perceive digital identity as a threat to privacy despite the expected benefits. One recent example is the speed at which public perception soured over Statistics Canada's plan to collect personal financial information. Despite the involvement of the Privacy Commissioner and plans to anonymize the data, perception quickly turned negative toward this prospect.

The contrast between CRA's EFILE success and Statistics Canada's attempt to gather financial information is a guiding light for the committee. Digitizing government services will be welcomed by the public if managed and messaged thoughtfully. The upside of this effort is more access for historically marginalized groups and geography, so the opportunity cannot be ignored.

Historically, identity-proofing has required a trusted centralized authority to govern provisioning and usage. If I want to prove who I am, I need to show government-issued identification. I foresee this authoritative proof as a permanent feature of modern democracy, so despite the advances in decentralized identity, the government has an important role to play in identity management.

In sum, I strongly recommend that the committee seize the opportunity to further digitize components of citizen identity to enable the efficient and secure delivery of government services, while being cautious in the line that we must draw between centralizing data and ensuring that individual privacy is maintained.

● (1535)

Mr. Matthew Anthony (Vice-President, Security Remediation Services, Herjavec Group): Thanks, Ira.

My name is Matt Anthony. I'm the vice-president of security remediation services. I've been working in information security for over 20 years. I'm honoured to be here today to address the committee. I'll keep my remarks focused on two main areas.

Firstly, I'd like to address the issue of e-government, specifically the pace and volume of change. There have been great successes. Ira has already mentioned tax filing. You can do anything from tax filing to pet registrations at all levels of government. I think we're seeing real advantages from some of those, but I also see that fear of missing out and reputation enhancement are drivers for a lot of the initiatives that influence the adoption of and adaptation to electronic government services.

Mark Zuckerberg, the founder of Facebook, is famous for saying, “Move fast and break things”. While that was taken on as a mantra for global developers in all areas of business and the private sector, I don't think the Government of Canada should or could have that same kind of capability to move fast and break things. Herjavec Group's cyber-incident response teams have see the direct impact of moving fast and breaking things. We come back and sweep some of that up. Breaches are large, costly and very damaging.

Adding to that, there is a global skills shortage in the core capabilities needed to securely govern, develop, test, deploy and maintain complex software systems. Current published figures show that there'll be about three and a half million cybersecurity job openings by 2021—that's worldwide, obviously. The global digital transformation is in direct tension with that. There are more projects, more services and more data being created, stored, managed and mined. Canada and Canadian governments will feel this tension very directly.

The committee has heard a great deal about three case studies. Ira mentioned this already, and I've heard some talk in the corridors about a couple of them. They are Sidewalk Toronto, Estonia and Australia.

I want to address the Estonian example briefly, because it's been held up as a high-water mark for digital transformation, but Estonia has had a few major advantages in doing this that Canada doesn't enjoy. They have a very small population, a very small geography, a relatively green field in the post-Soviet era for technology and a relatively homogenous population accustomed to central control.

When I talk about those things, I think you can reflect on Canada not having many of those advantages in trying to do these kinds of services. The model would look very different for Canada.

While that transformation appears successful, we also don't know a whole lot about the security and privacy concerns. The political and cultural aspects of what would be expected, including how much we might learn about security and privacy aspects, might not be evident for years, or even longer than that. I caution against using Estonia as a North Star for our transformations in Canada.

You can't stand still, obviously, and we have to move forward, but my hope is that we go slowly enough to be assured that the changes we do are fully governed and secured to the appropriate level. Go carefully according to strong principles. Wait for the necessary technology, such as AI and automation controls, to support us better. Don't allow fear of missing out in international comparisons to cause us to hurry ahead of our abilities and capabilities.

Secondly, I'd like to briefly address information-sharing. I want to commend the data strategy road map, in that there are six most important things laid out in that document. I can't do much more than say that they are precise and correct. I would like to amplify them.

The concepts are simple: develop a strategy; provide clarity on data stewardship; develop standards and guidelines for governance; improve recruitment to gather the needed skills; and, develop technology systems that support the strategy. Those are all easy to say, but enormously difficult to do, individually and severally.

In 1984, Stewart Brand presciently wrote, “Information wants to be free.” At the time, he was talking about how the technology costs were going lower and lower, but now it has become synonymous with the difficult problem of keeping access control. Once information is beyond the source's control, it will tend to get distributed widely. It follows, then, that secondary and tertiary uses of the government's data need to be as acutely and astutely controlled as primary use is.

The government faces a monumental task in understanding and managing legacy data and systems. Reconciling inconsistent or undocumented consents for use, information silos, usage rules, data structures, identity platforms and administrative processes will each also be monumental in scale.

I believe that taking a greenfield approach may be advantageous, that is, by establishing rules clearly for new data collection and allowing legacy data to be integrated in the future, as capabilities such as AI and other data collection and tagging can be paired with lower costs for transformation through automation. Don't rush to data lake models, as unexpected de-anonymization and information correlations will emerge—I've seen them—some of which may be contrary to public policy, law or intent.

● (1540)

There are a lot of assertions being made that opportunities will emerge and efficiencies will be achieved by aggressively mining, aggregating and sharing data. I urge the committee to show evidence for that. It's easy to get caught up in the rush to take that approach.

You cannot stand still, but I advise, indeed urge, the committee and industry to slow down, be more careful and do not allow ambition to overshadow capability. Go slowly enough to fully understand, measure and manage information risks. Remember, criminals like data, and breaches are messy, complicated and very expensive.

Thank you.

The Vice-Chair (Mr. Charlie Angus): Thank you very much.

We'll go to SecureKey Technologies, please.

Ms. Rene McIver (Chief Security Officer, SecureKey Technologies Inc.): Good afternoon. I am Rene McIver, chief security and privacy officer at SecureKey.

I'd like to begin by thanking the committee for giving us the opportunity to participate in its study on privacy and digital government services. My background is in crypto-mathematics, biometric standards and identity. I've spent time at the Communications Security Establishment and have been with SecureKey for the past decade.

I'm joined here today by my colleague Andre Boysen, our chief identity officer and co-founder of SecureKey. Andre's been in the fintech industry for 30 years and is a globally recognized leader in digital identity and privacy. He also serves on the board of the Digital ID & Authentication Council of Canada.

SecureKey is a proud Canadian company. SecureKey has been the provider of record for the Government of Canada's partner login service since 2012, also known as SecureKey Concierge. We are a world leader in providing technology solutions that enable citizens to efficiently access high-value digital services while also protecting the security and privacy of their personal information. We do this by building highly secure networks that span and merge the strengths of the public and private sectors.

As we know, the digital age has ushered in a host of new services, business models and opportunities to participate in the world. Not long ago, it would be unimaginable to order a shared ride from a device in your pocket, or to confidentially access government services from your home. Today, we take these things for granted and often get irritated when we come across something that can't be done online.

