HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 151 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Wednesday, February 27, 2019

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Wednesday, February 27, 2019

● (1550)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Ladies and gentlemen, I apologize for being late, but I was presenting the 31st and 32nd reports of the committee on estimates.

I also apologize to our witnesses for the change in location. There's apparently something going on today on the Hill, I'm told, and those who are not following that are watching CNN, so I expect we'll have a fairly private meeting.

Colleagues, I propose that we go past our usual stopping point. Our witnesses have come a long way in order to be able to give testimony. One witness was unable to attend, so we've merged the two hours....

Have we merged the two hours? I don't see the other witness here.

The Clerk of the Committee (Mr. Naaman Sugrue): We might just take them on—

The Chair: Okay, when they come along....

Again, we'll follow our structure, but we might be a little bit flexible in terms of how we present.

With that, I see that we have here Mr. O'Higgins and Michele Mosca from Quantam-Safe Canada, and Mr. Parsons from Citizen Lab. Welcome.

We'll start with 10-minute presentations from each group. Then we'll go to the usual question and answer period.

Quantam-Safe, you're up for 10 minutes, please.

Mr. Michele Mosca (Director, Quantum-Safe Canada): Thank you.

Good afternoon, Mr. Chair and members of the committee. I am Michele Mosca, a professor of mathematics and cryptography at the University of Waterloo in the Institute for Quantum Computing.

[*Translation*]

It's an honour to be speaking to you today.

[*English*]

When I started my research career at Waterloo and Oxford, I believed my fields would have important implications for the world and offer Canada great economic opportunities, though decades in the future. A quarter century later, it's showtime.

Of course, Canada should proactively seize the great opportunity for economic prosperity created by the decades of work and billions of dollars that we've invested in making Canada a world leader in quantum technologies. However, before we unleash all the wonderful powers of quantum technologies, we have the responsibility to first prepare ourselves to be safe in a world with these technologies. Right now, we are tremendously and dangerously vulnerable. I'll explain briefly what I mean.

First, our economy depends on digital technologies, and their security relies fundamentally on cryptography. Cryptography is perhaps best known for providing confidentiality, which is critical for financial transactions and protecting intellectual property. Cryptography is also what allows our devices to know whom to trust when we engage in transactions on the Internet. For example, you want to make sure you're downloading legitimate software updates and not malware. If you're transferring money to your bank, you want to know that's really your bank and not someone pretending to be your bank. Robust cryptography is absolutely necessary for the proper functioning of our digital economy, which now is pretty much synonymous with our economy.

I'll explain in a minute how quantum computing seriously threatens all of this, but first let me point out one of the biggest challenges. Because the threat may be 10 or more years in the future, there's a natural human tendency to simply ignore it for now. But procrastinating any further and managing this as a crisis will have devastating consequences for our safety and our economy.

First, it will take more than a decade to prepare our economy and our critical systems to be resilient to quantum attacks. This is a very fundamental retooling. We're not talking about patch management and bad passwords. There's no quick remediation and fix. We're talking about systemic collapse with, again, no remediation in place.

Second, a loss of confidence in our cyber-resilience and the economic impact of that may happen much sooner, even in the next two to five years, as key quantum computing milestones are achieved. The quantum threat itself is simple. We don't need Schrödinger's equation to understand it. A quantum computer is a powerful new type of computer that will be able to perform previously impossible calculations. However, it will also decimate today's cryptography, which of course must be dealt with in order for the advent of the quantum computer to be a positive milestone in Canadian history—not just in Canadian history, but in human history.

The impact on our financial industry and economy will include the following: first, a direct attack on the financial services sector—money stolen, legitimate activities impeded, loss of confidence in the Canadian financial sector; second, cyber-attacks on other sectors driving our economy, where much of our money is invested—most importantly, critical infrastructure such as government services, power and other utilities, transportation systems and smart cities; third, theft of strategic intellectual property that is protected by quantum-vulnerable cryptography; and fourth, disruption of Canadian jobs, today's and tomorrow's, that produce or rely on technologies that are not resilient to quantum attacks and don't have a plan to become quantum-safe.

These are four distinct and very serious risks to the financial services sector and our economy as a whole.

We know what the threat is, and we have a good idea of the tools we'll need and how to use them to protect against those four risks to our economy. But this is not an academic exercise. This is where our species does not always shine, because we have to work together across multiple departments and multiple sectors. None of us can do this on our own, and we have to work proactively to get the job done, starting as soon as possible.

It's very challenging, very hard, but the potential silver lining for Canadians at least is that Canada is actually a world leader in quantum science, in cryptography, in quantum-safe cryptography, by which I mean cryptography designed to be safe against quantum attacks in cybersecurity and in financial services. This is our opportunity to lose, basically.

Given our stature and resources, we should be able to move relatively quickly to deploy new quantum-safe tools and to develop the workforce needed to do the work.

● (1555)

If managed proactively, the quantum threat can be turned into great economic opportunities for Canada. We know how to make ourselves quantum-safe, and we can do that and then export our quantum-safe tools and know-how abroad.

On the other hand, if managed reactively, if we choose to do that —which is human nature—we'll be susceptible to quantum attacks. We'll also be susceptible to mundane attacks, the everyday attacks we see today that simply exploit the mistakes intrinsic in a rushed crisis response, and we'll be importing, potentially backdoor, the implementations of our own innovations. That's what will happen if we manage this reactively. Not responding proactively means that new opportunities that we've invested in over decades will be lost, and much of our existing economy will be at risk.

ln closing, our recommendations to the committee are as follows.

First, please urge the government to move quickly to put in place the elements needed for Canada to become quantum-safe from a technology and human resources perspective, in particular including support for targeted research into quantum-safe cryptography, the rollout of a Canadian quantum key distribution network—a Canadian invention, by the way—via satellite and fibre systems, and the creation of a robust pipeline of expertise in quantum-safe cybersecurity.

Second, please urge the government to use the policy levers at its disposal, including approval, planning, procurement and funding powers, to ensure that the new digitally enabled infrastructure is designed and built to be quantum-safe, and not waiting to be decimated as quantum computers become available. In other words, let's create a pull for the technology and workforce needed to make Canada and the world quantum-safe.

Third, to make all this work, given the broad multisectoral, proactive effort needed—again, no one entity can pull this off on its own—please urge the government to provide suitable funding to a not-for-profit entity such as ours, Quantum-Safe Canada, to help coordinate the multi-faceted work needed for Canada to implement a robust quantum-safe strategy.

[*Translation*]

Thank you for listening.

[*English*]

I'd like to give my colleague Brian O'Higgins the rest of the time to say a few words. He is the chair of Quantum-Safe Canada and a world-renowned cryptographer and security entrepreneur.

The Chair: You have about two and a half minutes.

Mr. Brian O'Higgins (Chair, Quantum-Safe Canada): Thank you.

I've been involved in cyber for probably over 30 years. It's always a war between the good guys and the bad guys. The bad guys seem to be winning. Now, one of the most important tools that the good guys have, encryption, is ready to be broken, with this quantum threat that's on the horizon.

This really is a big issue, and it's down to safety and security. We know that industry, when it's left alone with commercial and market forces, is not always the best at handling that.

A bit of a government push to encourage industry to behave in the right direction could go a long way. In this case, some of the solutions to these problems are Canadian worldwide strengths. Having something happen in Canada first will really give a good opportunity for a worldwide export market.

The Chair: Thank you very much. We appreciate that.

Mr. Parsons, you have seven minutes, please.

Mr. Christopher Parsons (Research Associate, Munk School of Global Affairs and Public Policy, University of Toronto, Citizen Lab): Good afternoon.

My name is Christopher Parsons. I am a Research Associate at the Citizen Lab, which is part of the Munk School of Global Affairs and Public Policy at the University of Toronto. I appear at this committee in a professional capacity that represents my views and those of the Citizen Lab.

My comments today focus on a range of securitization practices that, if adopted, would mitigate some of the contemporary risks that participants in the financial sector face.

Canadian government agencies, private businesses and financial institutions, as well as private individuals, rely on common computing infrastructures. We use the same iPhone and Android operating systems, the same customer service interfaces and e-commerce platforms, the same underlying code bases and largely identical third party cloud computing infrastructures.

The sharedness of these platforms means that efficiencies can be leveraged to improve productivity and efficiency, but these benefits are predicated on the overall security of these shared products. To be blunt, the state of computer insecurity is profound, and a large number of vulnerabilities in these shared products, writ large, threaten the financial sector to the detriment of Canada's national security interests.

In my remaining time, I want to point to four issues in particular that I believe need to be taken up to ensure that Canada's national interests are better secured in the future than they are today. These issues include the need for Canada to formally establish a responsible national encryption policy, update Canada's vulnerability equities programs, develop a vulnerability disclosure program framework and promote two-factor authentication.

I now turn to the issue of responsible encryption policies. Given the state of computer insecurity, it is imperative that the Government of Canada adopt and advocate for responsible encryption policies. Such policies entail commitments to preserving the rights of all groups in Canada to use computer software using strong encryption.

Strong encryption can be loosely defined as encryption algorithms for which no weaknesses or vulnerabilities are known or have been injected, as well as computer applications that do not deliberately contain weaknesses designed to undermine the effectiveness of the aforementioned algorithms.

The benefits of strong encryption cannot be overstated. In a technological environment marked by high financial stakes, deep interdependence and extraordinary complexity, ensuring digital security is of critical importance and extremely difficult. The cost of a security breach, theft or loss of customer data or corporate data can have devastating impacts for the private sector and individuals' interests. Any weakening of the very systems that protect against these threats would represent irresponsible policy-making. Access to strong encryption encourages customer confidence that the technology they use is safe.

It is important to recognize that there are risks in the availability of strong encryption. As an example, one of Canada's closest allies, Australia, has adopted irresponsible encryption policies, which may introduce systemic vulnerabilities into code used by the financial sector, as well as other sectors of the economy. Once introduced, such vulnerabilities may be exploited by actors holding adversarial interests toward Canada or Canadian interests. Threat activities might be carried out against the SWIFT network, as just one of many examples, should any element of that network rely on cryptographic products made vulnerable by Australian demands.

Furthermore, strong encryption prevents our closest allies from monitoring Canada's financial activities beyond the above-the-board processes associated with a program such as FINTRAC.

