HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 096 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, March 22, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, March 22, 2018

● (0850)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): I call to order the 96th meeting of the Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3)(h)(vii), we are on our study of privacy of digital government services, a study of e-Governance Academy. We have with us, via teleconference, Liia Hänni, senior expert, and Raul Rikk.

We've just been informed that they have a presentation, but it's only in English. They don't have a French translation, so I'm going to seek unanimous consent that they can present that to committee at this time. Do we have unanimous consent?

Some hon. members: Agreed.

The Chair: Thank you for that. We can go ahead with the English-only presentation.

Go ahead. Raul, can you hear us?

Go ahead, Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Given that we have some time, Mr. Angus has a motion on notice with respect to the issue we read in the news about Christopher Wylie and Facebook. Our job is to protect Canadians' privacy as best we can, and so I would seek unanimous consent that we adopt that motion today.

The Chair: Has everybody seen the motion?

Mr. Nathaniel Erskine-Smith: If I can't formally adopt Mr. Angus's motion, then I move identical language.

Some hon. members: Oh, oh!

Mr. Nathaniel Erskine-Smith: With the analysts' consent, we can do anything.

The Chair: I was just talking to Jean-Denis, and what we need is unanimous consent to move the motion. Do we have unanimous consent to move the motion?

Some hon. members: Agreed.

The Chair: Mr. Erskine-Smith, would you like to make your motion?

Mr. Nathaniel Erskine-Smith: I move, in the language of Mr. Angus's motion, that we invite Christopher Wylie, Facebook officials, and others, including the Office of the Privacy Commissioner, to discuss the recent privacy implications for Canada and Canadians with respect to the recent media attention of Cambridge Analytica.

The Chair: Would it be fair to say that the language is exactly the same as Mr. Angus's motion?

Mr. Nathaniel Erskine-Smith: It's identical language to Mr. Angus's motion.

The Chair: Go ahead.

[*Translation*]

Ms. Anne Minh-Thu Quach (Salaberry—Suroît, NDP): I have the motion here. I'm not sure whether you'd like me to read it.

[*English*]

Mr. Nathaniel Erskine-Smith: Yes, I have it here.

[*Translation*]

Ms. Anne Minh-Thu Quach: I can read it, if you like. The motion reads as follows:

> That, in light of the large data breach perpetrated by Cambridge Analytica and unreported by Facebook for several years, the Committee conduct a study of the privacy implications of platform monopolies and possible national and international regulatory and legislative remedies to assure the privacy of citizens' data and the integrity of democratic and electoral processes across the globe….

[*English*]

The Chair: There's no translation coming, so I'm just wondering if it's....

[*Translation*]

Ms. Anne Minh-Thu Quach: Do I have to start over? Is the translation coming through now?

It's important that we have the translation, so that we don't have the motion just in one language.

[*English*]

Mr. Nathaniel Erskine-Smith: We have a motion in writing, though, from Mr. Angus, and we have unanimous consent to move that motion. We're simply adopting the motion from Mr. Angus, the notice of which we've already received. I don't even think it needs to be read out, frankly.

The Chair: For clarification, is that Mr. Angus's motion, an NDP motion?

[*Translation*]

Ms. Anne Minh-Thu Quach: Yes.

[*English*]

The Chair: You moved the motion. Is there any discussion about the motion? We'll vote on the motion.

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

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

Mr. Nathaniel Erskine-Smith: In light of the fact that we have today's witnesses, then Mr. Fishenden on Tuesday and the former president of Estonia on Thursday, and then we're going to finish the net neutrality study, I would suggest that the subcommittee meet on Tuesday for the second hour, after Mr. Fishenden, to hammer out witnesses for this study.

The Chair: Sure. Yes, I'm sure that can....

Go ahead.

[*Translation*]

Ms. Anne Minh-Thu Quach: Forgive me, but would it be possible to get the presentations now? As a matter of principle, we are supposed to receive all briefs in both official languages.

[*English*]

The Chair: Do you mean the presentation here?

[*Translation*]

Ms. Anne Minh-Thu Quach: That's usually how it works for all presentations in all committees.

[*English*]

The Chair: We just moved a motion to unanimously accept the presentation in English only, and we all voted for that.

[*Translation*]

Ms. Anne Minh-Thu Quach: I was under the impression that the presentation would be given in English, but that we would have both versions in writing. We aren't getting the written versions until later, however. As a matter of principle, I generally object to that. Sorry, but this is a bilingual institution.

[*English*]

The Chair: As far as I know, I don't see that it's a bilingual issue. It's already been unanimously accepted that it would be in English only. This committee just accepted that unanimously. I'm not sure what the issue is there.

Other than seeing the presentation physically in front of you, you're going to see it on the screen, directly in front of you, as it's presented.

Go ahead, Mr. Picard.

[*Translation*]

Mr. Michel Picard (Montarville, Lib.): I'd like to make two points.

I certainly support the member for defending the French language and its place. That said, we need to consider two things. First of all, we have to take into account the circumstances and show some flexibility. I think the situation today is rare. Second of all, unanimous consent was obtained, as per procedure. I don't think there's reason for debate.

[*English*]

The Chair: Okay. The documents will be translated.

Liia Hänni and Raul Rikk, you may present. Please proceed.

Our technical folks have just said that your device is muted right now. Can you un-mute your device, please?

● (0855)

Mr. Nathaniel Erskine-Smith: I don't know if this bodes well for a digital government study.