It's not just about citizen expectation. Companies, governments and other organizations have strong incentives to move services and transactions online in order to enhance client experiences, realize cost savings and increase business surety. An organization's ability to do this hinges on a single question: Can I trust the person or digital identity at the other end of the transaction?

This digital identity challenge is equally problematic on both sides.

To recognize clients and provide trusted access to services online, organizations typically deploy a mix of analogue and digital measures to confirm identity and mitigate risk. As we have seen, however, these solutions tend to be complex and inadequate. As a result, confidence in them has suffered.

On the other side, citizens are asked to navigate a myriad of identification methods to satisfy the organizations they seek services from, without knowing where the information's going and in the face of a steady stream of news about data breaches and online impersonators.

These concerns are well founded. Fraudsters are collecting information to know as much, and sometimes more than the citizens they are impersonating. Standard physical cards are easily counterfeited, and it's often impossible to check their validity with the issuing sources. Even biometric methods, which have often been touted as the solution to digital fraud, are targeted by hackers, increasing the risk that biometric data may also be compromised.

These factors are driving complexity up, trust in the system down, and adversely affecting privacy—exactly the opposite of what needs to happen. Our siloed system is too hard for consumers to use and too expensive to be sustained.

The challenge we face is not simply a matter of finding the best technology, the right skills or enough money to fix it; rather, everyone with a stake in the system needs to focus on solving the digital identity problem that underpins all digital services. We need to bring data and identity information back under the control of the citizen.

To solve this challenge, we must find ways to combine the prime factors of identity. These factors are the unique things we know, like shared secrets; the unique things we have, like verifiable chip cards or mobile devices; and the unique things we are, like our fingerprints or our face scans. By combining these factors, we can resolve identity and give organizations confidence that their clients are who they say they are.

Experience to date proves that single-factor methods are not up to the task. This means that trusted networks—ecosystems of trusted participants—are needed. All participants must be involved in the solution, including, and perhaps especially, the citizens, whose control over their own data and privacy will underpin its security.

● (1545)

Only by combining the best aspects of each system can we solve the digital identity problem and rebuild the trust that is equally required by both organizations and citizens. For example, governments are the initial issuers of individual identities, including birth registries, immigration documents, permits and licences. Governments also can link their records to a living person by issuing a driver's licence or passport. But governments are not as adept as the commercial sector at knowing if that person is actually at the other end of a given digital transaction. Banks, however, successfully conduct billions of authentications a year.

Compared to other organizations, citizens only rarely interact with governments during their lives. They may renew a licence or passport every five years or pay taxes online once a year, but they will log in to their bank accounts several times a week. This frequency generates a higher level of trust and immediacy to that interaction.

Then think about mobile devices, which are both identifiable within a cellular network and tied to subscriber accounts through the user's SIM card. All parts have something valuable to offer within a successful network.

Imagine a scenario where citizens can choose to share information securely within a network made up of organizations that they already trust. This gives the ability to use a layered approach to proving identity. The citizens would access the network using their trusted online banking credentials on a mobile device that the telecommunications operator can validate, all to share reliable information from multiple sources, including information from digitally enabled government issued documents. Using this layered approach, we get a significantly higher level of confidence in the identity of the person conducting the transaction.

The trick is how to do this without becoming a surveillance network or creating a new honey pot of data. We need to establish the basis for privacy and trust while minimizing the level of data sharing going on between the parties.

Triple blind privacy solves this challenge. The receiving organization does not need to know the actual issuer of the information, only that it comes from a trusted source. The issuer does not need to know who the receiving organization is. And the network operators are not exposed to the unprotected personal information. That's triple blind.

What this means is that none of the transaction participants actually gets a complete picture of the user transaction. This proven formula has been recognized by the privacy community worldwide, including by the office of Ontario's information and privacy commissioner.

This is not the distant future. All pieces are already in place to enable a system that has authoritative information, provides receivers of information with confidence in the transaction and allows the citizens to fully trust the system as they control their own data in a privacy-enhanced way. This type of arrangement is the cutting edge and is happening now.

With the information and resources we have, Canada has the opportunity to solve the digital identity challenge and become the model for the world. These include co-operative jurisdictions, technologically advanced telecommunications and world leadership in developing new approaches, such as privacy and security by design, developed by Dr. Ann Cavoukian, as well as the pan-Canadian trust framework that's championed by the Digital Identification and Authentication Council of Canada. We have the opportunity to build services that can provide identity validation claims from multiple parties in a single transaction while ensuring complete privacy and control for the citizen.

Key factors for any solution to be successful will be citizen acceptance and trust and the potential to reach a large user base quickly.

The responsibilities to protect privacy and to provide a sense of security to citizens are fundamental factors in the success of any solution. It is critical that Canada's approach connects together the trusted parts of the digital economy such as finance, telecommunications, government and commerce. Only this will provide citizens with the confidence they demand to use the providers they already trust and to have access to the information they want to securely share.

The cyber-risk around digital identity is high. Any solution that does not involve both private and public sectors will be of limited success. It will perpetrate the siloed approach that is currently under strain and will not have the security or public trust to enable the digital economy of tomorrow.

Thank you.

● (1550)

[*Translation*]

The Vice-Chair (Mr. Charlie Angus): We will start the round of questions.

Ms. Fortier, go ahead.

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

My thanks to the witnesses for being here. I see you have a higher level of expertise than I do. I am very pleased to see that you have the expertise that will allow us to go further in this study and accomplish what we want to do.

Mr. Anthony, your expertise is very important to the committee. You said it was important to go slowly, which is interesting. However, it is also important to go surely. That's my understanding.

Everything in society is moving very fast right now. There is some pressure to move faster to meet the digital service needs of Canadians.

How can we strike a balance to do things right? If we proceed slowly, which government services do you think we should put forward first?

● (1555)

[*English*]

Mr. Matthew Anthony: I'm afraid that's a very specific question without a very specific answer, which is how you balance a very complex, multi-variant challenge with a simple clear strategy.

When Rene Heller from the Max Plank Institute described an innovation trap, he said it doesn't matter when you might want to launch a spaceship for interstellar travel; it would always be better to wait because you'll always overtake yourself because of technological change.

We can also see that with regard wondering whether or not to buy a personal computer this month or next. That's the same kind of innovation trap.

We're faced with that in public policy as well, in making considered decisions on a case-by-case basis about what data we're comfortable with and whether we can comfortably control the necessary aspects of information security and privacy before we make the decision to move forward. You have to do the research continually, which is the go-slow part, to make an assessment about whether we're ready to go through to production, which is the move-fast part.

Go slowly until you're ready, and then move quickly when you are.

[*Translation*]

Mrs. Mona Fortier: I understand. Thank you.

The second question I would like to ask the other three witnesses is about cybersecurity.

We know that things will evolve. How far do you think cybersecurity can go? Are there more effective and reliable innovative approaches that you would like to share with us and that we should consider?