As an example, The Globe and Mail revealed that the United States' National Security Agency was monitoring the Royal Bank of Canada's virtual private network tunnels. The story suggested that NSA's activities could be a preliminary step in broader efforts to “to identify, study and, if deemed necessary, 'exploit' organizations' internal communication networks.”

In light of these kinds of threats, we would suggest that the Government of Canada adopt a responsible encryption policy. Such a policy would entail a firm and perhaps legislative commitment to require that all sectors of the economy have access to strong encryption products, and it would also stand in opposition to irresponsible encryption policies, such as those calling for back doors.

I now turn to the management of computer vulnerabilities of the Government of Canada itself. Vulnerabilities in computer code are acquired by Canada's Communications Security Establishment, or CSE. Thereafter, the CSE determines whether to retain or disclose the vulnerabilities. The CSE is motivated to retain vulnerabilities to obtain access to foreign systems as part of its signals intelligence mandate and also to disclose certain vulnerabilities to better secure government systems.

To date, the CSE has declined to make public the specific processes by which it weighs the equities in retaining or disclosing vulnerabilities. In contrast, the United States publishes how all federal government agencies evaluate whether to retain or disclose the existence of a vulnerability.

CSE's stockpiles of vulnerabilities could potentially be uncovered and used by adversaries, and this has happened to both the United States' National Security Agency and the Central Intelligence Agency. The effect can cost billions in direct economic damage.

● (1600)

The ongoing presence of these stockpiles and lack of clarity concerning what vulnerabilities are retained in the businesses and private individuals have reduced confidence in the reliability and security of products needed to enhance Canada's economic efficiency and productivity, and prospectively slowed Canadians' adoption of contemporary and next-generation software platforms and infrastructure.

To alleviate these concerns, we would suggest that the Canadian government publicize its existing vulnerabilities equities programs and hold consultations on their effectiveness in protecting the software and hardware that is used in the course of financial activities. Furthermore, the government could include the business community and civil society stakeholders in the existing, or reformed, vulnerabilities equities programs. Including these stakeholders would encourage heightened disclosures of vulnerabilities and thus improve the availability of well-written software and reduce threats faced by the financial sector.

Now, it is also important to recognize that security researchers routinely discover vulnerabilities in hardware and software that are used in all walks of life, including in the financial sector. Relatively few organizations, however, have explicit procedures that guide researchers in how to responsibly disclose vulnerabilities to the affected companies. Disclosing computer insecurities absent a vulnerability disclosure program can lead companies to inappropriately threaten litigation to white hat security researchers. Such potential reduces the willingness of researchers to disclose such vulnerabilities.

Beyond studying the laws around unauthorized access to computer code, I would recommend that this committee, and this government, create a draft policy for the financial sector companies to adopt. Such a disclosure policy should establish to whom vulnerabilities are reported, how reports are treated internally and how long it takes for the vulnerability to be remediated. It should also insulate security researchers from legal liability, so long as they do not publicly disclose the vulnerability ahead of the established delimited period of time. Moreover, the government should move to develop and adopt a similar disclosure program for its own departments so that the government can benefit from researchers reporting vulnerabilities in government systems.

Finally, I turn to the topic of two-factor authentication, or 2FA, which refers to an individual being in possession of at least two factors to obtain access to their accounts. The factors most typically used for authentication include something that you know, such as a PIN or a password; something that you have, such as a hardware token or a software token; or something that you are, such as a biometric like a fingerprint or an iris scan. These multiple factors mean that losing a log-in and password pair does not necessarily enable third parties to access a protected system or data store.

It is important for customer-facing systems to have strong 2FA to preclude unauthorized parties from obtaining access to personal financial accounts. Such access can lead to better understandings of whether persons can be targeted by foreign adversaries for espionage recruitment, cause personal financial chaos designed to distract a person while a separate cyber-activity is undertaken, or direct money to parties on terrorist or criminal watch lists.

Admittedly, some Canadian financial institutions do offer 2FA but often default to a weak mode of second-factor authentication that relies on SMS or text messages. This is problematic, because SMS is a weak communications medium and can easily be subverted by a variety of means. It is for this reason that entities such as the National Institute of Standards and Technology in the United States no longer recommend SMS as a two-factor authentication channel.

To improve the security of customer-facing accounts, I would recommend that financial institutions be required to offer 2FA to all clients, and that the 2FA utilize hardware and/or software tokens. Implementing this recommendation would reduce the likelihood that unauthorized parties can obtain access to accounts for the purposes of recruitment or disruption activities.

To conclude, Canadian businesses and private individuals rely on digital tools for all aspects of their lives, including activities that intersect the financial sector. To be clear, the proposals I have outlined will not solve all of the computer insecurity problems that threaten Canada's national security interests and the financial sector, but we believe these proposals do represent a good effort in resolving the most basic threats and would also serve to build trust in the security of our digital tools and the governance of security.

Thank you for your time. I look forward to your questions.

● (1605)

The Chair: Thank you, Mr. Parsons.

Ms. McCrimmon.

Mrs. Karen McCrimmon (Kanata—Carleton, Lib.): Thank you very much.

I'd like to begin by thanking you all for being here today. You've added quite a bit to our discussion.

I'll start with Professor Mosca and Mr. O'Higgins. I was really happy to hear you talk about the need for collaboration. Can you tell us a little bit about the relationships, the networks between academia, industry and government? Are they functioning? Are there weaknesses that we should be looking at improving?

Mr. Michele Mosca: Academia is a pretty close-knit community. We tend to know each other. In this specific sub-discipline, we were successful in getting buy-in. In addition to focusing on the cutting-edge world research we're each doing as individuals, everyone was keen to collaborate and work together and have it have a positive impact for Canada and the world.

There are a number of venues where two of the three meet. All three is pretty rare, though we do host a symposium twice a year with about 40 people who are thought leaders from the three sectors. It focuses on cybersecurity. Quantum is just one piece of that discussion. We discuss what it means for Canada to be a leader in cybersecurity, how we can get there and how we can work together. There have been a lot of positive interactions. It's still relatively small-scale and ad hoc. I think we would benefit from a more proactive pull for this kind of benevolent, mission-oriented activity.

Brian, did you want to add something?

● (1610)

Mr. Brian O'Higgins: I think you nailed it there. Collaboration among all three entities—government, industry and academic—is almost unheard of. The cyber symposium that Michele hosts is about the only example I know. It has a very small government participation, but it is a start. Putting a bit more focus on and encouraging these types of symposia is only going to help.

Mrs. Karen McCrimmon: Following on that, what do we need to do to incentivize this, or are we the ones who are missing at the table? How do we encourage others to participate in these forums?

Mr. Michele Mosca: I should also mention our colleagues at SERENE-RISC. Their driving force, the head of SERENE-RISC, is on our governing board as well. That's another venue with a number of workshops that try to bring together these various stakeholders.

Organizations like SERENE-RISC and ours are the few that actually step up to do more than just focus on.... The thing with cybersecurity is that we're all over-employed. We're super busy. For everything we choose to do, there's something else that's really important we're choosing not to do. We're not bored. It's not that we don't have anything to do and so we think maybe we can address this quantum threat. We're way too busy with too many things. There needs to be some encouragement. The thankless work that Benoit and the SERENE-RISC network do, for example.... They hardly get any money and they still do amazing work. I think these people need to be encouraged, thanked and supported.

Part of it is funding. We say “funding”, but when you're a professor and you ask for funding, people assume you want more undirected research money. Canada's already great at that. I'm talking about very focused, mission-oriented support to achieve these very important objectives for Canada, and working backwards from there.

There is a small, committed group of people across Canada who would help with that. They need to be proactively encouraged to do this. Right now, what they're told is that they have to keep advocating, but they don't have time and resources to do this. We, as a country, need to recognize the value they bring to us, the citizens, and tell them to keep up the great work and help them do more.

I also think there are not enough of us. Another thing we need, as part of developing the brain trust, is the intellectual capital and the workforce needed for Canada to even survive in the cyber world a decade from now. We're way behind. Two to five years ago, looking ahead a decade, I said that there's no way we're going to have a fighting chance if we don't have 20 new positions targeted in cybersecurity, with at least five of those in the social and human sciences, because that's a really important part of this equation.

Of course, now the number I see is 50. Our friends in Germany were talking about 50 faculty positions in applied cybersecurity at Saarbrücken, and I don't know how many more at the new Max Planck Institute. We're talking about over 200 serious faculty positions in this targeted area, because it's really important to their economy and security. In Canada, there are zero—not even a CERC, or a Canada 150, nothing. I think there's a huge catch-up there to build up our brain trust in these targeted areas.

Mrs. Karen McCrimmon: Okay.

The Chair: You have one minute.

Mrs. Karen McCrimmon: I'll ask my last question, and later on I hope we have a chance to talk.

Mr. Parsons, you talked about responsible encryption policies. Does anybody do these right? Does any country have the policies right? You can talk about that and the vulnerability programs as well.

Mr. Christopher Parsons: I think that, currently, there are challenges within the Five Eyes countries: Canada, the U.S., New Zealand, Australia and the U.K.

The United States, outside of its law enforcement discussions, has showcased a strong desire to support strong encryption. The National Security Agency, the Central Intelligence Agency and all parties outside of the FBI, actually, are strong advocates for unvarnished, strong encryption for intelligence purposes, because they need it themselves in order to efficiently conduct their business. So I think we can turn to our ally to the south to actually derive some inspiration from their intelligence services.

With regard to vulnerability disclosure programs, there are certain companies that have good models for this. The United States' HackerOne has worked with the Department of Defense, and recently legislation has been discussed, if not quite passed, that would also authorize vulnerability disclosure programs to affect the state department.

I think that's how it works on the government side. I think it's a good, strong initiative, and it's leading to substantive patches of major vulnerabilities. You're also seeing, through HackerOne, a large volume of private companies slowly move towards more holistic disclosure programs. In both cases, it means that the infrastructure of government and of private business is secured, and it's often done at a low cost.

● (1615)

The Chair: Thank you, Mrs. McCrimmon.

Mr. Motz, you have seven minutes, please.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you, Mr. Chair.

Thank you, gentlemen, for being here.

My first couple of questions will be for Mr. Mosca and Mr. O'Higgins.

One witness who previously appeared before the committee noted that he had zero confidence in our readiness to deal with cybersecurity as a country. How much work remains for our government systems to be ready to protect against such an attack?