Voices: Oh, oh!

The Chair: I think we have sound now.

Please proceed with your presentation.

Ms. Liia Hänni (Senior Expert, e-Governance Academy): Okay.

First, this is a great forum for us to have this virtual meeting with your committee. My name is Liia Hänni. I am a Senior Expert on e-democracy and open governance, and it is a real pleasure to share with you some views on how privacy can be protected in e-government systems. I understand that this is your main concern in Canada, to develop safe e-government systems in your country.

You may know that in Estonia we have succeeded in developing an e-government system that is very much used by Estonian citizens. I think we should first explain to you the foundations of a secure e-government in Estonia. I had the opportunity to present yesterday to a Canadian delegation from your Treasury Board Secretariat, so I have an understanding now of the kinds of issues you face in Canada.

In Estonia, the e-government—

[*Translation*]

Ms. Anne Minh-Thu Quach: The translation isn't coming through.

[*English*]

Ms. Liia Hänni: Can you hear me?

The Chair: I'm sorry; I'll have to ask you to pause for a second.

Go ahead, Madam Quach.

[*Translation*]

Ms. Anne Minh-Thu Quach: The translation isn't coming through. I'm not sure whether it's working for everyone else, but I'm not hearing the translation.

[*English*]

The Chair: I'm sorry, folks. Let's suspend for two minutes.

Ms. Hänni, just hold on for two minutes while we get this sorted out. You have my apologies.

●

(Pause)

●

● (0900)

The Chair: I'll call the meeting back to order. The translators weren't translating because there was an echo in the translation device.

Again, my apologies to Liia and Raul. Please proceed. You should be good to go.

Mr. Raul Rikk (Programme Director, National Cyber Security, e-Governance Academy): Good morning from my side as well.

My name is Raul Rikk. I work at the e-Governance Academy as the Director of the National Cybersecurity Program.

My background is from the security sector in Estonia. I was years ago responsible for establishing the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. I have worked in the cybersecurity and data protection area for 15 years.

Thank you for inviting us to present the Estonian model for data protection for a digital society, as well as for cybersecurity. Because of the video conference, we decided not to go through the whole presentation. We'll just use one slide that combines all the different aspects that we will probably discuss today. This slide points out the main principles in the data protection and cybersecurity area and describes the general architecture of how interoperability and security are ensured in Estonia in the digital space.

I believe that we could actually go straight to the questions. It is probably better to proceed this way.

The Chair: We will proceed, then. Thank you for that.

Just to let the committee know, there is about a three-second delay for them to hear us, even though there doesn't appear to be.

We'll start off with Ms. Vandenbeld for seven minutes.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you very much, Mr. Chair.

First, I'd like to give my greetings to Liia, whom I've worked with in the past. I'm quite an admirer of your work.

Thank you very much to both of you for being here in front of the committee this morning.

I'd like to ask Liia how this was initiated in Estonia. We know that Estonia is one of the countries that is leading the world when it comes to e-governance. Where was the inception of the idea? What was the foundation? Where did you begin in order to get to this point?

● (0905)

Ms. Liia Hänni: Thank you.

Of course, it's a long story because Estonia celebrated 100 years, and we've now had our independence again for 27 years.

We had this opportunity to start anew, starting from a new constitution. Immediately we had this question in front of us of how we can meet all the requirements of democracy and pick up on what the state.... It was decided that we should use the power of technology.

This was an important decision. Also, we could see that policy matters. If you have a strategic vision of your country and your society, you can do a lot. Several of these kinds of strategic principles really have been new, but it was for the well-being of all members of society. Nobody was left behind when we developed e-government and an information society.

Also, our conviction was that the e-governance structure and model in Estonia should be a platform for all society, not only for the government itself. It's a benefit we receive from e-governance. The system should be for all citizens of Estonia. Based on these principles, we have this model, which is presented on a slide by Raul.

This Estonian model has three important components. First, a strong digital identity is given to us by our government. Our vision is that it is a role of government not only to deliver paper passports but also digital certificates and digital identification tools for citizens. This is one building block of Estonia's e-governance system.

The second component is digital data resources. We have hundreds of databases that will take digital data, but it is not enough to have good electronic services for citizens. It amounts to interoperability. It means that all these numerous datasets need to form one uniform system. This has been realized in Estonia through a system we call X-Road, which allows us to connect all datasets into one system. This is the basic architecture of Estonian e-government.

Third, e-government is not separate datasets; it's a system that needs to have well-established architecture. Many view these as basic components of the e-government model in Estonia. A citizen's digital data and interoperability are realized by the X-Road system.

Ms. Anita Vandenbeld: I notice you are referring to the direct link between democracy and e-governance or digital governance, which I think is very compelling.

I know your institute has worked with 90 countries around the world. Can you tell us a little about some of the challenges faced by different countries and some of the lessons, particularly as we look at the fact that Estonia is a very small country? Canada, of course, is very large and very spread out. Do you see differences in the application of the lessons from Estonia when you go around the world into different countries?

Ms. Liia Hänni: I think that the size of the country is not as important as it seems at first glance. The challenges we have met are always the same. All governments want to have a good e-government system and provide good electronic services to their citizens, but to do this there are certain preconditions. I listed three of these preconditions. Usually what is missing in different countries is this understanding that e-government should not consist of separate information systems and that these systems need to work together.

This is mainly about interoperability, which is not only a technical issue but an organizational issue first. Different state agency organizations should be able to work together to share data and to put together these electronic services we have in Estonia.