Ms. Mclver or Mr. Boysen, do you want to go first?

Mr. Andre Boysen (Chief Information Officer, SecureKey Technologies Inc.): Yes. Thank you for your question, Ms. Fortier.

[*English*]

I would say that one of the tricks here is that cybersecurity and privacy is a very complex topic, and the challenge with the model today is that everybody in Canada has to understand how the system works in order for the security system to be effective. That to me is fundamentally bad design.

What I'd like to do is pick up on Matt's comments about Estonia. Estonia did an amazing thing for itself, but when it comes to digital ID, I'd say there are two key messages I want to deliver today. Message number one is that every government in the world wants their digital identity information to be sovereign. They don't want to be beholden to some foreign corporation beyond the reach of their jurisdiction. That's one challenge.

However, the bigger challenge is that identity is very cultural. What works in one country won't necessarily work in another. This is particularly acute in the example of Estonia. When it comes to national ID cards, I would say that there are only two types of countries in the world: the countries that have national ID cards, and the countries that hate national ID cards. I would say Canada, the U. S., the U.K., Australia, New Zealand and many parts of Europe are against this idea of a national ID card.

There are several reasons for this. Part of it is because of World War Two. We saw all of the harms that came from governments having these large databases. The government had no intent of harm when it created these systems, but when somebody came in after—the Germans—they created all sorts of unanticipated harms. We saw the danger of having all the data in one place. I would say that this, on balance, is a better scheme, but I'm not here to criticize what Estonia did. I think their model is very good, but they come from a different cultural place, and I think Matt made that point very well.

If we're going to do this right, then rather than looking at a country of a million, why don't we look at the biggest and most successful identity and authentication scheme in the world—the credit card scheme? We have six billion cards in circulation for payments around the world, and we don't see news breaking every week about a credit card being compromised here, or Starbucks having problems there, or users losing credit cards. We don't see that. Why is that?

The reason is that the global payment system is managed very differently from the online identity system we have today. As a consumer, I don't have to understand how the payment scheme works. I just have to know how to tap my card, and if I can do that, I'm good. When it comes to the cards, we've done two very clever things. One is that we made it super simple for the user—when I do this, I know I'm committing myself, so it's hard for a crook to trick me out of it. Moreover, I don't have to understand it. I know the barista can't change my $10 to $1,000 after I leave. That's the first thing that makes the global payment system safe.

The second thing that keeps the global payment system safe is that there's a trusted network operative in the middle. The crook can't pop up in the middle and say, “I'm a crook, I take Visa.” You have to apply to get into that network and you have to behave to stay in the network.

It's not the same as the Internet. On the Internet, it's very different. None of the banks in Canada send SMS messages to their customers for security. The reason is that they don't believe it's secure enough. The problem is that every other service does. Facebook does it, Apple does it, Netflix does it, Google does it. When my dad gets a message on his phone saying “Suspicious activity on your account. Please click on this URL: www.bmo.com.crookURL.com”, my dad doesn't know how a URL works, and he clicks on this thing, thinking it's going to go to BMO. Despite the fact that BMO has very good control—by the way, this is not about BMO, which has very good security controls in place—BMO's got a security breach on its hands because my dad didn't get what was going on.

So hiding the complexity from the user and having a trusted network operator is really important.

Now, I want to bring it back to something Rene said a second ago. The third thing that keeps the global payment system safe is user behaviour. When I lose my payment card, I will call the bank within minutes. I didn't call them up because I promised I would—I don't care about them, I care about me. I'm terrified that the crook who found my card is going to spend my money and I'm going to be responsible. That user behaviour, that self-interest, causes me to do the right thing and turn it off. That's what keeps the global payment system safe, which is very unlike the way we manage digital identity today.

So if we want to look to a model, rather than look at Estonia—though I do think that what they did is good for them—we should look at and learn from what we've done in Canada. We should look at our own experience here. Every other government in the world is looking at us and asking how we got this partner login service with all the banks in Canada. They all want that. Everyone else is looking here, and we're looking over there.

● (1600)

The Vice-Chair (Mr. Charlie Angus): Thank you.

Mr. Andre Boysen: We have an amazing story to tell here. We need to build upon it rather than trying to reinvent.

Mrs. Mona Fortier: Thank you.

The Vice-Chair (Mr. Charlie Angus): Mr. Kent, I'm going to have to take one minute of her time off yours. Is that okay?

Hon. Peter Kent (Thornhill, CPC): Collegiality prevails at this committee, so I would share my time if you feel it's necessary to do that.

The Vice-Chair (Mr. Charlie Angus): Continue, continue.

Hon. Peter Kent: Thank you all for coming in.

To pick up on that point, the Canadian Bankers Association is pursuing a digital ID program, but their CEO, in a speech in January, suggested that the banks could well play a central part in any national digital government network extension. How many levels of proprietary technology could eventually be involved and at what cost? Or would you suggest that after RFPs, after pilot projects, one digital technology vendor would be selected and run the entire show?

Mr. Andre Boysen: No. In fact, I'd argue that would be a bad thing.

To go back to my example of the global payment scheme, when we look around the world, we see five to 10 global payment brands—Visa, Amex, Mastercard, Discover and others. The reason they all exist is that they all serve their constituencies in a slightly different way. Some are merchant-focused; some are more consumer-focused. Some try to do it all. They all exist because they serve in the right way.

What's good about that model is that all of us can make different choices about our favourite financial provider, and we're not stuck with that choice. If you start with one bank and you say, “I hate this bank. I want to go to another one,” you can, and you can continue on as you were.

I think having a single provider of this whole thing would be dangerous. We want to have an open scheme so that we can have multiple providers. That's quite important. And it has to be based on standards, not on proprietary, lock-in technology.

Hon. Peter Kent: That would argue against the Estonian single-chip common card technology.

Mr. Andre Boysen: To draw the difference on that, Estonia is trying to make sure other countries do what it did, so that they're not doing their own thing—which is smart. Otherwise, if the rest of the world goes in a different direction, they're going to have to change. That's why they're out there evangelizing—and doing a good job of it, I would say.

We have that same opportunity. The challenge for us is that if we did what Estonia did, just as an example, and the U.S. decided to go in a different direction, then we'd have to change. The opportunity for Canada is to get our own house in order, get our own economy working, and then we can make this an export standard and create a gold standard for the world, because everyone else will be looking here and saying, “This is really cool. We want this.”

That's our opportunity.

Hon. Peter Kent: I think, Mr. Goldstein, it was you who suggested starting with a basic-scale pilot project. What size are you talking about? Would it be in one single government department?

Mr. Ira Goldstein: I think we should look at the services that are already online and the capability that's already in the federal government. The Canadian Centre for Cyber Security was a huge step forward in bringing that capability together. There is immense capability there, even if Canadians are just now starting to learn about it publicly because of that announcement.