Mr. Michele Mosca: Do you want to start?

Mr. Brian O'Higgins: Actually, I wouldn't be so harsh as to say zero readiness. Canada is actually quite well regarded. The Canadian federal government is a smaller entity, compared to that of the U.S., for example. It's about one-tenth the size, so it's almost like one U.S. department. If there's a focused effort to pay attention to cyber, the cyber stance will improve, and that's all good.

In our financial sector, we have a few large banks. They're generally very well regarded and are good international models. They could do a lot more, absolutely, but our starting position is not too bad. We're quite.... I've been involved in cyber in probably 50 countries, as a Canadian speaking about technology, what our government is doing and what our companies are doing. We are always very welcome and listened to quite a lot.

Mr. Michele Mosca: I think we have all the building blocks to win this game, but we don't have the plan of how to put these blocks together and really take advantage of them.

Mr. Glen Motz: It's the lack of confidence that this witness had in putting that together.

Mr. Michele Mosca: I think that we don't see the plan. The new cybersecurity centre is a wonderful first step, but there's just.... The puck was in the back of our net. We crossed the goal line, and we're halfway to our own blue line. We're not even close enough to the net to actually win this game, and I haven't seen a game plan designed and implemented to get us there. What we've been doing.... Again, we have great, world-class building blocks, but we're not in Kansas anymore. This is a potential threat.

Mr. Glen Motz: I have a quick question before I move on to Mr. Parsons.

Would we ever know when a quantum computer starts launching an attack? Could these activities go unnoticed today for significant periods of time? Do we currently have the systems to even detect them?

Mr. Michele Mosca: That's a great question.

It's hard to predict how threat actors will exploit it. It's a scary game that we can play with each other. If you had a quantum computer, what would you do with it? What's your objective? Do you want to destroy the planet? Do you want to be rich? Do you want to do this or that? Then you would have a different strategy, different tactics, depending on what your strategic outcomes are. It is certainly....

It's like the movie *The Imitation Game*, about World War II. When the Allies broke Enigma, they were very tactical in terms of how they responded. They didn't want it to be known that they had an Enigma machine.

You might not notice, but there are some indicators. When you start seeing stuff that looks like it came from Microsoft or whatever—it has their official signature, but it never came from them—those are some red flags. That's a big part of the problem. Breaking cryptography is like giving somebody the digital key to the front door. It's a lot easier to go undetected, I would say.

I don't know if Brian wants to add to that.

Mr. Glen Motz: Thank you very much.

Mr. Parsons, I believe you were in Washington D.C. when my colleague PPH, Pierre Paul-Hus—

Voices: Oh, oh!

Mr. Glen Motz: Sorry.

You met with intelligence officers there. Around the same time that was going on, our head of the Canadian Centre for Cyber Security, Mr. Jones, made comments to this committee, alluding to the superiority of our testing facilities compared to those of our allies. He explained that this would set us apart in our ability to do business with companies—maybe from hostile states, such as possibly Huawei.

Could you explain to this committee what our American counterparts had to say about Canada's security capabilities?

● (1620)

Mr. Christopher Parsons: This came up extensively in our discussions in Washington and throughout the United States. The U.S. officials were very circumspect and did not state explicitly that Canada had the right or wrong policy. Rather, they indicated that should we adopt an approach that parallels that of the United Kingdom—one where we would inspect foreign equipment, then evaluate it, then release it into the corporate sector should we desire—then we should look to what has happened in the U.K. They pointed to the fact that last year the U.K. recognized that there were serious supply management problems. Their ability to ensure the safety of Huawei equipment could not be guaranteed as of last year.

Mr. Glen Motz: In my last minute and a half, Mr. Parsons, can you describe, from your research and in your opinion, what dangers Canada may be facing if we allow a company like Huawei to become part of our 5G network?

Mr. Christopher Parsons: There's a series of different problems. One of them pertains to the potential for equipment to be updated in ways that are detrimental to Canada's national security interests. This could involve a firmware update that modifies the way the most basic elements of the boards operate. It could also involve modifications to the software systems that are one layer up on the routing equipment.

Associated with that, there's the possibility that if there are vulnerabilities that are accidentally inserted—code has bugs all the time—the Chinese government could issue an order telling Huawei not to patch it. That may be the most significant type of vulnerability, because it would not be one that was deliberately inserted. Indeed, these types of vulnerabilities have been exploited by the members of the Five Eyes alliance as well, minus any sort of legislative requirement, as far as we know.

Those would be the primary issues. That kind of back door could then be used to modify data, which is probably as dangerous as, or even more dangerous than exfiltrating it. All of a sudden, you would be unable to determine whether the data you were receiving that was being processed through the network was accurate, inaccurate or something else.

Mr. Glen Motz: You'd never know whether that was done. In the first instance, it was a malicious code or some bug that wasn't fixed, but if they were purposely adjusting their equipment and putting in monitoring software and hardware, as a country, our networks would never be able to recognize that.

Mr. Christopher Parsons: It would be incredibly challenging to ascertain it. By the nature of updates, you might be safe at one point and unsafe at another point in the future.

The Chair: Thank you.

Mr. Dubé is next, for seven minutes, please.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Chair.

Thank you all for being here.

I want to continue on the discussion between Dr. Parsons and my colleague Mr. Motz.

Even if the network is secure.... I'm particularly looking at the Pegasus iPhone hack, which your organization has worked on—or even was a victim of, if I'm not mistaken. Even if the network is completely secure—a metaphor was given to us of an armoured vehicle between two cardboard boxes—I'm wondering, in the era of the Internet of things, whether there's concern about still being able to remotely access devices. Firmware updates might not be provided to devices, so you might have the data transiting—and I'll say this in layperson's terms—between devices on a very secure network, but once they land on a device that is cheap, so to speak, out of date and whatnot, is that a problem?

I'll hear from you, and if our other witnesses want to jump in as well, I'd love to hear them.

Mr. Christopher Parsons: From the perspective of the Citizen Lab, and more broadly the computer security community, security is an ongoing state. Security imposes friction and decreases the likelihood of an opportune activity taking place, but there's no such thing as perfect security.

You point to activities by Pegasus, which was developed by NSO Group, an Israeli group that produces cyber weapons for a variety of organizations and countries. They're exploiting vulnerabilities for which there are no known patches. The vulnerabilities themselves are unknown to the manufacturers. There is the concern that a group like NSO or something like it could target Huawei equipment on the basis that it has a vulnerability that no one is aware of, and that is a very real concern.

Associated with that is having data transiting across these insecure devices, which also opens the possibility that data transmitted from the Internet of things could be modified. One example I like to give is that you might see on your thermostat that it's a balmy 25°C inside and you're enjoying a nice warm Ottawa winter, and it's actually -30° C outside but the thermometer is not sending messages to your furnace to come on.

That would be an example of your Internet of things communicating back and forth and being modified by an insecure middle point.

● (1625)

Mr. Brian O'Higgins: In the Huawei example, it's very important to trust our network because everyone is using that. We could never control the individual devices that people use, and when there's a specially targeted attack, one individual here and there will always be compromised, but it's very important to pay attention to the network that the world, the whole population, uses.

Mr. Matthew Dubé: It's interesting, because a point was just made that some of the flaws in devices may not be known to the manufacturers, and obviously not to the public in that case.

When HackerOne was here, there was a bit of discussion about the bug bounties, discovering the bugs and reporting them, but then there are also the concerns about whom they're being reported to, the “highest bidder” phenomenon.

I wonder what all of you have as a perspective on how that should be approached and whether we need more explicit rules about how these vulnerabilities are disclosed, particularly when they're discovered by government organizations—for example, if CSE was aware of serious flaws on devices that we all as Canadians use.

Mr. Christopher Parsons: In the case of CSE, it does possess what's called a vulnerabilities equities program. This is a way by which CSE determines whether it will disclose or retain vulnerabilities that it identifies. It's not public. It's not clear how effective it is, and it's not clear what data is or is not presented to manufacturers, so I think it's important to work through that and present it.

Bug bounties are prospectively very helpful. Quite often, people who are doing security research aren't necessarily actually motivated by the money out of it; it's the prestige, and those are effective processes. They're often the later stage of a vulnerabilities disclosure program that's developed.

I would note that one of the concerns pertaining to the Australian legislation is that, reading through it, there's the prospect that the Australian government may be able to go to companies and say, “We want to know all the bugs that you know exist in your software but have not yet been patched”, in order to run policing or national security investigations. That's a serious concern, because if that is the way the government chooses to read its legislation—and it is suggested that it is how they will do it—it means that bug bounties and vulnerability disclosure programs can actually be used to channel data that is then used by other states, with the risk being that those vulnerabilities might not always be used to the benefit of Canada's interests.

Mr. Brian O'Higgins: Vulnerabilities, of course, are very valuable, especially to people who want to cause a lot of damage. The NSA had its secret stockpile of vulnerabilities. That got out somehow, and a series of the most damaging viruses and malware in recent memory were born from that set of vulnerabilities, so it's a problem all around.

Mr. Michele Mosca: For context, to compare and contrast with the quantum threat—because there are so many ways we can get hacked and it can get really confusing—breaking cryptography fundamentally would be like the mother of all vulnerabilities, because you can't just fix the code. There's no algorithm to fix. A good implementation of a bad algorithm is still vulnerable.

Second, if we deal with this as a crisis, there are going to be many more vulnerabilities for hackers to exploit without a quantum computer.

Mr. Matthew Dubé: The last question I have is about third party apps, in regard to banking in particular. Given that there's a lot of sensitive information, should there be more regulation, once you're getting outside of...your bank's app on your phone, which you have with RBC, let's say, and then the type of information that's being shared?

What can we do about that as well? That's a concern that we've seen raised.

Mr. Christopher Parsons: There's definitely a concern associated with third party applications gaining access to information and using it in ways that individuals aren't aware of. We see that throughout the app ecosystem.

A variety of things could be done. I would identify one of the lower-stake things, which is to ensure that when legitimate, white hat security researchers—groups such as us at the Citizen Lab—look at these sorts of applications, we aren't put in legal liability or jeopardy by looking at them. We have been in the situation previously where we faced litigious organizations on the basis of our security work. We are not trying to break things in order to ruin the Internet; we're trying to do it to keep everyone safe. We're a comparatively well-funded, well-situated organization.