● (0910)

Mr. Raul Rikk: If I may add, the very typical situation in different countries is that different organizations have developed their systems themselves, and the systems are not interoperable. That's the very basic problem.

The second problem is how to ensure security if you establish connectivity between different systems. That's the typical situation in different countries. That's exactly what we are dealing with on a daily basis.

Ms. Liia Hänni: I still want to stress how important digital identity is, because without this strong system of digital identity, people cannot use their very personal secure public services. This is their ID card, which has already been in use for 15 years. It's a very basic element of the secure economic system in Estonia. Raul, of course, can explain how it also protects security of data in the Estonian system.

The Chair: Thank you, Ms. Vandenbeld. That's time.

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

Hon. Peter Kent (Thornhill, CPC): Thank you very much, Chair, and thanks to both of you for your patience as we try to overcome some of these technical challenges. I'm still having some difficulty in hearing everything that you say through the messages, but we'll continue. That may be a reflection more of my age than of the technical shortcomings.

Mr. Rikk, some years ago in a parliamentary study of the defence of North America, an authority on cyber told us that any defences and any security applications were at best temporary because as the Internet was designed on an open principle, an open concept, so sooner or later the best security can always be breached.

Given that you are neighbours to one of the greatest cyber-vandals in the world today, how intense and constant is your maintenance of the security of your system?

Mr. Raul Rikk: I can assure that the situation is exactly as it was in the report [*Technical difficulty—Editor*].

The Chair: Just hold on, Raul. Your sound is completely gone now.

Raul, is your mike close to you when you're speaking, or is it farther away? If you can get the mike a little closer to you, that would help us out a lot.

Mr. Raul Rikk: We have the mike at the other side of the table, but the wire wasn't—

The Chair: If you can bring it closer to you, that would help a lot, because we're getting a lot of echo. It's very difficult to hear what you're saying.

Mr. Raul Rikk: Can you hear now?

The wire is...I have to sit closer, then.

The Chair: If that's possible, it would be appreciated. Our interpreters are having great difficulty translating.

Mr. Raul Rikk: Maybe you can turn the camera so that you can see us better. Now we are next to the microphone.

Is it okay now? Can I continue?

● (0915)

The Chair: Okay. Raul, if you speak, then we can see if that's better.

Mr. Raul Rikk: I will confirm that the study that you were referring to is correct. Our approach to cybersecurity is that it is a continuous process. We work on a daily basis to make it better and better and to coordinate with general ICT development.

Here's just one example. The whole security system that we use in Estonia is based on a state-of-the-art encryption system. Encryption is this technology that needs to be updated at least every two or three years. We have a specific department to deal with that. It does studies about encryption and supports the implementation of new encrypting systems every second or third year.

Hon. Peter Kent: If I could follow on, then, what devices do citizens use to access the service? Do you have an encryption key with a rotating password on it? How do you handle that?

Mr. Raul Rikk: That's exactly what Liia Hänni was talking about regarding the ID cards that we use. We call them ID cards, but from the security point of view, it is an encryption device that every citizen has in Estonia. On the ID cards, we have a chip that contains a cryptoprocessor, so basically, when a citizen uses an ID card, they actually use an encryption system.

Hon. Peter Kent: This question is in regard to one of your points on the baseline cybersecurity principle of no overlapping databases. Have you centralized the databases of all of the different services that you have on this interchange? Have there been problems with various institutions being reluctant to relinquish authority?

Mr. Raul Rikk: We have not centralized the databases, but the logic behind no overlapping databases is that we don't collect the same data in different databases. For example, if we have a population registry containing basic information about citizens and residents, then when police forces create their own police database, we don't allow them to collect the same basic information there. They have to take the most recent information from the population registry.

The idea is that different state institutions have authority over certain data. If they are allowed to collect this data and keep it in their database, then nobody else can collect and keep the same data. In this way, we keep the data in order at the state level.

Ms. Liia Hänni: This is a once-only principle that is applied in Estonia. It is that government cannot ask for my data if I have already contributed this data to some other information system in Estonia.

Hon. Peter Kent: Thank you, Chair.

The Chair: Thank you, Mr. Kent. Again, you have my deepest apologies for this situation. It was supposed to be all sorted out before, but it seems we can hear now and that things are moving along.

Next is Ms. Quach.

[*Translation*]

Ms. Anne Minh-Thu Quach: Thank you, Mr. Chair.

Thank you to our two witnesses from Estonia.

I'd like to know what kinds of oversight and data protection mechanisms the Government of Canada should deploy to prevent security breaches and digital attacks. The case involving Facebook and its sharing of users' personal data comes to mind. It's all over the media right now. Do we need to take legislative action? What kinds of resources do we need to deploy to ensure people's data are properly protected, investment-wise or expertise-wise?

● (0920)

[*English*]

Mr. Raul Rikk: There is no single answer to that, because when we talk about security, there are three main categories that we need to keep in mind.

One is confidentiality. The breaches can be against confidentiality.

The second is data integrity. It means, for example, that in the population registry where we have citizens' names, there is nothing secret about the names, but we have to keep the integrity of this data. We have to protect it so that nobody can access the population registry and change my name, for example.

The third aspect is availability of information. It means that we have to protect the network and data communication so everybody can access the data when it's needed. It's always these three aspects when we talk about cybersecurity.