We should look at the government services that are already somewhat digitized, and look at how we can leverage those together to get better outcomes for citizens.

I agree with a lot of what everyone has said, but I think interacting with services outside of government may be step three or four. Step one is to enable the digitization of government services that currently aren't digital.

One of the other reasons people are so confident in the banking system is the deposit insurance. There is backing that tells me if money is lost with a financial institution, it's probably not going to come out of my pocket as long as I follow the rules of the game.

I reiterate that I think government has an important role to play as the arbiter of that identity. Let's look at what is already digitized within the government. CRA is an example; let's add to that. Let's go through the federal government services and see how we can bring those together and leverage the existing digitization.

● (1605)

Hon. Peter Kent: The website in Estonia tells us that 98% of their population have been issued digital ID cards. Given human nature in Canada—the reluctance, the skepticism, the cynicism, the fear of or opposition to digital ID—would you suggest making it optional in any pilot project?

Mr. Ira Goldstein: When I say "pilot", I mean more that the capability should be piloted, but it should be available to all Canadians. I don't think it should be necessarily a pilot group, or one province or group. The capability should be piloted to a specific-use case. With the CRA example, you could just continue to expand it.

I'm not worried about the government having information about me as a citizen that they already have. Look back to the StatsCan example. The reason there was public outrage was that people said, "Hmm, the government doesn't have this information today. Now they want it. This is outrageous." Had we said—

Hon. Peter Kent: It was also the lack of consent.

Mr. Ira Goldstein: But if the information is anonymized, where is that consent?

If we had said we're embracing open data and we want certain aggregated, anonymized information to make the provision of services cheaper, better and more focused, a lot of people would have been really excited about it. Canadians are progressive with that mindset of moving to digital. It's almost more about how you do it than about what you do.

To Matt's point about treading lightly, you need to go slowly with it in that way, plan your communications carefully, but I think we all firmly believe that Canadians are ready for this. It's just a question of execution.

Hon. Peter Kent: Okay.

I have a chicken and egg question. The EU has brought in the general data protection regulation, or GDPR. There have been suggestions that Canada is far behind with regard to the protection of privacy, which has now been enabled—perhaps over-enabled or overprotected in some aspects—in Europe. Before digital government is implemented in Canada, would you suggest the writing of regulations similar to the privacy protections and guarantees of the GDPR?

Mr. Ira Goldstein: That's a big question.

I think Canadian privacy legislation is not something we should just say is insufficient. There are some good privacy frameworks here. It's a question of what are those definitions? What is "real risk of significant harm"? What does that mean to a company like the companies we help, who are trying to determine what they should tell the government when there is a security or privacy breach?

We need to make it more practical for companies and individuals to abide by these frameworks. I'm not saying that we should go all the way to GDPR. I'm sure we all have varying opinions on GDPR. Matt is shaking, now.

The reason people are abiding by GDPR is that there are financial fines behind it, and that's why there are a lot of—

Hon. Peter Kent: Absolutely.

Mr. Ira Goldstein: —consultants making a lot of money on it, and all of that.

We shouldn't go all the way in that direction, but we need to make it easier for Canadian business to consume that type of regulation in Canada. We need to keep that strong privacy framework, but make it easier for businesses to consume.

Mr. Matthew Anthony: Could I just elaborate for a second on Ira's comment and respond to your question on whether we should we go all the way to a GDPR-type answer?

The answer is yes. I think the global push towards having governments protect citizens, balanced with citizens maybe becoming less interested in privacy on an individual point level, raises the interest of government to protect citizenship collectively.

But what Ira said is really important and I tried to address it tangentially as well, which is making the expectations really clear about how to handle and manage data so that people understand what they are expected to do and how they're expected to do it before you start pushing stuff to the online realm. That is really very useful.

I can't tell you whether or not we need to make a change to our regulations, policies and practices, but at the very least making those transparent and easier, so that—

The Vice-Chair (Mr. Charlie Angus): Thank you very much.

I'll now speak for seven minute. Just to be fair, I will put the gavel beside the clerk and if I go over the time, he will hit me with it.

I find this fascinating, and Mr. Anthony seemed to tread lightly. I find that very surprising.

I used to be a digital believer, and in the digital believing world things were going to be better, we were going to move faster. The longer I am in this job, the more wary I get. I think "tread lightly" is a very interesting example.

I just want to talk a bit about my sense of how Canadians see privacy and digital innovation. I was talking with tech people in the U.S. and they were marvelling about and saying that we really take this stuff seriously.

We had a serious digital copyright battle that involved citizens and letter writing campaigns. The net-throttling issue was a big issue. It was Canada that did the first investigation of Facebook, but at the same time, as Mr. Boysen has pointed out, people here hate identity cards. I think of my voters and they would be up in arms over this.

We look at Statistics Canada as a good example of how not to do this. Statistics Canada has a worldwide reputation and the trust of Canadians. They thought they were doing something in the public interest, but it struck Canadians the wrong way.

What would your advice be to a government that may think that gathering more information is in the best interest? You talked about the danger of the opportunities they say will emerge from increased efficiencies from mining, aggregating and sharing data, but you're saying that we need to require evidence to show that. What are the parameters we need to be looking at on this?

● (1610)

Mr. Matthew Anthony: There is a lot bundled into that question —

The Vice-Chair (Mr. Charlie Angus): Yes.

Mr. Matthew Anthony: —and I'll try to set it out.

Firstly, I'll say that when you collect data, it's an addictive process. It's easy to do. You collect large amounts of data and you can't lose what you don't have. When I say “go slowly”, I want to reiterate that I see people on their worst days very often dealing with breach management. I see the outcome and aspects of the failure to do the things that I am advising to do.

How to balance out the issues of what data to collect, why you're collecting it, making sure that there is consent for its use are the real keys to answering your question, I think.

When we have historical data, consent to use might be very difficult to derive. I can't tell you what consent I gave to the data I gave to the federal government five years ago. I don't remember and can't tell you. I don't remember signing anything away. It was probably in the fine print. You can make a studied case that I did somehow give you, the government, my consent to do that, but if I didn't have clarity about that, if it weren't communicated correctly to me, then I am going to be very unhappy with you when you use the data exactly the way you said you might.

I think that communication and clear consent is probably at the centre of the Statistics Canada case in particular. But I would say, don't collect data you don't need, and be very clear about how you're going to use it and get clear consent for how you're going to use it if it's personal information.

The Vice-Chair (Mr. Charlie Angus): Thank you.

Mr. Boysen, I was interested in what you were talking about with the example of the banks. If I don't like the banks.... Actually, I go to my credit union, the Caisse populaire—

Mr. Andre Boysen: It's part of the service.

Some hon. members: Oh, oh!

The Vice-Chair (Mr. Charlie Angus): —and I have good service, and if I have a problem, they call me right away and we deal with that.