When individuals who engage in this research, and I speak from personal experience, get sued or threatened to be sued once, it's not that security researchers stop doing the work. They keep doing it, but they don't report it. They're not doing it because they want to hack; they do it because that's what gets them going. This is their intellectual curiosity. We need to find a way of helping those people help us, as opposed to making them hide in the shadows for fear of legal liability.

● (1630)

The Chair: Thank you, Mr. Dubé.

Mr. Spengemann, you have seven minutes, please.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Mr. Chair, thank you.

Gentlemen, thank you for being with us. I want to sum up the conversation so far by putting it back through the lens of the structural challenges and opportunities that we're facing here, perhaps even looking at it as an infrastructure investment lens. We've heard the whole gamut of concerns. Dr. Parsons, I think you've described Canada as having a profound state of cyber insecurity. Mr. Mosca, you said there's an economic opportunity at the other end of that spectrum; if we get it right, we can actually achieve positive economic gains.

If we take an investment lens, I wonder if you could start us out by differentiating between the quantum and the non-quantum portion of the problem. How much do we need to be concerned about quantum computing at this point? How much of a future threat is it? In the current constellation of conventional cybersecurity problems versus quantum, how do things line up there? Where's the crux of the challenge?

Mr. Michele Mosca: Maybe I can take a quick stab at it. Unfortunately, you have to deal with all of the above. Obviously, human nature is to dodge the bullet that's about to hit you now, and the bigger catastrophe that might hit you in 10 years you can always put off without any immediate consequence. We need the discipline to do both at the same time, which is hard.

In the day-to-day stuff, there's a quick turnover in terms of threats changing. As we figure out how to solve one problem, people take advantage of a new one. What was previously not the most economical way to hack you might now be the most economical way to hack you. We have to do the tactics and the strategy at the same time.

Quantum offers us two things. One is a way to leapfrog. Perfect security is not possible, but you want to do the best you can. If we do this as part of life-cycle management, if we proactively transition the foundations of our cybersecurity to fight against future threats, it's a chance to.... It's like when you have to fix your basement. While we're at it, let's redo the plumbing and the wiring. We can retool the foundations of our cyber infrastructure. It won't be perfect, but it will be a heck of a lot better than the band-aid on top of band-aid on top of band-aid that we have now.

It's a great opportunity to retool, to do things right. It won't be perfect, but it will be much better than it is today.

Mr. Sven Spengemann: That's very helpful.

Dr. Parsons, how much of the gap would we close simply through developing a cogent national policy framework?

Mr. Christopher Parsons: I believe it would begin to go a long way. Ideally, any strategy that is laid out should be clear and direct. I think this is an area where you can look to the United States—where it's taken about 10 years, but most of the agencies have started to come together, the intelligence community—to say, here is the way we approach national security. We can agree or disagree on the actual policy framework they are laying out, but it's coherent across branches. That means that all pieces are working toward roughly the same ends. That means that it's productive—for people within government, to see where they have to go; for those external to government, to see what services are needed; and for academics and other parties, to see what technologies or what goalposts we need to move toward as a country.

Mr. Sven Spengemann: Do any of you have data, or would you be able to speculate on an informed basis about whether Canadian private sector companies are spending, as a percentage of operating expenses, more or less than companies in other jurisdictions, with respect to Five Eyes at the moment? What should they be spending in the future to do things right, if there is a gold standard in terms of jurisdictions that have gotten this right?

Mr. Brian O'Higgins: The response to cyber is typically led by government and finance sectors, and that's universal around the world. Canada is not bad in both of those, in particular because we have only five or six banks, and not 30,000 banks, compared to the U.S. Our banks tend to be big and do a fairly good job. The rest of the industry is woefully behind, and there are sectors that are really pathetic. I get more and more concerned, especially when I look at the critical infrastructure, power generation and so on, and I see they have a lot of embedded equipment with vulnerabilities. It's very hard to update them. Now hackers are getting smarter and more motivated under nation-states, and the risk is becoming greater all the time.

● (1635)

Mr. Sven Spengemann: To what extent do you think that's a factor of Canada's domestic economy size, its market size, its status as a mid-tier nation? One of you mentioned Germany and said there are 50 people in this field, and we have zero. I'm reading in your written testimony that China is investing billions of dollars in quantum research. Is our economy size a factor in this, our economic structure, in terms of limitations we're under in the sense of how much we can or should invest?

Mr. Christopher Parsons: I would just say that this is an area where government can be very effective. If you look at the investments by the Canadian government compared to those of our closer allies, obviously the U.S. is the juggernaut to the south. You can also look at the U.K. and other countries. You can go to European countries. They're investing magnitudes more money into figuring out how to do cybersecurity more effectively.

The other component, just to recognize what my colleague said, is that large banks are comparatively well secured, but the majority of Canadian businesses are small and medium-sized enterprises, and frankly you're just not going to be in a situation where an enterprise of three to 30 people has a security expert on staff. It's essential in that sense, from a structural perspective, for either government or some other group or organization to find a way of facilitating security in those organizations. That's where many Canadians are employed. That's where our economic growth is often derived from, and that's where I think the most important targets are at this point.

Mr. Sven Spengemann: I have a minute left. To follow up on that question, to what extent are any governments or private sector economies able to stay on the frontier, on the cutting edge of the pace of change, for any sustained period of time? In other words, is everybody always playing catch-up and are we just trying to be the best at playing catch-up? Or is there actually a way to get out front and be proactive and positive?

Mr. Brian O'Higgins: Yes, it's been mentioned several times. Being perfectly secure is rather impossible, but for all intents and purposes you can be secure, because the definition of security is that you have to be just an inch better than the effort any hacker is going to be willing to spend against you. If there is a level of security in the industry and you're just a tall poppy and a little bit better than that, you're safe, because the attacks go somewhere else.

Mr. Sven Spengemann: Also, that's measurable.

Mr. Brian O'Higgins: It's about paying attention to it, always following best practices and budgeting appropriately, with any of the incentives to get you to pay attention. There will be legislation around liability and all kinds of things as people wake up to a cyber-threat. It's starting to happen slowly, but we need more incentives.

The Chair: Thank you, Mr. Spengemann.

Mr. Eglinski, please, you have five minutes.

Mr. Jim Eglinski (Yellowhead, CPC): Thank you, Mr. Chair.

I'd like to thank the three witnesses who are here today.

I've always been pretty secure in life, until we started this study here and I started hearing from guys like you out there. It's like, “Oh, now I'm not so secure.” I'm coming out of this meeting with a feeling of insecurity, but anyway....

Mr. Mosca, you mentioned a very interesting thing. You talked about the football field and who builds that plan. We don't quite get to the blue line.

Who does build the plan? What is your recommendation for us in building that plan? We're here to listen to you about cybersecurity, but we need to know what we need to do. Do we need to work with universities? Do we need to work with industry, with government, etc.? I wonder if you could comment on that, please.

Mr. Michele Mosca: I think we need to convene a handful of thought leaders from each of these sectors to figure out the plan. As I said, anyone on their own doesn't have the know-how or the ability to implement the plan, or to even understand what the total plan should be. Together, we can figure it out, but you have to actually do it. It's not a theoretical thing. We have to convene this group of thought leaders with this mission to make us as cyber-safe as we can be, including Quantum-Safe. Let's be economic leaders in this space.

I'm talking about top levels of government. This has to be a top-level mandate. This needs to be implicit in all the relevant mandate letters of the ministers. Industry will show up. In academia, we're here to help. We do need to bolster our ranks, but those of us who are here are here to help, if we're actually summoned with that mandate. We know that it's not academia's job to protect citizens from deadly cyber-attacks or to oversee the economic development strategy of Canada, but we definitely want to help. We'll serve at that table, but we should be pulled into that table very proactively.

● (1640)

Mr. Jim Eglinski: Just following through on that, then, I think a way to see what you're saying is that we need a quarterback to lead us off. Who do you think that should be?

Mr. Michele Mosca: Well, we need a coach and a quarterback, yes.

Mr. Jim Eglinski: A coach and a quarterback.... Do you think that should be the federal government?

Mr. Michele Mosca: I think the federal government has the strongest moral authority to do that, alongside industry leaders and research thought leaders.

Mr. Jim Eglinski: Earlier, my colleague asked you about how long it would take us to notice if someone were to launch an attack. Do we have anybody watching right now in Canada, any agency that is watching what you spoke about, or is it just in limbo-land and hopefully we might catch it?

Mr. Michele Mosca: Well, I don't know what's happening in the classified space. I would anticipate that there is some activity there. In academia, we're watching and very openly explaining what we know.

One important thing I didn't emphasize is that at some point we're not going to know, and we just need to take that threat off the table. Why are we playing this crystal ball game when we know how to just take that threat off the table? What I was saying earlier is that it's really in the threat actors' hands whether they want to just bleed us slowly or completely decimate us. It's their choice. We hope that it's not in their business interests to completely destroy us, but they can if they want to, so why would we even want to go there? Let's just take that threat off the table.

Mr. Jim Eglinski: At one point Canada was a leader in quantum computing, I remember, at the University of Waterloo and at a couple of B.C.-based companies. Where do you think we stand today compared to the rest of the world? Are we getting interest from our youth through academia? Are we getting people interested in moving into that field, or are you having a hard time recruiting?

Mr. Michele Mosca: I think we're still second to none in fundamental science and technology development and so on. We wrote the business plan for owning the quantum world, and we raced ahead in implementing it, and we still have absolutely world-class assets, very much to be proud of, all across the country—in Quebec, Ontario, the west, and the Maritimes. We have a lot going for us on the fundamental science in tech, and we're sort of inching forward toward more applied stuff.

This is sort of separate from the cybersecurity thing. Quantum-Safe Canada can be one pillar of a broader quantum strategy to really own the podium in terms of benefiting economically from these decades of investments, but that coordination isn't happening yet. It is urgently needed, because we're talking about tens of billions of dollars being invested around the world in sort of eating that lunch that we've been preparing for however many decades.

We need to do that very quickly if we're serious about this. We don't want this to be the quantum Avro Arrow, so there's a great urgency to coordinate these wonderful assets we have in quantum. Again, Quantum-Safe Canada could be the leading piece of that, and as these other pieces keep maturing, we can also own the podium economically in quantum tech—not just tech, but the applications, the software and so on, the uses of quantum computing and quantum technology.