When it concerns, for example, Facebook, then there is nothing to do with availability, I believe. Your question was targeted to personal data protection, and in this case, only regulations are of use because they put the responsibility to the company that provides the service. That's exactly why the European Union implemented the new General Data Protection Regulation that gives the power over the data to the owners of the data, the citizens, and imposes better control over the companies that provide digital services.

[*Translation*]

Ms. Anne Minh-Thu Quach: I missed part of your explanation. I heard what you said only at the end, about citizens being in control of their data security. However, when a breach does occur, how can the government make sure that it is reported or even that sanctions are imposed? I'm not sure whether Estonia has any sanctions in place.

Who is the authority making sure that data are protected and that corrective measures are taken in the event of a breach? If it's the responsibility of citizens, they aren't necessarily equipped to detect privacy violations. When it comes to government services, who provides that oversight?

[*English*]

Mr. Raul Rikk: That's what the General Data Protection Regulation is all about, putting in place different mechanisms to control the digital service providers. One very similar principle is that, for example, as a data owner, I must always get an overview of how my data is used. For example, if I use Facebook, when I approach Facebook and want to know how Facebook has used my data, they have to give a total overview of how they have done it. Also, if I want some data erased, they have to do it. Also, the third principle is that companies cannot make long-lasting commitments. For example, if the company asks whether I'm willing to give power over my data to them for 10 years, then this is not legally possible. The next day I can approach the company and say that I don't want them to use my data anymore, and they have to delete it. There are several regulatory mechanisms to control them.

Also, if something happens, there are very big sanctions against the companies, up to 4% of the annual global turnover. These regulation are bringing big changes, at least in Europe, to companies that provide digital services.

● (0925)

[*Translation*]

Ms. Anne Minh-Thu Quach: Who is the authority ensuring that oversight? Does your privacy and ethics commissioner make sure that all of those laws are followed and that private service providers are subject to oversight? Is that who takes care of that?

[*English*]

Mr. Raul Rikk: In Estonia we have a data protection agency, and every European country that belongs to the EU must have such an agency. The agency has the power to supervise everything related to data protection.

[*Translation*]

Ms. Anne Minh-Thu Quach: That's great.

[*English*]

Mr. Raul Rikk: Actually, it's an area where the EU has put a lot of attention in the last 10 to 15 years.

[*Translation*]

Ms. Anne Minh-Thu Quach: I see.

How much do governments invest?

[*English*]

Mr. Raul Rikk: I don't have the figures, but concerning the Estonian files, the agency has about 100 people. It's not a massive organization, but I would say that over the years their role has become more significant, because the whole of society has been digitized.

The Chair: Thank you, Ms. Quach.

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

Mr. Nathaniel Erskine-Smith: Thanks very much.

Previously when this committee did a study on sharing of information, witnesses suggested that an act put in place by the previous administration was too permissive of sharing of information. When you have a “tell us once” principle and you have agencies in Estonia that are able to access, using the secure data exchange, individuals' information more easily, how do you address the concerns about sharing of information that is perhaps too permissive?

Mr. Raul Rikk: In our situation, actually there is not a single agency that can get access to all exchanged information. That's why what you see on the slide is each route. This secure data exchange environment we also call the secure Internet. It works the same way as the Internet. The data exchange happens among different organizations or among the organizations and citizens. All this information exchange is encrypted and blocked, and nobody else can see it. There is no single agency that can see the contents of the information exchanged.

In the case of the security agency or a police investigation, they must have a code, permission, to do the investigation. It happens according to the regulations of investigations. In principle, everybody can only see the data that they are allowed to see. That's why we see the routes on the slide. You can first of all enter into the system as a citizen or a government official or a businessman; in each case you see a different view. It also depends on your personal role. You can see only those datasets that you are authorized to see.

Mr. Nathaniel Erskine-Smith: Thank you.

I know we have concerns here in Canada sometimes about identity theft. A classic example right now and for the last number of years is that scammers call people, particularly seniors but others as well, pretending to be our revenue agency.

Your citizens have an identity card that can potentially access all of the government services. I recognize you said there's encryption and that the card is in fact encrypted, but how does Estonia address identity theft of these cards, potentially? Has that been a concern? What are the processes you have in place to address that?

● (0930)

Mr. Raul Rikk: It might be surprising, but since we implemented the electronic ID cards, we have not had identity theft cases. We have had cases regarding their Facebook activities, but that's not the same thing. Regarding ID cards and accessing and using government services, we have not had any identity theft cases. That's because of the ID card.

Just to be correct, the ID card is not encrypted, but the ID card itself is an encryption device. By using my ID card, I can create secure connectivity to government services, or also private services —for example, banking services.

The ID card is issued by the government in the same way as passports. It's electronic and specifically designed for cyberspace. By that government process of identifying persons and issuing ID cards, we ensure that nobody can steal another person's identity.

Mr. Nathaniel Erskine-Smith: Thanks very much.

I've read about the Estonian system. When public officials access a citizen's information, there is a record of it. Perhaps you could speak to the transparency of the system. I would view my privacy as better protected if I knew when government officials were accessing my information, and why. How extensive is that documentation? What does that look like in Estonia?

Mr. Raul Rikk: The system works this way. When I want to access government services, I have to go to the state portal, which is basically the Internet site where all government services are listed and presented. When I log in to the state portal, I will see first all the information that the government has about me: my name, whether or not I have a driver's licence or medical insurance, and whether or not I own real estate or vehicles. I can see all the information that the government has about me.