Our committee has spent a lot of time looking at how we access online. We don't have choice. This is what we found with Facebook, and this is what we're finding with Google. We've begun to talk about the issue of antitrust, which is not generally in the realm of our committee, but for the rights of citizens and protecting data.... I mean, if you have a problem with Facebook, what are you going to do? You can't do anything. You can't go to WhatsApp, because it's controlled by them. They control all the other avenues.

In terms of overall public policy, do you feel that the issue of having not enough choice in how we engage online and in how our private information is collected and used by the data-opolies has a negative effect overall on where we're moving?

Mr. Andre Boysen: Yes. The short answer is, yes, it's a problem.

I think we have to think about this in a very different way.

The challenge we have today with the architecture of the Internet is that every web service delivery organization is on its own when it comes to registering customers online. We can see what that's produced for all of us in the room. Some of us have ten passwords, some of us have 25, some of us have 100. Some of us have 100 but it's really just one, because it's all the same password.

So what we see in this model is that when everybody is by themselves, the only way we can have confidence that someone is really who they say they are is by having a very thorough enrolment process. This is particularly acute in government because your duty of care is so high. The consequence is that oftentimes the customer can't get through this process, and when they do, the problem is that you have all of the data. So when you get breached, you have to remediate all of the data.

We only have this problem online. In person, it's not as much of a problem. In person, we already collaborate and co-operate when it comes to identity. When I want to get a bank account, I bring in a government-issued ID and something from somewhere else and I can get a bank account. When I want to prove I've lived in Ontario for six months, I bring my bank statements to show I've been living at that address for that long. We already co-operate in the real world in doing these identity services. It's only online where we have this challenge.

So one of the things I would put to you is that one of the things you should be thinking about is not merely solving this from the government point of view but thinking from an economy point of view. The challenge, and one of the reasons the banks are here and they want to be in on the scheme, is that from a banking point of view, this is not that interesting from a revenue point of view. They want to be able to open bank accounts online and they want to take the risk problem down. The challenge they have is that they can't verify that the driver's licence is real. What the crooks do is to take a real driver's licence like mine, scratch my photo out, stick their photo in it and go get a line of credit; and they're defenceless against that type of attack.

What the banks want the government to do is to get its house in order and to make all government-issued documents ready to participate in the digital economy.

Back in 2008, Minister Flaherty put together a task force here in Canada to talk about how we were going to make digital payments work. That task force ran for about two years. I participated in it and the report that was produced by Pat Meredith—who did a very good job of running the task force—said that you can't have a digital economy and can't do digital payments without having digital identity.

With digital identity, the point is that it has to work across the economy. It's not about solving health care. It's not about solving the CRA's problem. It's about solving it for the consumer across the economy, because when you look at your own life, the counter is that you have to show up with your driver's licence to get the thing you want, and that takes a long time.

● (1615)

The Vice-Chair (Mr. Charlie Angus): I have to stop you there so that I can end five seconds short of my time, just to put that on the record.

Some hon. members: Oh, oh!

The Vice-Chair (Mr. Charlie Angus): Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you very much for your presentation.

I want to get some clarity, because you mentioned that there's an issue whenever we have a national identity card. But I would say to you that we already have subnational identity cards. We have a driver's licence; we have a passport; we have a social insurance number.

Mr. Andre Boysen: Yes.

Mr. Raj Saini: In Ontario I have an OHIP card. We might not have one number that's ubiquitous across the whole system, but we have cards underneath.

Mr. Andre Boysen: Yes.

Mr. Raj Saini: With regard to the Estonian model, I agree with you. I think the reason we use that or the reason we started with that is that Estonia is one of the countries that are more advanced than are maybe some others.

Mr. Andre Boysen: Yes.

Mr. Raj Saini: But as you said—and I agree with you wholeheartedly—or I think Mr. Anthony said, the population of Estonia is 1.3 million. They had a lot of greenfields. They had no legacy systems from the previous regime that they had under Russia. They have four million square hectares of land, half of which is forest. So they don't have any problems compared to what we have.

However, eventually, we will have to move to some sort of digital identifier. I'm asking you this question, Mr. Boysen, because I know your company. I'm looking at a March 2017 press release. In that press release, you wrote that IBM and SecureKey were working together to enable a new digital identity and attribute-sharing network based on IBM blockchain.

I really don't know what that means—

Some hon. members: Oh, oh!

Mr. Raj Saini:—but it sounded good. The reason I mention this is that blockchain would be one of those processes we could look at to see if there's any deviation. You mentioned credit cards. I'm a retailer, a pharmacist, so I know how difficult it was even to get credit card machines in my store, because of all the knowledge, all the paperwork and everything that had to be sent to them. Could blockchain, that technology.... Maybe you can highlight, now that you've been working with IBM for a year, how that has come forward. Could the government not adapt that?

Mr. Andre Boysen: The short answer is yes. The scheme we're proposing actually sees the government, at both the federal and the provincial level, being a key participant in the scheme. You're required to make it more successful. It could run without you, but it would be way more successful if you participate.

However, your point is right that we already have these documents that we use. We use the documents we have to get the things we want. That's how the current model works. We use the stuff we have to get the new service that we don't yet have and we want.

That's the way the real world works. It's only online where we have this problem because the documents aren't digitize. One of the asks is actually to digitize the government documents so it can participate in the scheme with the banks, the telcos, health care, insurance and the rest of them.

To get to your question about blockchain, there are a couple of things I hear. The first thing I would say is that the best way to be successful with blockchain is not to talk about blockchain, because the problem is that it is very laden. There are a lot of different ideas about what it is and what it isn't.

Secondly about blockchain, one of the things I would bring on is the privacy component. One of the properties and benefits of blockchain is that it's immutable; it will never change. The challenge is that when you put that together with the GDPR, with my right to be forgotten, if I sign up for your service and then say “I want you to forget me”, the only way to honour my agreement is to blow up your blockchain.

Putting personal information on blockchain is a really bad idea. This is standard industry wisdom now. However, what it is good for is integrity proofs.

I want to go back to the credit card example I gave you a few minutes ago. The challenge is, Raj, if I know enough about you today, I can be you on the Internet. The organization that I'm trying to fool is defenceless, because I have all your data. I got it from the dark web.

We don't have that problem in the credit card scheme. There are two types of payments in the credit card scheme. When I go to the store and I pay in person, the risk of fraud is almost zero for the reasons I outlined earlier. However, when I go online and buy something at Amazon, Amazon didn't get to see my credit card, so that transaction is riskier. It's called “card not present”. Today, all e-commerce is “card not present”. It's riskier.

Here's the thing: All identity today is “card not present”. We have no idea if these assertions that are being presented to us at the counter are real.

● (1620)

Mr. Raj Saini: So—

Mr. Andre Boysen: Sorry. I'm just going to answer your blockchain question.