The Chair: Thank you, Mr. Eglinski.

Mr. Picard.

[*Translation*]

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

I share your enthusiasm for identifying challenges in a sector that is so unknown to us. This is Quantum-Safe Canada's area of expertise, so I'm going to tell you what I think, and you can correct me if I'm wrong.

You consider the threat to be very serious, and it is clear that Canada is at the back of#s the pack as far as its ability to defend against outside threats is concerned. The threat is not exaggerated per se, but is certainly more serious than people in general realize.

The solutions you are proposing focus on mechanics, techniques and technology. Given your extensive expertise, we can assume those solutions address the problem that lies before us. I don't necessarily think the threat has been exaggerated, but I do think the level of confidence in the proposed solutions is very high. The more, however, we talk about the technical dimension, the less we consider one specific element. I'm talking about the only risk you have no control over: the human element. No one has been able to come up with a satisfactory solution to that problem thus far.

Even if you have the best, most ironclad system in the world, the unpredictability of the human element makes it impossible to control the situation. The system can fall apart like a house of cards, because of the psychological element, or social engineering. I don't think, though, that AI is the way to manage the human risk. I'd like to hear your thoughts on that.

● (1645)

Mr. Michele Mosca: Thank you for the question.

[*English*]

You're absolutely correct. The human factor is one of the greatest, if not the greatest, vulnerabilities, and that's not going to fundamentally change. New mathematics, quantum entanglement, is not going to change our fallibility as humans and our corruptibility as humans, but good cryptography does reduce our dependence on trustworthy individuals. We still need some, but it reduces our dependence, which is a really important thing.

Second, the vulnerabilities intrinsic in human mistakes and human compromise tend to be more ephemeral and fixable. If there is a corrupt individual, if somebody uses a bad password or clicks on something they shouldn't click, you detect and you remediate. That's sort of at the top of the stack in terms of stuff that's hurting.... It's very common. It's not going away, but we have a fighting chance if we adopt better discipline and better detection mechanisms and, again, reduce our dependence on smart—not smart; we're all smart—but on people who are not making mistakes, because of course we're going to make mistakes. We can reduce that vulnerability, but not to zero.

Further down the stack, for broken crypto, there is no quick remediation there.

You're absolutely right—you can't just deal with one solution in isolation, because it's the whole ecosystem that works together. Definitely that's why I wanted to advocate for these 20 senior research chairs for Canada. Now it's 50, because we have to catch up. About a quarter of those need to be in the social and human sciences to help us get around the best way to handle all those aspects.

Mr. Michel Picard: Mr. Parsons, any word?

Mr. Christopher Parsons: I think there's a fundamental challenge in building out secure infrastructure and secure systems. It is very hard. To give you an example, it has taken probably the better part of 10 or 15 years to simply ensure that when you update your web browser or your operating system, it works, and we can guarantee that it works.

I say this because encryption is complicated, and any effort to undermine the few systems that are working would have devastating consequences. Unfortunately, we are seeing that this has happened in certain jurisdictions, Australia being one...and calls in other domains to do it, such as the United States for law enforcement purposes, and to a lesser extent in Canada, also for law enforcement purposes.

I think we're in a situation where it isn't just about evaluating how we can be secure. It's also about how to evaluate what we need to do. My argument, and certainly the argument of Citizen Lab, is that we need to preserve the few functional tools we have now to facilitate secure systems, rather than risk them in the pursuit of short-term law enforcement investigative pursuits.

Mr. Michel Picard: Thank you.

The Chair: With that, before we bring this to a close, the chair has a question. I want to direct it to Mr. Mosca.

The history of Canada, in terms of being on the edge of leading technology, is to never miss an opportunity to miss an opportunity. You used the example of Avro. You described a critical situation where, if we don't get this right, we'll just fall off the cyber map, shall we say.

Mr. Parsons put forward a series of suggestions as to the steps we should take as an organizing entity. Like you, possibly, I have a little skepticism about the government being able to do that. What do you think about his series of suggestions on how we should approach our cyber vulnerabilities?

● (1650)

Mr. Michele Mosca: From my perspective, they seemed like sound approaches to dealing with the issues in the short and medium term, which we absolutely must do. I see this as part of a broader cyber program for Canada. We have to simultaneously figure out that this is where we want to be in 10 years and that these are all the important disciplines and practices we should at the very least consider, or adopt in some form, to solve the issues he's saying we need to solve. The endgame, however, should also include resilience to future attacks.

Ultimately, we want to build a stronger cyber immune system. It's not about solving the latest...or just defending with one defence after another, like plugging holes in a dam. If you're thinking 10 years in the future, it's not that far. We just need to find a way to have a better cyber immune system where we're better able to detect new and emerging threats and adapt quickly to deal with them, instead of just drinking water from the firehose all the time.

Part of that does require a greater coordinated effort in Canada. I think Brian O'Higgins has advocated for a RAND-type organization where the cybersecurity research has to be funded by the government. You want trustworthy, objective, knowledgeable advice to the government so that we can react quickly to new and emerging threats. I think that's a fundamental part of a national cyber immune system. It's not the only part, but that's one of the next pieces I would strongly advocate for, in addition to the current cybersecurity centre and all the great things we do have going for us.

The Chair: Thank you.

Go ahead, Mr. O'Higgins.

Mr. Brian O'Higgins: I'll give you another example of a model that I quite liked. Back in my history as a founder of Entrust, a world-leading provider of encryption technology, the Canadian federal government was our very first customer. In fact, that got the company going. It led to an export market, and before we knew it, we were in 50 national governments. That was a big win.

We're still riding off that kind of aura that Canadians are good in encryption technology. There's an opportunity now with quantum resistance. Encryption has to change wholesale around the world. It has to be resistant to a quantum attack. Guess what? Canadian quantum technology from the University of Waterloo and other places is world-leading. There's a good opportunity to repeat that kind of effect.

The Chair: Let's hope it's not our opportunity to lose.

Mr. Brian O'Higgins: I felt your comment.

Voices: Oh, oh!

The Chair: With that, we'll suspend and re-empanel.

● (1650)

(Pause)

● (1655)

The Chair: Ladies and gentlemen, we're back on.

We have as our second panellists Mr. Masnyk from SkyBridge Strategies and Normand Lafrenière from the Canadian Association of Mutual Insurance Companies.

Have you two flipped a coin as to who is going first?

Mr. Lafrenière, we look forward to what you have to say for the next 10 minutes.

Thank you.

[*Translation*]

Mr. Normand Lafrenière (President, Canadian Association of Mutual Insurance Companies): Thank you, Mr. Chair.

I'm going to be sharing my time with my colleague Steve Masnyk from SkyBridge Strategies.

My name is Normand Lafrenière, and I am the President of the Canadian Association of Mutual Insurance Companies, or CAMIC for short.

CAMIC represents 79 mutual insurance companies across Canada that ensure people's cars, homes, farms and businesses.

Mutual insurers were formed over a period of 100 years, beginning in 1836. They were formed because farmers could not find farm insurance or find it at a fair price.

Mutual insurers are owned by their policyholders. There are no stockholders or share capital, and they aren't on the stock market. Policyholders elect their company's board of directors and vote on the major orientations taken by their company.

The premiums of the many serve to pay the losses of the few. When a profit is generated, that profit is transferred to the surplus of the company to be better able to pay future claims, is refunded to the members or is used for the betterment of the community.

Canadian mutual insurers have formed two mutual reinsurance companies—their own reinsurers—to share risks amongst mutual insurers and access reinsurance in the international market.

They have also created guarantee funds to fully compensate policyholders should an insolvency occur. In passing, I would like to mention that, over the past 60 years—ever since guarantee funds have been in place—no mutual insurance company has gone under.

Today, CAMIC member companies have a 15% market share of the non-governmental Canadian property and casualty insurance market. Being especially present in rural Canada, mutual insurers insure 75% of Canadian farms.

We are here today to address the issues of cyber-risks and threats to the financial system in Canada and, in particular, how open banking could possibly increase the risk of cyber-attacks.

Generally speaking, the insurance sector is not a likely target of cyber-hacking. Apart from insured's credit card and debit card numbers, mutual insurers generally keep very little information of interest to cyber-hackers.

We do, however, have serious concern about the discussion at hand today, especially as it pertains to open banking. This is a concept that began in Europe, the U.K., Austria and Japan. The concept was put in place only recently in those jurisdictions, so there is very little anecdotal evidence on how well or not well it is working.

We can, however, offer thoughts about the discussion points raised by the government when it began its recent open banking consultation.

● (1700)

[*English*]

CAMIC is particularly concerned that the open banking concept will undermine the long-standing prohibition barring banks from engaging in the insurance sector. This long-standing prohibition, supported by governments of all stripes, is in place to protect consumers of insurance from credit-granting institutions coercing them into buying an insurance product that is not appropriate for them. We hope that any open banking framework would not undermine this legislative prohibition.

I would now like to ask my colleague, Steve Masnyk, to touch on other concerns related to open banking and the cyber risks.

Mr. Steve Masnyk (Principal, SkyBridge Strategies): Thank you, Mr. Lafrenière.

Thank you, Mr. Chair. Good afternoon, committee members.

I'm not sure if this little diagram has been distributed to everybody. You may have it in front of you. I hope it will be able to guide the discussion, because with me talking in the abstract, it is a bit easier to understand the concept once you have the diagram in front of you.

I'd like to explain the concept of open banking and the cyber risks it poses to the Canadian financial services sector. I'm sure that many members are not aware of what open banking is all about.

It's a concept where a consumer can request that all their data held by their bank—their chequing account, credit card transactions, debit card transactions, investments, RRSPs, mortgage, insurance or any other loan—be transferred to third parties who are in financial services. By third parties, we mean financial technology firms, also known as fintechs.

These fintechs will then be able to underwrite you a financial service product that you may or may not already have, based on the banking data your bank has about you. This transfer would happen via a middleman called an API, which stands for application program interface.

APIs are pretty much platforms or apps that would act as a conduit among the customer, the bank data and all the fintech entities they're associated with. Once a customer submits a request of this API to authorize the API to gather and disseminate their data from their bank, the API would follow through and disseminate the data to fintechs that are affiliated with the API.