Second, I also can see if there are some cases where government has used my data. For example, when I drive on the streets with my car and the policeman checks my licence plate number, the police patrol car doesn't stop me. They just type in my licence plate number to get all sorts of information about me, my vehicle, and other aspects. When the police patrol does that, it is immediately recorded. I will see later in the state portal that this policeman accessed my data because he did this patrol and I will see when exactly he did it. I get an overview of that.

In the same way, if I go to the doctor and the doctor sees my medical information, there will be a record of that. I will see it later, as an overview.

This way, the government provides the transparency. They show what data they have about me and how they have used it.

Mr. Nathaniel Erskine-Smith: I'm pretty well out of time, I think, so I'll give back my 10 seconds.

The Chair: We'll go next to Mr. Gourde for five minutes.

[*Translation*]

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

I'd like to stay on the same topic and discuss the state portal.

Is it a multi-purpose portal where a number of departments can go to retrieve information with or without citizens' consent?

[*English*]

Mr. Raul Rikk: This portal is designed for citizens and for residents as well. There are different.... Let's put it this way. Different state agencies provide different electronic services. Altogether, we have about 1,500 different electronic services. If you want to access these services, you can do it directly through the agencies' websites. If you don't know exactly what kinds of services are there, you can enter through the state portal. All these different state services are listed there.

● (0935)

[*Translation*]

Mr. Jacques Gourde: Can other public or private organizations, or businesses, use the state portal to retrieve information that could be of use to them in their work?

[*English*]

Mr. Raul Rikk: Maybe you can clarify your question.

[*Translation*]

Mr. Jacques Gourde: All right.

Can private companies, political parties, or others access the information in the state portal for their own gain?

[*English*]

Mr. Raul Rikk: No, absolutely not. That's the information that only I see. Not even different state institutions see that. Only I see the whole picture that concerns me. Different state agencies see only the portion for which they are responsible.

[*Translation*]

Mr. Jacques Gourde: What threshold do you apply to the data in the portal to determine what is considered public information? It provides a person's name and address, but does it stop there? For instance, are public telephone numbers, cell phone numbers, or email addresses considered public information? Where does the threshold lie?

[*English*]

Mr. Raul Rikk: Information is very specifically described in the public information law. We have specific law that describes what information is public, what is personal, and what is for administrative use. The whole system, the technical system, is built according to this law.

[*Translation*]

Mr. Jacques Gourde: Some websites list the cell phone numbers of nearly everyone on the planet, even though those devices are the private property of citizens. Is there any oversight of those kinds of sites?

[*English*]

Mr. Raul Rikk: Yes, exactly. The control is done by the data protection inspectorate, the same agency that I mentioned before. They have the authority to oversee all activities in the digital world.

Ms. Liia Hänni: Generally the information in government databases is not public information. This is personal information, all about me, but in Estonia to get that from the different databases is based on my private identification code. This is very basic for digital identity in Estonia, and also this special number gives me access to different databases that contain data about me. Personal identification codes are basic for Estonian data exchange and privacy protection.

[*Translation*]

Mr. Jacques Gourde: I have one last question. Do we need international legislation? Different countries have different laws, so we can't guarantee the same level of privacy protection if information is obtained through another country.

[*English*]

Mr. Raul Rikk: We believe that we don't know the Canadian situation so well. What we can say is that everything—at least, what we do in the digital world—is based on legislation that was developed with digital development in mind.

● (0940)

Ms. Liia Hänni: The Estonian experience is that we can protect private data better in the digital environment than in paper forms. If someone is looking at my paper documents, I cannot get information about that, whereas digital information transactions are visible to citizens. This is a very important fact to consider, actually.

The Chair: Thank you, Mr. Gourde.

Next up, for five minutes, is Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good morning. Thank you very much for being here.

I want to ask a more general question related to foreign policy.

The attacks in 2007 were in part precipitated by a domestic move that you had made in Tallinn to move a statue, from what I understand. Please correct me if I'm wrong. Going forward, the decision was made legitimately by a sovereign country to do what it wanted domestically regarding certain issues. The attack emanated from that.

Going forward, in terms of your foreign policy, have you been more hesitant? Are you more tempered in what you say? Has it changed your outlook in any way to not irritate certain countries in the world? Has that changed in any way?

Mr. Raul Rikk: If I think back to the time when we had this incident, I ask myself what lessons we learned.

One is that we have to co-operate more closely with the countries that believe in the same values as we do—basically, all democratic countries. Regarding those countries that don't appreciate the democratic way, we just have to keep in mind that we need other solutions, technical solutions or otherwise, to prevent other incidents from happening.

I think it has certainly been reflected in the foreign policy, but more to the positive angle of how to co-operate with democratic countries. In the NATO environment, the EU, there is a very good example: somebody mentioned earlier that Estonia is quite a small country—and that's true; it's only 1.3 million people—but now we have influenced the whole European Union in that the same principles we talk about today are already implemented in the EU, where there are 500 million citizens. That certainly was the product of our foreign policy.

Mr. Raj Saini: One of your strategic objectives in your cybersecurity policy is international co-operation, and since the attacks of 2007 certain things happened. One was that NATO undertook their own review. I also believe the U.S. government has people there to help protect against cyber-attacks.

However, when we talk about international co-operation—I'm specifically talking about your objective, which I think is a very noble objective—in many cases the countries that are predisposed to creating attacks may not be democratic and may not have the democratic principles that we enjoy. How do you navigate that?