What we're using blockchain for is integrity proofs. We use it as a method to implement triple blinds so the issuer of the data can demonstrate that they wrote the data and that's the same data that they gave to the user to present. The receiver can get the data and know that it hasn't been altered. Then the consumer can have confidence that we're not oversharing data. That's what blockchain is being used for.

Mr. Raj Saini: Thank you for that point. I appreciate that.

My second point is that the one benefit that Estonia has is that it has a unitary level of government.

Here in Canada, in the region I come from, southwestern Ontario, there are actually four levels of government, because we have a regional government. Now you have the federal government that is a repository of certain information; you have the provincial government that's a repository of certain information; you have a regional government that does the policing and other things, which is another repository of information; and all my property tax and everything is in another level of government, municipal government.

Mr. Andre Boysen: As well, you need user IDs and passwords for all of them.

Mr. Raj Saini: That's fine.

The thing is, though, when you look at taxation or at health, if I have to prove something, I might have to acquire information from different levels of government.

How do you get the interoperability?

It's not just one level of government. You can start off at the federal government level, but eventually, if this is going to work, you should have access to all the information that's reposed, deposited or held through the different levels of government.

Mr. Andre Boysen: I'm going to comment, and then Rene is going to add something.

The truth is, the way the world works today, every service makes its own rules. The organizations that you just listed all make their own rules. They want to keep that property. They want to force everybody to do the same thing, because they want to make their own business decisions.

However, what's important, as you said, is that when you talk to the driver's licence folks in Canada, they will tell you that the driver's licence is not an identity document. It just proves that you learned how to drive, yet you cannot sign up for any online service without your driver's licence. It's not an identity card; it just gets used that way.

The Vice-Chair (Mr. Charlie Angus): You have one minute left.

Mr. Andre Boysen: The important thing here is making sure that we can get a scheme that works for consumers across the economy.

I want to get Rene in, so I will just stop there.

Ms. Rene McIver: Briefly, the expectation for this service is that all of these departments and authoritative sources of information participate in this ecosystem so that when I as a user need to share information from these multiple sources, I can do that through the service with no expectation that the service is collecting any of that information to now create this new centralized honeypot that becomes another centre of attack.

The authority of the information is where the information stays.

Mr. Raj Saini: How much time do I have, 20 or 30 seconds?

The Vice-Chair (Mr. Charlie Angus): You have 15 seconds, but I'm being nice tonight.

Mr. Raj Saini: Okay.

I agree with you on that point. The one thing I like about the Estonian model is the fact that they have an X-Road system, where you have silos of information along the route. I don't know whether that's safe or not in terms of technology. I would never suggest that information be held in one place where it could be attacked, but I think that's what Estonia did. They have this X-Road that everything diffuses into.

Maybe you could comment. Is that scheme the same?

Mr. Andre Boysen: The scheme is the same.

Mr. Raj Saini: Okay.

The Vice-Chair (Mr. Charlie Angus): Thank you.

Ms. Rene McIver: Sure.

[*Translation*]

The Vice-Chair (Mr. Charlie Angus): We'll continue with Mr. Gourde for five minutes.

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

My thanks to the witnesses for being here this afternoon.

The unique digital identifier seems to be a way forward. However, I liked Mr. Anthony's rather moderate position that you have to take the time to do things right, for a number of reasons. First, we already have a digital service infrastructure available to Canadians, unlike Estonia, which started from scratch and went all the way to the unique digital identifier. However, the baby should not be thrown out with the bathwater.

We have already invested a lot of money to build digital infrastructures. Will we have to drop them and gradually replace them with the unique identifier, or will we be able to recover the base of the existing infrastructure? If we have to start from scratch, we will have to spend billions of dollars. Do you have any idea how challenging it is to provide this service to all Canadians across the country?

My questions are for everyone. I'm not sure who wants to answer first.

● (1625)

[*English*]

Mr. Matthew Anthony: I wouldn't mind answering that question, or at least contributing to the answer to that question. I don't have an opinion about whether it's a private sector or a public sector function to create that single digital identifier. I do know that, when I hear concepts that I'm going to use my bank or perhaps some other identifier, I have to understand that better. I do tend to trust that our public institutions maybe have more information that's more trusted, and might look at that. The scale, though, is immense.

I would start in the federal government at least looking at all of the different identifiers you have now and picking places where you could integrate and create a single authentication system that would allow high-fidelity identification for transactions that are happening within and around the government services. I would start there before I looked outside.

The scale is enormous, and I can't help but hear Andre's comments about how we have a good identifier physically and the problem only exists online. I would argue that our very weak tower of identifiers aggregating into a passport or a driver's licence document are not actually strong authentications. There's very little proof today that I am who I say I am. I am, but there's very little proof of that.

Mr. Andre Boysen: I just want to add to that by saying that it's not about having a single identifier; it's about having confidence about who's on the other side of the transaction. I have today already in my real life, both online and in person, lots of identifiers, and what's good about that is it allows me to segment and compartmentalize my life so that I can only share this much information with this organization and this much information over there.

A single identifier will allow somebody to see everywhere that I've gone across the Internet. The service that we have with the Government of Canada is that the thing you originally asked for was a service that had a single identifier. You wanted an MBUN service, a meaningless but unique number that I could use across government, and when we looked at this we said this is a terrible idea because you're going to create a surveillance network. You're going to be able to see everywhere: they went to the beer store, the doctor, the beer store, the doctor, the tax department. You could have followed me everywhere. I don't want this thing. We designed triple-blind privacy to solve that problem. It's not about getting to a single identifier. In government, the service we built actually gives you a plurality of identifiers.

When I go to each government department, I have a unique identifier that I only use there and that's a better scheme because my relationship is contextual. I don't have a global view of my data. I have very contextualized, compartmentalized view of my life and I want it to stay that way. I don't want a big honey pot somewhere. Giving people the tools and the capabilities to do this is important.

I just want to pick up on Mr. Anthony's comments for a moment, though. The passport is not an authentication document. We use it for identity to prove that you're in the government's book of names. Let me just share something that's really important when you get to identity. When you are asking who somebody is, you're asking two questions that have to be answered at the same time. The first question is: Does such a person named Andre Boysen exist? The government, without dispute, is the author of that record and has domain over that record.

The second question has to be answered concurrently: Is he Andre Boysen? If you can't answer those two questions at the same time, you can't do a good job. Awesome authentication that's really strong but you don't know who it is, it's not that helpful. You have to be able to bind it to who did it. If you can combine it with self-interest, then the users will do the right thing when they lose access to the credential, which means the crook gets shut down. An identity is three components and they need to be kept separate.

The Vice-Chair (Mr. Charlie Angus): Thank you.

Mr. Andre Boysen: The first part is the identity question: who are you? The second question is authentication: are you the person who showed up the first time? The third thing is authorization: what can I do inside your service?

That third domain is mostly what you've been talking about today. The first two questions are what we're arguing: it should be both a public and private service across the economy. We need all of these organizations to participate.