The fintechs would have your banking history and, using this data, underwrite you a product to outbid something you already have or something you do not have. Based on the data, they would pretty much know everything about you: what products you have, what products you don't have and what products you might need.

This is the essence of the concept of open banking. As you can imagine, the risks and threats surrounding open banking are many: Who regulates the APIs and by what privacy standards, provincial standards or federal standards? Who regulates the fintechs? Which privacy rules do they follow? How does a consumer authorize these players to disseminate their banking data? Once a consumer has given consent, can they revoke it? What happens to the data once a consumer has withdrawn their consent? How does a consumer know which players are holding their data?

Some of the bigger questions on cyber risks and hacking also apply: How easily can a fintech get hacked? What rules do they follow, and who enforces these rules?

Banks are highly regulated players with tremendous privacy standards in place in Canada, as are insurance companies. Where do fintechs fall into that hierarchy of standards? Canada's banks spend millions, if not billions, on technology to protect their customers' data, and even they get hacked. How about these fintech firms, which spend very little? These are a few of the big-picture issues that I will leave for this committee's consideration.

With respect to the insurance sector, as Mr. Lafrenière mentioned, with threats of cyber risks, we can say that, when it comes to mutual insurance companies, we believe there is minimal risk. lnsurance companies do not hold valuable financial data and, as such, are not as exposed to hacking as banks, for example, which hold much more valuable data.

I will leave you with an example. Of course, an insurance company insuring your home or car could be hacked; however, I am not sure a hacker would find it worth his while to know how old your car is or how many washrooms you have in your basement. Of course the risk of hacking exists; however, it is a question of degree.

With that, we're pleased to take any questions you may have.

● (1705)

The Chair: Thank you very much.

Mr. Spengeman, you have seven minutes.

Mr. Sven Spengemann: Mr. Chair, thank you very much.

Thank you both for being with us.

Let me start with open banking. You mentioned a couple of jurisdictions where this has become popular. What's the driver behind it? What do you see as the current trajectory for open banking? What's the case for the economic or social benefit, as it must happen for some beneficial reason? What's the upside of this? Is there an alternative to the way it's currently structured that might be functional?

Mr. Steve Masnyk: I'll start, and then he can add.

In Europe, the U.K., and some countries in Asia, it's a recent development over the last year to year and a half. The upside to open banking, as the pro-open banking people are saying, is that it provides consumers with more choice and that it provides more efficiency in the financial services sector. The trend is quicker, faster one-stop shopping. Some of the arguments that are being talked about are that a customer or consumer would have financial products with many different players. You might have a mortgage with your bank, another loan with another bank, and another product with a credit union. This would all encapsulate and regroup together all your banking data and your financial data. Those are some of the reasons why open banking is in place in these other countries.

Mr. Normand Lafrenière: Right now there are some issues. Some people do practise what is called, I think, screen scraping. Basically they're taking their data. They give their usernames and passwords to third parties so that they can take their data from one bank and from the other bank and so on and gather that information and provide that service, if you will. That would disappear with the advance of API. Basically, it would reduce the risk, in that sense, for those people who give their usernames and passwords to third parties, which, by the way, contradicts their contracts with their own banks.

Mr. Sven Spengemann: It's still too new to see if it consolidates as something of permanency. Is that your testimony, that it's really a fairly recent phenomenon and that the jury is still out on whether there's a state-of-the-art version of open banking?

Mr. Steve Masnyk: You're absolutely correct. As I said, in Europe and in the U.K. it's within the last 12 months, so there's no anecdotal evidence on how well it works or how badly it works, either way.

Mr. Sven Spengemann: Do you see it as a symptom of what some people call a diminution or decline of financial literacy among the public? Is that in part what could be driving it?

Mr. Steve Masnyk: It could be. I'm not a banking expert, so you'd probably have to speak to somebody a lot more knowledgeable than I am.

Mr. Sven Spengemann: Okay.

To those who would say, “If it consolidates itself and sticks around, regulate the fintechs better and encrypt the data transmissions better”, would that solve the problem?

Mr. Normand Lafrenière: I think we need standards to pass the information from banks to third parties, and those standards are not there right now. They're in different formats.

Mr. Sven Spengemann: It's just like the protection of medical records. It would be quite similar in that sense.

Mr. Normand Lafrenière: I would say so.

Mr. Sven Spengemann: Okay.

Mr. Steve Masnyk: Just to answer your question, Mr. Spengemann, most fintechs are registered and regulated provincially, so in a federal regime there would be a gap in regulating these fintechs. For example, now you have five or 10 strong federal players—the banks and insurance companies that are strongly regulated. If you have 2,000 weak fintechs or weak players that are not federally regulated, how does that open up the whole risk to cyber-attack throughout the country?

Mr. Sven Spengemann: I wonder if I could take a minute or so to ask you a slightly different question about the insurance industry. Your testimony is that the data that's held by insurance companies isn't of such sensitivity that there's a disproportionate risk in terms of cyber-threats to that data. Do you see the insurance business coming in and providing insurance to financial institutions for the protection of their data? In other words, can you insure against cyber risk? Is that something that's currently in place or being contemplated or developed?

● (1710)

Mr. Normand Lafrenière: Certainly the protection of data is there. Even though we represent less of a risk in the insurance industry, it doesn't mean that we don't have strong standards for the protection of the data of our customers.

Mr. Sven Spengemann: But in terms of product development and insurance packages, if a start-up is getting going, instead of developing their own cybersecurity system, they could get a third party to do it for them and then get an insurance policy for breaches. Is this a model that's...?

Mr. Steve Masnyk: Cyber insurance does exist. There are some very large players who do cyber insurance. But the question is, what exactly are you insuring? Are you insuring somebody to get a new identity, and how does that work? What kind of claims would you pay out? What kind of monies would you pay out for a person to get a new identity? How much does it cost or how difficult is it to get a new SIN number in Canada? I don't know.

That product does exist, and those are some of the arguments that fintechs are proposing—that cyber insurance is available and would cover these risks. But what is the cost of a new identity? How do you quantify it?

Mr. Sven Spengemann: Okay. That's helpful.

I have a bit of time remaining. I'm wondering if we could take advantage of your presence to supplement the testimony of the previous panel in terms of your assessment of where the Canadian banking sector is in terms of protection compared to other jurisdictions, maybe the Five Eyes, and what kind of trajectory it's on with respect to future threats and evolving threats.

Mr. Steve Masnyk: I think you would probably have to talk to the banking sector about that. It's not something we would have an intelligent opinion on.

Mr. Normand Lafrenière: For sure, we only have a certain number of players right now, and we know they spend a lot of money on protecting the data. Our concern is, of course, that when you come up with a whole bunch of new players, be they fintech companies, we're not sure the same protection will be there for data.

Mr. Sven Spengemann: I asked the question earlier about Canada's market size, or the size of our economy, and whether that's a constraint with respect to the net investment from private or public sector sources in cybersecurity. The sense I got was that, yes, in other jurisdictions there is disproportionately more investment because the economies are bigger and more complex and have more players.

Is it fair to say, then, that Canada would benefit from greater public commitment and contributions to the field of cybersecurity?

Mr. Steve Masnyk: When it comes to cyber insurance, most insurance companies that deal in this type of product are global. For example, you would have multinational insurers who do this. Lloyd's comes to mind, which is a very large multinational insurance company. It does quite a bit of cybersecurity.

Again, it wouldn't be the Canadian stand-alone entity; it would be the entire group that would be in that line of business. It's quite a global.... I don't think the size of the Canadian economy, and population-wise, would really matter.

The Chair: Thank you, Mr. Spengemann.

Mr. Motz, you have seven minutes.

Mr. Glen Motz: Thank you, Mr. Chair.

Thank you, gentlemen, for being here.

Unfortunately, most of Canada, I'm sure, has been watching the justice committee and what's going on with that, the implosion of this government and the pressure that was put on a member of their own government. Now, I say that—

Mr. Michel Picard: On a point of order—

Mr. Glen Motz: Hold on. It's coming.

A voice: Relevance—

Mr. Glen Motz: I say that because I understand that you gentlemen experienced something similar. Last year you raised concerns specifically about cybersecurity, and you were pressured by a minister's office not to testify, to keep quiet—

Mr. Sven Spengemann: Mr. Chair, he's putting words in the witness's mouth.

On a point of order—

Mr. Glen Motz: Let me finish the question, and then you'll understand.

Mr. Jim Eglinski: It's not putting words—

The Chair: Order.

First of all, Mr. Motz, you were wandering off a little bit on—

Mr. Glen Motz: It's exactly about cybersecurity—

The Chair: Excuse me.

You were wandering off on what may or may not be happening today, and that is your interpretation. Having said that, the issue of whether there were any discussions between the representatives of these companies and any minister of the Crown, insofar as these were not protected by privilege and they are prepared to speak to it, is a valid question.

Mr. Glen Motz: When you raised these questions and you were asked to play ball for their plans in the budget from last year.... Has either of you ever been provided with an explanation on why the government didn't want the public, in particular, to know and why they didn't want MPs from all parties to be aware of the concerns you raised about cybersecurity?

● (1715)

Mr. Steve Masnyk: No.

Mr. Normand Lafrenière: It was mostly about the open banking issue. We had concerns, the same concerns we just expressed, and we were encouraged not to talk to MPs.

Mr. Glen Motz: In that budget bill, the Liberals say their intention was to allow fintech companies to access and use data to provide services. Is that correct?

Mr. Steve Masnyk: Not exactly. It permitted banks to sell or transmit their data to third party providers, including fintechs.

Mr. Glen Motz: That seemed like legitimate legislation. Would it seem as though, if they wanted to convince you, they could show you draft regulations or provide an opportunity to comment on the issues prior to...? Did that occur? Did they allow you to provide that on this issue with fintechs?

The Chair: Mr. Motz, you're getting into conversations that may or may not have happened at some other point. We are limiting our study to the financial sector, and not beyond that. If you could focus your questions on how these gentlemen can contribute to the concept of open banking, I think that would be useful, as opposed to other areas.

Mr. Glen Motz: If we're talking about cybersecurity and open banking, are you aware of anyone else who may have been asked not to speak to committees on changes of sharing information from banks and other companies or groups?