You talked about the European Union—which is fine, since the countries are democratic—but when it comes to international co-operation, a lot of the attacks that will emanate against certain sovereign states will not be from countries that are democratic or stable.

How do you approach that issue when a part of your founding principles in your cybersecurity document is international co-operation?

Mr. Raul Rikk: We do that through the European Union, because all these countries you've probably referred to are quite big. They are simply not discussing this matter with us, so the only way to deal with these countries is through the EU foreign policy.

Also, let's say that the international co-operation or foreign policy in this area gives something like probably 30% of the security, but most of the things that we could do are still technical. Implementing new technology ensures security in cyberspace for us, and through the foreign policy we handle only the part that we cannot do technically.

● (0945)

The Chair: There's a bit of a delay, so if you have one last....

Mr. Raj Saini: That's fine.

The Chair: Thanks, Mr. Saini.

Next up for five minutes is Mr. Kent.

Hon. Peter Kent: Thank you, Chair.

To your point that there have been no instances of identity theft—and I think that's an impressive reality— I understand that several months ago, some 760,000 personal certificates were suspended, not because there had been a breach but because of a threat assessment that the chips within the cards were perhaps defective or vulnerable.

Could you explain what happened there?

I understand that these chips are not made in Estonia but in Switzerland.

Mr. Raul Rikk: Yes.

We found out that the company that produced the ID cards for us didn't use the best possible encryption logic. The cryptoprocessors that were on the cards were not made as per what was written into the contract. Basically, they were not good enough. These chips were produced by the Swiss company Gemalto, and the specific chips were made by German company Infinia.

That was a case that affected not only us but also Spain, Slovakia, Microsoft, and everybody else in the private sector and public sector who used the same chips. It concerned the chips that were produced in a certain time frame, from late 2014 to 2016.

Regarding Estonia, it was a massive incident, because it concerned about half of the ID cards that we use in Estonia. We could say that half of the population was basically under theoretical danger.

I have to emphasize that nothing happened, because we got out of this vulnerability and we reacted very quickly. Basically we developed a solution in two months, and we started to issue new certificates immediately after that. We didn't have any security incidents, but it put the specific concern on our table of how to approach that problem in the future and how to avoid buying a product that is certified and later finding out that the certification is not correct.

Hon. Peter Kent: That brings up another question.

Given the rapid evolution of technology and the evolution of cyber-threats, what sort of turnover would you foresee in terms of having to reissue new certificates with updated safe encryption technology?

Mr. Raul Rikk: The update was done over the Internet, the same as we do updates for our personal computers. Resource-wise, it wasn't very massive. It simply meant that each person had to plug their ID cards into their personal computers and update the certificate. They have to do it anyway every second year, so in this case they had to do it earlier. Resource-wise, it wasn't a massive problem, but it was a problem of possible vulnerability that we didn't know about.

● (0950)

Hon. Peter Kent: What is the cost consideration in terms of the individual certificate and the chip it contains, the technology that it's capable of managing?

Mr. Raul Rikk: I don't have the calculation of how much the certificate costs, but the ID card with cryptoprocessor certificates and everything costs 20 euros per person. We didn't need to change the ID cards, only the certificates, so I would guess that it cost maybe 1 euro per person.

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Next up for five minutes is Monsieur Picard.

Mr. Michel Picard: Thank you.

Since we just have five minutes, let's go straight to the questions.

A system is as good as the persons who manage it. How do you manage the risk to avoid an inside job, from your human resources standpoint?

Mr. Raul Rikk: We manage the inside vulnerabilities again by using the ID cards. With respect to what different persons do in the cyber-environment, there is going to be a log. Everything is going to be logged, and we can investigate the log later. If the administrator, for example, wants to do something in the system, they have to identify themselves with their ID card. That's how we prevent that. That's one measure.

The second measure is that we don't have one big database. As you see on the slide, there are hundreds of different databases under different authorities, and different persons have access to these databases. Everything is decentralized and nothing is concentrated, so if somebody even gets access to certain systems and is able to cause harm there, they have limited scope to do that. They cannot take down the whole system.

Mr. Michel Picard: About the fact that you have a separate databases, there are two things. First, from an investigation standpoint, we develop more and more software to create bridges to look at different databases to be able to create relationships, because the quality and efficiency of a database is its capacity to create relationships. By separating your databases, do you create redundancy and therefore slow down any process of research or investigation?

Mr. Raul Rikk: To be honest, I'm not sure that I understood your question.

Mr. Michel Picard: Okay, let me go again.

I'll give you an example, and it's not promoting the product, but just to know how it works.

In investigation, i2 Solutions developed bridges that can catch data from different databases and put them together, because the quality of a good database is its capacity to create relationships—the name, address, time, patterns, friends, and so on. By creating databases that are separate, do we have to make redundancy? Also, going from one database to the other, from an investigation standpoint or research standpoint, is slowing down the process quite importantly.

Mr. Raul Rikk: Let me explain how the system works. Maybe it will answer your question.

On the slide you see these different databases. Some of them are in the public sector and some of them are in the private sector. We make the connectivity between the databases through the secure data exchange environment. We call it the X-Road. It's a state-controlled environment. Everybody who wants to be connected to this data exchange environment has to, first of all, implement certain security regulations, security guidances, be up to the standards, etc. They have to apply to be part of this secure data exchange environment. It means that we keep an eye on the data exchange. We control that. We don't go into the data itself, but we control how the data exchange happens. Everything is encrypted, as I mentioned, logged, and time-stamped.