The Vice-Chair (Mr. Charlie Angus): All right, thank you.

I'm going to turn it over to Mr. Graham.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): It was a good answer.

The Vice-Chair (Mr. Charlie Angus): Yes, it was a good answer. That's why I've been so reasonable.

Mr. David de Burgh Graham: That's fair.

I don't have a lot of time, so I'll ask you to use...I'll call it “lossy compression” on your answers.

Voices: Oh, oh!

Mr. David de Burgh Graham: In the digital world, is there privacy without security?

● (1630)

Mr. Matthew Anthony: Yes.

Mr. David de Burgh Graham: There is privacy without security.

Mr. Matthew Anthony: Well it depends on how you think about that question. It deals with access, so a record can be kept private. You can talk about making it secure, but you don't.... It's a complicated question.

Ultimately, every aspect of privacy is expressed as a security control of some type. I think academically the answer is yes, but practically, no.

Mr. Ira Goldstein: I think if you flip that around and say that you can have security with varying levels of privacy, it's more aligned to what we're talking about here.

The reason that companies driven by advertising revenue are so popular is that it allows them to be better at the provision of services or selling you more things. The government should take a page from that book—with respect, obviously, to citizens' privacy—to say that the future of government is going to be a more directed and precise provision of services, and that can be secured at the level of privacy that the citizen is willing to participate in.

If we give citizens a trade-off to say that can do much more with government with the existing information we have if we can derive analysis from that, like the private sector does, and ask whether they are in, I think the overall answer from Canadians is going to be yes, if they understand what we're talking about here.

Mr. David de Burgh Graham: Okay.

Mr. Anthony, when you started answering the first question from Ms. Fortier, you had trouble hearing because the microphone was on and therefore your speaker was off. It was causing a problem. It ties to a point that I want to make about non-intuitive interfaces and that the biggest problem we have in security is the user. I checked and it's not on the record, and perhaps it should be.

Who is Kevin Mitnick, and could we talk a bit about that?

Mr. Matthew Anthony: Do you want to talk about Kevin Mitnick?

Mr. David de Burgh Graham: I think it's a really important point. He hacked a massive number of systems. He wasn't really using a computer to do it; he was using social engineering.

Mr. Matthew Anthony: Yes. In the industry sometimes, we don't like to talk about Kevin Mitnick being a hacker. He was a social engineer at heart, which meant he was working human and offline systems to get information, and then replaying that into trust relationships with other people and to some extent other computer systems. He got famous. He went to jail. He's now making a career from getting famous and going to jail.

When we look at the entirety of accessing computer information systems and stored data, if you're attacking that, you're going to naturally use the least effort. The least effort is almost always people. So it's not enough just to secure the technologies, you also have to help secure the people.

Mr. David de Burgh Graham: That's fair.

Yes?

Ms. Rene McIver: Sorry, I just want to add that we have to get to a point where we make the data almost useless. What is important is the validation that comes with the data. Therefore, if there is an attack—a social engineering attack or otherwise—where the data is collected by the attackers and somehow attempted to be invoked into the system, it's rejected because it's not coming from a validated source.

We want to make our personal information, on its own, useless. Give it to the attackers. Fine. They can't do anything with it it because they can't validate it properly.

Mr. David de Burgh Graham: That's fair.

Mr. Andre Boysen: That's the card-present identity idea. The only person who could have done this is somebody who had something that belonged to the real user, and the real user will turn it off when they lose it.

That's where trust and integrity will come from.

Mr. David de Burgh Graham: Another weakness I see is that when you're processing encrypted data, at some point you have to decrypt data to figure out what you're doing with it.

Is there any way around that? Can we process data without decrypting it? I know the EFF has worked on it a bit, but I don't know if there's been an answer to that.

Ms. Rene McIver: I think there are a couple of things there. It depends on who the “we” are.

In the service where there's an identity network, the network never needs to see the protected information, right? Sure, it has to send it. It has to hold it temporarily until the receiver of the information picks it up, but the network doesn't need to see the personal information. So, yes, you can process data without having to decrypt it.

Really, the encryption happens at the provider. The receiver of the information should decrypt it.

The other thing is about data minimization. We also need to get to a point where I'm not sending my birthdate to say how old I am or that I'm the age of majority; I'm sending a validated, “Yes, this person is over 19.”

Those two things together can add the security we need from a data-minimizing point and reducing the exposure of personal information.

Mr. David de Burgh Graham: I want to—

What's that you're telling me?

The Vice-Chair (Mr. Charlie Angus): Five minutes.

Mr. David de Burgh Graham: Is time up?

The Vice-Chair (Mr. Charlie Angus): Yes. Is that okay? You're doing so well.

Mr. David de Burgh Graham: I have at least five more minutes.

The Vice-Chair (Mr. Charlie Angus): I know you do, but I have to give them to Mr. Kent.

Hon. Peter Kent: It's always a hard reality.

Mr. Boysen, I'll come back to your point. The NEXUS card uses biometrics, not at every occasion, but there's a place.... And sometimes the Canadian passport does; we're using the iris or the fingerprint. Is that the sort of double perfect-positive identification that you're talking about?

● (1635)

Mr. Andre Boysen: Yes. What I liked about the NEXUS card is it gave consumers choice. If you told Canadians they had to get a retina scan to get a passport, there would be outrage.

Hon. Peter Kent: Yes.

Mr. Andre Boysen: However, when you gave people a choice, saying, "If you want to get through the airport faster, submit your biometrics and you can get through faster", lots of people made that choice. By providing choice it was accepted.

I would also say your own GC login service, the partner login service, also gave choice. You did not compel Canadians to use the bank account to get to CRA if they didn't want to. They could still use a government-issued user ID and password. By giving choice, that gave comfort. You're not compelling me, so I'll try it out and see what happens. That choice element is a key component to getting the adoption of schemes like this.

Hon. Peter Kent: The iris identification technology in the NEXUS card, which has to be purchased, would seem to be a huge mountain for the government, for the finance minister and his budget, to climb.

Mr. Andre Boysen: I would argue that's not really a good thing for online service delivery. It feels heavy-handed to do a retina scan if I'm trying to vote. I would argue that each of these things needs to be used.... We need to look at the spectrum of services and then the level of assurance. Not all of these things are in the same kind of category.

For low-level assurance services, we don't need as much trust, so getting to that higher level is not as important. What's also important about the retina scan and the NEXUS card is that it's done in a controlled environment. I have to go to a controlled kiosk with people watching me so they can see if I'm tampering with the machine or mucking about with the card. It's that controlled environment that gives them the confidence to do it that way. You couldn't do a retina scan from home, as an example, with any kind of confidence, because it could be a replay attack.

Hon. Peter Kent: Yet.

Mr. Andre Boysen: Yet.