The Chair: Now we really are wandering off. I don't know that this is a relevant and material question to what is before the committee at this point. What these gentlemen are presenting is what's relevant to this committee, not what may or may not have happened with other people doing other things.

If you could, please focus your questions on what they would know or not know, not what other people may know or not know.

Mr. Glen Motz: Sure.

Gentlemen, do your members have cybersecurity-sharing mechanisms, or do most of you belong to other various threat reduction or awareness organizations?

Mr. Steve Masnyk: I don't understand the question.

Mr. Glen Motz: Do you have your own cybersecurity mechanisms yourselves? Do you protect yourselves, or do you share those mechanisms with other similar industries? Do you contract that out? Are there awareness organizations that you use to ensure that your data is safe and secure?

Mr. Normand Lafrenière: Member companies use services to make sure that their system is kept intact.

We understand that all the companies use different outsiders, if you will, to help them do that, or they use internal knowledge, internal employees. There are many ways that are being used to do that, but they all spend money to make sure that their system is kept intact.

Mr. Glen Motz: Okay.

Those are my questions. Thank you, Mr. Chair.

The Chair: Thank you, Mr. Motz.

Mr. Dubé.

Mr. Matthew Dubé: Thank you, Chair.

I don't want to purport to know what Mr. Motz was asking about, but I do want to say for the record that my understanding is that there have been government consultations on the notion of open banking. If that was the direction of the questioning, I'm sure it does have some merit to the discussion, in my humble opinion.

The Chair: Had the question been phrased along those lines, it might have been a more appropriate question.

Mr. Jim Eglinski: He was continuously interrupted.

Mr. Matthew Dubé: That's fair enough, Mr. Chair. I respect your ruling, but certainly, when we shout down members with points of order as the point tries to get made, the chair has the right to rule on that.

Gentleman, thank you for being here. Forgive me for my layperson's understanding. When we talk about about apps, I'm wondering if we're also talking about applications through social media and things like that. What I'm getting at is, when we look at the Cambridge Analytica situation, part of what was at stake there was the fact that there was a legal grey zone with regard to data that was collected when a Facebook user would do one of these personality quizzes, or whatever. They were sort of clicking “Okay” and signing away a bunch of data they weren't aware of.

Is there a concern that by opening the floodgates for third party applications with regard to banking, someone could, say, log on to an application with the good intention of using it for a credit check or things like that—we see a lot of these services being offered—and then just scan through, as a lot people do, and click “Okay”, and then they've basically sold away a bunch of very private financial information?

In and of itself, this may not be bad; it may be used in the right way by the application user, but then if you get a breach, as with Equifax, the next thing you know, that data is being used for nefarious purposes—especially given that the third party app may or may not have the same type of security protocols in place as a large institution like one of the banks, which have been at this much longer in some cases.

That's probably a long-winded, convoluted way of getting to the question. What are some of the ramifications of where this could go, potentially?

● (1720)

Mr. Steve Masnyk: To your point, Mr. Dubé.... One, what is expressed and informed consent? What is a person agreeing to when they start dating a third party or an application, when they start having some kind of relationship? What is the consumer consenting to? Does the consumer understand what he or she is consenting to? What are the implications once you want to revoke that consent? How do you do that? Can you do that? Do people read the 75 pages, where it says, "Do you agree..." when they buy a product online? Does anybody ever read those 75 or 150 pages, other than going right to the bottom and agreeing? I think the bigger-picture question is, what are people consenting to?

Once you've consented with apps one, two and three, do they have any relationships with fintechs a, b, c or d afterward? Does anybody really know what they're consenting to?

I think if somebody really knew what they were consenting to, it would make a lot more sense. It would be truly informed, knowledgeable consent. In this case, regarding these APIs and these fintechs, what are you actually consenting to? That's one of the answers to your questions, I hope.

Mr. Matthew Dubé: I'm wondering how we make it clearer what's being given away and the implications of that. In other words, the concern I have is that the accountability might be different for a third party app versus a large player like a bank, which, just by the size of the enterprise and its role in society, ultimately has different accountability towards the public.

The question is about the potential proliferation of this. Should we be exploring stricter rules as to how the data is treated and how it's taken on from the banks, especially if this transaction is taking place on a device that itself may not be secure?

Mr. Steve Masnyk: If I were a public policy leader, I think I'd be very scared that this is opening up. As I said, you'll have 2,000 to 4,000 fintechs running around the country. Who knows who regulates them, what standards they have or how much money they spend on privacy? It opens the floodgates to massive cyber-hacking.

[*Translation*]

Mr. Matthew Dubé: Did you have something to add, Mr. Lafrenière?

Mr. Normand Lafrenière: Our position is that the consumer should have ownership over their personal information, not the financial institutions that currently hold the data. The consumer should be the one to decide whom to share their personal and financial information with. We'd like to see standards put in place to govern the transfer of data between banks and fintechs to reduce the risk of information being stolen.

That said, in a case where information is sent from a financial institution to a fintech and the data is then stolen from the fintech, the financial institution would feel responsible for data content and data keeping. We aren't sure that the fintechs participating in the system will have the same data protection standards.

● (1725)

Mr. Matthew Dubé: My question is about insurers in this new digital landscape. I'm going to give you a bit of an odd example, but I hope you get the drift. Quebec's highway safety rules require drivers to have winter tires on their vehicles for a certain part of the year. In Ontario, winter tires are optional, but it affects people's insurance premiums.

Are you worried about differences in cybersecurity standards and the potential impact on premiums? Some players could be subject to lower standards, and others could have higher standards. Should those standards be the same across the board in your industry to make transactions and essentially insurance easier to administer?

Mr. Normand Lafrenière: Yes. Certainly, the system for fintechs should be very robust. We know that's the case for financial institutions, insurance companies and banks. If fintechs are to be allowed to participate in the system, we think they should have to adopt very stringent data protection standards.

[*English*]

The Chair: Thank you, Mr. Dubé.

Mrs. McCrimmon, you have seven minutes, please.

Mrs. Karen McCrimmon: Thank you.

Thank you very much for your testimony, and for coming today.

I just want to clarify one thing. If I heard you wrong, please correct me. I think what I heard was that there is minimum cybersecurity risk to your companies or your customers. Is that correct?

Mr. Normand Lafrenière: "Minimum" is probably a big word, but there is less risk, just because the kind of data we maintain is of less interest—except for the credit card numbers and debit card numbers that insurance companies have in order to take payments. Apart from that.... Again, with the example of the size of the bathrooms you have, there's not much interest in that for a third party.

Mrs. Karen McCrimmon: You're just saying that you're not an attractive target.

Mr. Normand Lafrenière: We are less so.

Mrs. Karen McCrimmon: Okay. That's good.

Mr. Steve Masnyk: Unless somebody wants to know how many washrooms you have in your basement.... I'm sure somebody would find that very valuable, but....

Mrs. Karen McCrimmon: We'll put the cybersecurity piece of this aside, then, and talk about open banking. It's important not to conflate the two.

The finance department just held some consultations. Were you part of that?

Mr. Normand Lafrenière: Yes.

Mrs. Karen McCrimmon: Did you give testimony? I wish we had gotten it—

Mr. Normand Lafrenière: We did not give testimony. We participated in the consultations.

Mrs. Karen McCrimmon: I wish we had received a copy of that. That would have been handy. We would have been better placed to have a real discussion about the challenges of open banking. I've done some research, but only a little.

Your organization, CAMIC, is having a hard time with this open banking. You think there are significant issues with it.

Mr. Normand Lafrenière: Well, the issue that affects insurance companies.... There is a wall between banks and insurance companies. As you may know, going back to the four pillars, there has been a wall maintained between the banks and the insurance companies. A bank cannot sell insurance from the bank. They can have an organization selling insurance, but it's completely separate from the bank. The bank's data cannot be shared with that organization. The purpose of it is to prevent coercion, if I can put it that way—banks forcing customers to buy their product at the time they're granting a loan. So these two are separated, not to prevent banks from getting into the insurance business, but they have to have separate organizations and not share data between the two.

Through these fintechs, that wall would just disappear. You would have the possibility of a bank sharing data with a fintech, and that fintech could very well share data with a third organization, be it an insurance company or whatever. Therefore, the separation or the wall between the two would just disappear.

Mrs. Karen McCrimmon: I'm having a hard time understanding why CAMIC is opposed to it but the Insurance Brokers Association of Canada is not. You must see there's a piece of this puzzle we're missing.

● (1730)

Mr. Steve Masnyk: Madame McCrimmon, CAMIC is not opposed to it. CAMIC is saying that there need to be parameters and a framework that protect the privacy rights and extend the privacy standards of banks and insurance companies to these third parties or fintechs. CAMIC is not opposed to it. The discussion should be guided by some principles, in order for the end result to have this framework in place.

Mrs. Karen McCrimmon: Okay, but wouldn't the insurance brokers feel exactly the same way?

Mr. Steve Masnyk: I don't know. I don't speak for them.

Mrs. Karen McCrimmon: The latest article said that the brokers and the mutuals are split on the tactics, on whether to support open banking or not.

Mr. Normand Lafrenière: We're not necessarily opposed to open banking. We're saying that there should be parameters surrounding that.

Mrs. Karen McCrimmon: Okay.

Mr. Normand Lafrenière: On top of that, there is a wall between the banks and the insurance companies. Under the new system, under open banking, we would like that wall to be maintained.

Mrs. Karen McCrimmon: You obviously have some concerns that the Insurance Brokers Association of Canada doesn't have.

Mr. Normand Lafrenière: That may be so.

Mrs. Karen McCrimmon: That's the thing. It would be really nice if we could get things in advance—

Mr. Normand Lafrenière: Absolutely.

Mrs. Karen McCrimmon: —so we can study and have the questions ready for you.

Let's talk about open banking. Do you not think there are ways we could mitigate those risks, or are you just concerned that we're not aware of all the risks?

Mr. Steve Masnyk: We believe the open banking concept exposes cyber risk and cyber-hacking to a degree that's a lot larger than the current regime allows or permits. As I said, banks spend a lot of money on privacy standards and even they get hacked, so how about these new entrants, fintechs, that would likely spend very little compared to the banks or the insurance companies? Public policy-makers, such as you, need to keep that in mind when devising public policy on this. That's really the issue we are raising.

Mrs. Karen McCrimmon: Okay.

I liked what you had to say about full and informed consent. How do we improve that? What approaches are available to us?