The way we get information from the databases is not by going directly into the database. Instead we get the information through the electronic services that you see on the slide. There is e-police, e-school, e-tech support. This is like a presentation format. The electronic service takes predefined data from different databases and then presents it.

● (0955)

Mr. Michel Picard: I have one last question regarding identity theft.

The problem investigating a computer crime is knowing who is sitting on the chair and typing on the keyboard. With someone using a card, how can we be sure the one using the card is the right owner?

Mr. Raul Rikk: Of course it's a very good question, but there is no way to be 100% sure or identify the person. Our police use different techniques to solve cybercrimes. One part is the ID card, but of course the ID card itself doesn't give 100% certainty, so they have to use other techniques as well to investigate the cases.

Mr. Michel Picard: Thank you.

The Chair: Thank you, Mr. Picard.

I want to welcome back Mr. Cullen, a former member. You'll just have three minutes. It's nothing personal.

Mr. Nathan Cullen (Skeena—Bulkley Valley, NDP): Yes, yes....

Voices: Oh, oh!

Mr. Nathan Cullen: Yes, I did notice that, Chair.

The Chair: I just wanted to alert the committee too. We have lots of time.

Mr. Nathan Cullen: We have lots of time, but I just don't have lots of time. Is that what you're trying to say? I get it.

The Chair: We have until 10:45 a.m., so after Mr. Cullen's questions for three minutes, we're just going to open it up and go around the table.

Go ahead, Mr. Cullen.

Mr. Nathan Cullen: I will be quick.

Thank you to the officials. I apologize that I missed the first part of your testimony, so forgive me if there's anything that I ask that you've already covered.

Let me start with a question. Are you able or prepared to answer questions about the electronic voting system that's used in Estonia? Can I assume it uses the same basic network and security system that you have for your e-card?

Mr. Raul Rikk: In general terms, yes, I am prepared to answer questions; if you go very specific, then of course I am not.

Mr. Nathan Cullen: Beyond the specifics, I'm wondering about the recent revelations, not just about Facebook but about the fairly massive data breaches that we've seen globally. In the United States and also here in Canada, both so-called traditional companies and companies that were electronically based and experts in the field have failed to keep their data secure. These are entities with an enormous business profit incentive to do so. They include Uber, Yahoo, Target, Sony, the U.S. government, and the Canadian government.

To return to voting, there has been some criticism of the security of your voting system, particularly because, as we've heard in testimony at a different committee here, the ability to breach an electronic voting system and then cover your tracks, so to speak, is a serious threat to democratic nations.

With the involvement of other nations and other actors in domestic political affairs, what has Estonia done recently to make your electronic voting system more secure, so that elections are free and fair?

Mr. Raul Rikk: The recent development was that when I vote, after that I can.... For example, if I go to a computer, I can check whether or not my vote reached its destination. I can check that with my mobile phone. There are two ways to make sure that my vote went to the place it was supposed to.

Regarding the whole voting system and the security of the voting system, there are many different technologies and procedures that we use. I have to say that the critique is always welcome but not always very relevant.

For example, very often the critique is like somebody claiming that a candle on the table may cause a fire in the building. We all use candles, especially during Christmastime, and very rarely a fire happens after that. Of course, when you have an open fire on the table, there is always the potential for a fire.

Mostly the critique against the voting system is of the same kind. They claim that something might happen, but in reality we have not seen that. We have not had any incidents regarding the voting system. There is always supervision and control and there are different ways we do that. If we implement all of that, we can say that it is secure. Of course, potentially there's always something, always some trick.

● (1000)

The Chair: Thank you, Mr. Cullen.

Go ahead, Ms. Hänni.

Ms. Liia Hänni: I was a member of a constitutional affairs committee when we made the basic decision to start Internet voting. Of course there were concerns, but the e-voting system is constantly upgraded to meet the different risks that may be there.

Basically, in the Estonian system there has been no case of some kind of breach or interference in the voting process, and because of that, Estonian citizens are using Internet voting more and more. There is trust already. Of course, it's always the case that technology may contain risks, but as I said, you need to be ready to meet these risks and not stop going ahead. That is my political view.

Mr. Raul Rikk: A very quick comment is that the voting system is not totally separate from what we have already talked about. It's still based on the ID cards, with a very good encryption system.

The Chair: Thank you both.

Next up we're going to go for seven minutes or less. I'm sure that it will probably be less.

To start off, we have Mr. Kent on the list, Mr. Baylis, and Mr. Erskine-Smith. If you want to be added, we have approximately 40 minutes.

Hon. Peter Kent: Thank you, Chair. I just have one question, which follows on the last remarks about the voting system.

Have you any measure of public acceptance of the electronic data system as it has been put into practice and continues with occasional challenges here and there, like the reprogramming of the 750,000 certificates? Have you done any polling to gauge public acceptance of the system or satisfaction with the system?

Ms. Liia Hänni: Generally, Estonians use the e-government system, and I think this is basic, because if there is no use of e-government to build it up....

About Internet voting, you can see from these slides that there is constant growth of the number of e-voters. We had local elections last autumn, and about one-third of those people who took part in the elections voted online. However, in Estonia, as I said, of course there are people who still oppose Internet voting, because there is no 100% insurance that nothing will go wrong. As you can see, it's part of the normal process in Estonia, but we can still choose what channel to use for voting.