Mr. Ira Goldstein: Yet maybe you can if we're trying to learn from the private sector and look at one of the more elegant authentication methods that exist today. On a smartphone, it's made biometrics and now face ID just ubiquitous. It is heavy-handed to do a scan of your face every time you want to unlock your phone, but do you know what? Now that's the reality, people don't seem to mind it because the technology is so good that they want access to it and it's easy for them.

I think we need to take a page out of that book. There are ways in which authentication is being handled today where they're doing a biometric every time you want to open your phone. And it's not a new system, but an existing system that's in place today.

Mr. Andre Boysen: Just to clarify, on-device biometrics is a good idea. Trying to register my biometrics everywhere is a bad idea. That's the point I was trying to make.

Hon. Peter Kent: Toronto hospitals, the hospital networks, have been trying for more than a decade.... The Ontario government's been encouraging them to have an online exchange of medical information for all sorts of reasons—emergency room access and so forth.

Have either of your companies worked with the hospital networks, with doctors' offices to try to come up with a safe system?

Mr. Andre Boysen: Yes, we have a pilot going on with UHN right now. One of the challenges...and I've actually done a TEDx talk on health care and identity, because as a country, the biggest need for digital identity is in health care. We need to solve this problem because we can't continue to have health care consume the whole budget.

We are doing pilots now. One of the critical elements in getting this right in health care is that a "health care only" bespoke solution won't work, because most of the population uses the health care system very infrequently, which means they're going to forget the damn password; and then the balance of the population are very heavy users of the scheme and they're always in there in person anyway.

We need a mechanism to access services online that will work for everyday Canadians. We saw how successful the government service was for CRA. We think that model can be extended to other public and private sector services.

The Vice-Chair (Mr. Charlie Angus): This is the final round.

Mr. Saini is beginning.

Mr. Raj Saini: I have one quick question. If you can't completely answer today, could you give written answers? I would appreciate that.

We keep talking about Estonia, but I know there are other countries that have begun the process. If you could give us a list of those countries or the countries you would suggest we study, and maybe some relevant reading material, we could include that in our understanding.

Second of all, this is something that fascinates me because coming from the private sector and owning a pharmacy, my technology was always cutting edge. Whatever was the newest, I had to keep up with. Now, you will have a NEXUS point eventually going forward where the private sector is going to interact with the public sector in exchanging information.

How do we keep the technology relevant, because the private sector is always going to be ahead? The public sector comes behind. You might get the policy directive right, you might get the understanding right, you can solve the issues with privacy, but eventually technology is going to be the key because one will always be out of step with the other. If this is really going to work, how do we solve that problem?

Mr. Andre Boysen: I want to pick up on Matthew's earlier comment about how you've got to go slow and then go fast when you can.

When you compare the Internet and the payment card system, what's interesting is that the way we pay for stuff has barely changed at all in 70 years. It started with a paper card and then we went to a plastic card. Then we had two problems, transaction speed and fraud, so we moved to a mag stripe. Then the crooks figured out how to do the mag stripe, and so we moved to a chip card. Since we've gone to chip card, in-person fraud has gone to zero, but we have this online problem, so now we're putting it in the phone.

What's important is that the way users pay for stuff across the globe has barely changed at all in 70 years. On the Internet, it's changing every single week. Users can't keep up.

● (1640)

Mr. David de Burgh Graham: You were talking a moment ago about face identification for logging in.

If your biometrics are compromised, what can you do about it? An example of that is the famous hacking of Angela Merkel's fingerprints by somebody who had a photograph of her.

Mr. Ira Goldstein: I would refer back to my depository insurance comment to say that, if we're actually going to roll out biometric authentication for government services, there has to be that buffer zone where citizens believe that if there were some compromise, there's a way to fix it.

How do you get new biometrics? I don't have a good answer for that. Maybe Matt does.

Mr. Matthew Anthony: I will say that it's become increasingly difficult to fake a biometric, as the technology for sensors has improved. Therefore, as we move away from a thumbprint to a face print to—we're looking now at vein pattern recognition on some new phone systems.... We've had palm print technologies for a long time. It is always perhaps possible to spoof those. Any problem can be solved with enough money and technology. They can be spoofed, but they can't perhaps be overtaken, unless you don't register them yourself.

If you have your phone and don't ever register anything except a four-digit PIN and then somebody comes along and puts their thumbprint in, it's in there. That's on you, not them. The ability to actively impersonate somebody with a biometric, unless it hasn't been registered to you in the first place, is getting to the level of practical impossibility. Fifteen years ago, I could fake a fingerprint and replay it fairly easily. I can't do that anymore.

Mr. David de Burgh Graham: That's fair.

Ms. Rene McIver: It really is about the way it's inputted into the system, again. I worked on biometric standards for about 10 years actually and it was interesting. There was always discussion about the input into the system and taking a fingerprint and putting the fingerprint in. There was always a discussion about liveness detection, but really, your input system should have a means to identify whether or not it's a live biometric. Liveness is really about a biometric, so it is increasingly complex to figure out how to accurately get the information in that isn't spoofed. It's not just a static fingerprint.

You see it in some of the face recognition algorithms. The input is that there's actually a request for you to do different things, like smile, turn your head, look down or close your eyes. There are increasingly harder ways to actually get the input.

Mr. Matthew Anthony: To amplify that, I would just like to say that if the level of access that you need requires you to go to those lengths, I guarantee you there are easier ways to get your data.

Mr. David de Burgh Graham: Fair enough.

Mr. Andre Boysen: I don't want to take your time, but I just want to say that with biometrics, don't think of it with silver bullet thinking, believing that you're going to solve it with biometrics. Rather, it's about the use of biometrics with what you have and what you don't have.

The Vice-Chair (Mr. Charlie Angus): Thank you very much.

I have a deep feeling that my colleague Mr. Graham would like to filibuster if he could, because he's really got a lot to say. I would normally like to continue, but we do have an agreement on Thursdays that for people who are going to head out for flights, we end after this round.

I want to thank you very much. This has been a fascinating discussion with really excellent information. If you have things that you think we should be looking at, or if you're checking our testimony in that regard, certainly feel free to write our committee because we will be preparing a report.

Go ahead, Mr. Saini.

Mr. Raj Saini: Just to all four of you, I mentioned the one specific issue about the countries, but if there's any other information that any of you think we need, we'd be deeply grateful if you could pass it on in a submission to give us the opportunity to expand our own thinking on this topic.

Mr. Andre Boysen: We'll share some information for sure.

Thank you for having us.

The Vice-Chair (Mr. Charlie Angus): The meeting is adjourned.

Published under the authority of the Speaker of
the House of Commons

Also available on the House of Commons website at the
following address: http://www.ourcommons.ca

Publié en conformité de l'autorité
du Président de la Chambre des communes

Aussi disponible sur le site Web de la Chambre des communes
à l'adresse suivante : http://www.noscommunes.ca