Mr. Steve Masnyk: I'm not a cyber expert or a tech expert. You'd probably have to have somebody a lot more intelligent on that matter.

Mrs. Karen McCrimmon: Other countries have adopted this open banking. They must have protections in place.

Mr. Steve Masnyk: Most of the European countries that have adopted this have a unitary state of government, so there is no arbitrage between provincial and federal. The rules that apply across the country for banks, for APIs and for fintechs would apply to the entire country. They don't have federations, basically.

Mrs. Karen McCrimmon: It's a challenge, no doubt about that.

Mr. Normand Lafrenière: Most fintechs are provincially incorporated and they're not regulated. It will be a new world in terms of whether they need to be regulated and by whom.

Mrs. Karen McCrimmon: Okay.

Mr. Steve Masnyk: There is an example in the U.K.—

The Chair: Mrs. McCrimmon, you have 15 seconds left.

Mrs. Karen McCrimmon: That's good. Thank you.

The Chair: Just before I go to Mr. Eglinski, which study are you referring to? Is it a finance committee study, or is it the department's study on this issue?

Mr. Normand Lafrenière: The department has consultations.

The Chair: Okay.

Mr. Normand Lafrenière: It is the department that has asked for the consultations. They have put together a committee that looks—

The Chair: Is there any publication from that study?

Mr. Normand Lafrenière: No, not yet.

The Chair: Okay.

Mr. Eglinski.

Mr. Jim Eglinski: I am going to refer my questions over to Mr. MacKenzie.

The Chair: Mr. MacKenzie, welcome to the committee, again.

Mr. Dave MacKenzie (Oxford, CPC): Thank you, Chair. Yes, I'm brand new.

Thank you to the witnesses for being here.

One of the interesting things.... You're talking about the mutuals, and I think they are an important part of the whole equation, but there is a bigger picture of insurance companies also. I know that what you're talking about is more the liabilities insurance coverage with the mutuals, but I look at some of the big insurance companies, such as Sun Life or Manulife, and they get into quasi-financial services, or certainly mortgages and all those things.

The sharing of this information and the tying of services from a financial institution, such as a bank, to those types of insurance companies would open up a great deal of consumer information to those insurance agencies. Would that be a fair assessment?

● (1735)

Mr. Steve Masnyk: I'll try to answer the question.

The prohibition is on banks doing insurance, not on insurance companies doing banking products, so it's a one-way street. The reason for that prohibition being a one-way street is that banks are in the credit-granting business. Credit is a very powerful tool. Credit can be used to coerce a consumer to buy other products based on that very powerful tool of using credit, so the prohibition is a one-way street.

You mentioned Manulife. Manulife does have a bank, and that bank follows the same rules as the big five banks.

Mr. Dave MacKenzie: Do they have a bank, or are they associated with a bank to do their banking in?

Mr. Steve Masnyk: They have a bank. I believe it's called Manulife Bank or Manulife One. I'm not too sure of the name.

Mr. Dave MacKenzie: There are some that are out there now that call themselves banks, but I think they are associated through one of the chartered banks.

Anyway, all that aside, the other part is that when we look at the banks, I think almost all of them are also located in other countries. Most of them are in the United States; some are in South America, and some are in Europe. When information gets into a Canadian bank that has affiliates in other countries that may or may not have the same rules for insurance, do you see that as an issue?

Mr. Steve Masnyk: It's up to the jurisdiction that they operate in. Canadian banks operate in Canada under Canadian law. A Canadian bank operating in the United States would operate under U.S. law or state law.

Mr. Dave MacKenzie: I don't disagree with you there, but the access to the information might very well also be available to the bank's offshore facilities, if that's what you would call it.

TD Canada Trust is probably the best-known in Canada and the U. S. Their branches are—

Mr. Normand Lafrenière: They have more branches on the U.S. side, I think.

Mr. Dave MacKenzie: Yes. You can bank at TD in the United States—they just call it TD; they don't use “Canada Trust”—and your bank account is directly connected to your bank account in Canada.

We can have our rules in Canada, and we can have our rules in the provinces, but once it gets into that bank, is there anything that would prohibit them—under what was proposed—from selling that information to another fintech?

Mr. Steve Masnyk: I don't know. In TD's case, you would probably have to ask TD that question.

Mr. Dave MacKenzie: Do you have any concern about that?

Mr. Steve Masnyk: I don't know how TD or any other bank operates. You would probably have to ask them.

Mr. Dave MacKenzie: I'm concerned about the sharing of information when it goes across borders. Whatever we agree to today, technology tomorrow changes the whole picture. That's why I'm concerned. I know the chair was sensitive to The Globe and Mail article of a few months ago, but there's a reason why government may not want to talk about it. That's what concerns me.

Mr. Steve Masnyk: I have nothing to add on that.

Mr. Normand Lafrenière: The two sections of the act that were approved in last year's budget basically allowed banks or financial institutions to share information with other organizations. They allowed them to sell, transmit or exchange whatever information with fintechs.

These are the concerns we expressed at the time. What is it that's before us? Who will control that information? Would it be the consumer, or would it be the financial institution? We're just raising questions that need answers.

Mr. Dave MacKenzie: Thank you.

The Chair: Thank you, Mr. MacKenzie.

[*Translation*]

Mr. Picard, you may go ahead for five minutes.

Mr. Michel Picard: Thank you, Mr. Chair.

Mr. Lafrenière, do any life insurance companies belong to your association?

Mr. Normand Lafrenière: No, just property and casualty insurance companies.

Mr. Michel Picard: I see.

No one cares whether I have one or two fridges in my apartment. I agree with you. However, the fact that I have three or four fridges or certain big-ticket items may be of interest to those wanting to know my personal situation. Would you not agree that personal information that may seem trivial could be seen as extremely valuable in another context?

● (1740)

Mr. Normand Lafrenière: Yes.

Mr. Michel Picard: As you mentioned earlier, the new measures allow for data sharing, and as a result, insurance companies can obtain information from banks. Could you tell us what that relationship covers in terms of data?

Mr. Normand Lafrenière: It's not in force yet. It's subject to regulation.

Mr. Michel Picard: I see.

Mr. Normand Lafrenière: The law was changed to allow for that, but the regulations have to be brought in, and that hasn't happened yet.

Mr. Michel Picard: Very well.

Mr. Normand Lafrenière: It's not in force precisely because of the open banking study currently being conducted. That's what we're trying to figure out.

Mr. Michel Picard: Could any of your members' transactions be viewed as financial transactions made for commercial gain?

Mr. Normand Lafrenière: Of course. Being financial institutions, we engage in financial transactions. Since people pay for insurance coverage, that's part of it.

Mr. Michel Picard: Security-wise, how would you rate your systems as compared with the banks?

Mr. Normand Lafrenière: Our system security is very good.

Mr. Michel Picard: How does it stack up against the banks?

Mr. Normand Lafrenière: I'm not familiar with what the banks have, but I can tell you that our members shell out a lot to make sure their systems are protected and secure.

Mr. Michel Picard: Who are your members?

Mr. Normand Lafrenière: Mutual insurance companies.

Mr. Michel Picard: To your knowledge, is what your members spend on system security comparable to what the banks spend, taking into account routine operations?

Mr. Normand Lafrenière: Absolutely.

Mr. Michel Picard: For now, that's speculation, since we don't have the information. Isn't that right?

Mr. Normand Lafrenière: That's right. We don't have the information, but percentage-wise, it's certainly true.

Mr. Michel Picard: How does your industry define a cyber-threat?

Mr. Normand Lafrenière: The risk of a third party gaining access to our systems and retrieving information.

Mr. Michel Picard: What criteria do you follow when recruiting staff to make sure you have some control over the human risk factor?

Mr. Normand Lafrenière: My job is simply to represent the association. It's not our staff; it's the companies who do the hiring and have the computer systems.

Unfortunately, I can't answer your question.

Mr. Michel Picard: Right now, do your member companies and the banks share any data?

Mr. Normand Lafrenière: No.

Mr. Michel Picard: As we speak, then, there's no electronic access. It's reasonable to believe that the members of your association do not offer third parties a way into the banking system, a vulnerable entry point, if you will.

Mr. Normand Lafrenière: Absolutely.

Mr. Michel Picard: Thank you.

That's it for me, Mr. Chair.

[*English*]

The Chair: Thank you, Mr. Picard. You've had the penultimate question, and I'd like to ask the ultimate question before we adjourn.

I wonder whether you are understating the significance of the data that you hold. You keep talking about how many bathrooms and who cares, but actually that can be quite significant data in the hands of certain people who wish to do us harm.

I wonder whether in fact you might be taking a bit too casual an approach to your own cybersecurity from the standpoint of data protection, because—and I guess this is a heightened sensitivity on the part of this committee—you never really know how individuals with malicious intention can use that data against both policy-holders and the institutions themselves.

I refer you to a $100-million lawsuit against Zurich Insurance. When the lawsuits start to happen over cybersecurity, everybody starts to run around in dizzy circles because they realize that maybe the data they had or have is far more significant than they actually realize.

I'm curious about your reaction to the value of your data.

Mr. Normand Lafrenière: We're always concerned with the data we hold. We hold personal information, names, addresses and that kind of stuff. Of course, we cannot ask for as much information as others can. We cannot ask you how much you make or what your job is and that kind of stuff. That's separate from what the insurance companies ask. They want to know what kind of use you make of your vehicle. That's the kind of information they ask for and that you see in the files of insurance companies.

● (1745)

The Chair: Google is awfully interested in how far I drive and when I drive. I got into the car in my garage on Sunday morning and it told me that it was 21 minutes to get to my church. I think it was kind of surprised that I went to church.

What I would describe as innocuous data becomes, in the hands of others, fairly significant.

Mr. Steve Masnyk: Mr. Chair, you're absolutely right. We don't know what we don't know until somebody finds out what we don't know and that becomes valuable.

The Chair: Yes.

Mr. Steve Masnyk: It could be that we're understating it, but I think it's a question of degree. Banks and financial institutions have 100,000 times more data on you as a consumer than an insurance company would. Sure, there is personal data that insurance companies possess, as well as brokers, agents and so on, but it's a question of degree.

The Chair: I don't want to press you on the point, but I'm not sure I buy your core argument.

Anyway, thank you for that.

With that, we are adjourned.