In Estonia, people think it's good to have electronic governance, and the biggest concern is about how we are progressing. Are we able to meet all these new opportunities that technology will offer us, like artificial intelligence, for example?

Hon. Peter Kent: How do you deal with the capabilities or the confidence that older generations might have, who are not fully engaged in the Internet or current technology?

Ms. Liia Hänni: I think you are referring to my generation, because I'm also a very nice age.

Voices: Oh, oh!

Hon. Peter Kent: It's my generation too.

Ms. Liia Hänni: It's important to understand that the older generation can still learn and have new opportunities. In Estonia, the government also had several special programs to encourage the older generation to take part in the information society. The programs involved looking at the world and sending buses to different villages in Estonia and training older people to use computers, but I think our younger generation, being 100% online, can also provide good assistance to their grandparents.

● (1005)

Mr. Raul Rikk: We have actually measured how younger and older people approach this voting process. The statistics are quite interesting. They show that young people take more time to vote, and the elders do it more quickly and efficiently. They don't surf on the voting website, but they follow exactly the procedure that they're supposed to follow, while the younger generation just surf and don't always push the correct buttons. It shows that members of the younger generation know very well how to play Minecraft or how to use Facebook, but not necessarily how to use ID cards and follow official procedures.

The Chair: That's interesting.

I just want to clarify who.... I only have three names on the list. I thought I saw more hands over here. I just have Mr. Baylis, Mr. Erskine-Smith, and Mr. Picard. We'd like Mrs. Vandenbeld, as well. Maybe just hold your hands up if I didn't get your names. Okay, so we have Ms. Murray and Mr. Cullen again.

Okay. We'll proceed with Mr. Baylis for up to seven minutes.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Thank you.

I have some questions for you, Ms. Hänni. I've looked at this excellent slide and how Estonia has arrived at this very comprehensive system, but obviously you didn't start there. If we were going to think about building something like this, where would we start? Is it the population register, the unique identifier? What would be the process?

Ms. Liia Hänni: That's a good question and a very important question.

I think what definitely is needed is an electronic identification system. In Estonia, it's based on the unique identifier of citizens. I know that in Canada there is no population register for the whole country, just provincially, so you definitely should think about how you ensure a strong identity for your citizens.

Second, since you have a great number of datasets that are not connected to each other, that belong to different agencies, you should think about how to build up a system in which data will move, and once you have this capacity for data to move when necessary, then, of course, a system to protect data integrity should be in place.

In Estonia, with X-Road there are different technical facilities to protect data, but basically, in connecting datasets with X-Road, there is a check on privacy issues, there is a check on security issues, and there is a very defined authority, a different institution to make the data work properly.

You have very good systems already, with lots of data online, and a good vision about open government, so I think it's a matter of political will to make these basic new decisions to have not only good separate information systems but to see Canada, the physical environment of Canada, as one system. This is, I think, the work you face now.

● (1010)

Mr. Frank Baylis: When you were building your system, were there concerns? I know you talked about how it integrates into the democracy itself. Were there concerns that you had to overcome? You mentioned one of them, electronic voting with older people, but in a general sense, as you were moving towards this highly digitized society, how did you bring your population along with you?

Ms. Liia Hänni: I think the Estonian population was quite positive about this use of technology. Even when we introduced electronic voting, a bigger part of society was not using the Internet, but still people who were not using the Internet were very positive. There wasn't that kind of opposition to the use of technology in Estonia, in my opinion.

What was right, what parliament did, was put some basic legislation in place, such as the digital identity we introduced in 2001. The digital signature is the most-used electronic service in Estonia. We don't need to sign documents on paper anymore. We use digital signatures, and there's a huge economy of resources, time, and money in having this opportunity at hand now.

The Estonian e-government development was not one project. It was step by step, but we made the right decisions at the right times. Digital identity use, legislation, and technology for that X-Road, and this interoperability layer we have were all necessities, because we had in Estonia a similar situation to what you have in Canada. There were different datasets not working together, and the X-Road exchange layer was a necessity to overcome this situation. Because of that, now we don't need to count how many electronic services we have, and it's very easy to have new electronic services, to put together information and data we have in our systems.

In Estonia, government can only use my data based on law. Data cannot be used by the government unless the law gives the authority to government institutions to ask for and use my data, and this is very important and different from private businesses, where gaining my consent may be the driving force to use my data.

Mr. Frank Baylis: I have one other question. You've clearly consulted with a number of different countries on things, and people have come to see and learn from Estonia. Are there some lessons on what we should avoid, some dangers, some pitfalls that we should be aware of if we start to go down this path, something you might have seen other countries do wrong?

Ms. Liia Hänni: Our experience is that all the countries we are working with are in favour of having good electronic services, but to have a system, the governments should be able to make quite radical changes to the attitudes they have had up to this moment. Electronic government development is not so much about technology or a new information system; it's about innovation, about innovative co-operation among different ministries. Interoperability is technology, but it's also about how to overcome the silos in state administration, how to get all organizations to work together. This is the most important challenge that many countries still face.

The Chair: Thank you, Mr. Baylis.

Next up is Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Thanks very much.

I have a couple of really short questions and a couple of longer ones. I'll start with the short ones.

We've previously spoken about how when government officials access information, there is a record and it's transparent. What's the penalty if government officials improperly access that information?

● (1015)

Mr. Raul Rikk: In this case, we don't have defined penalties. Every time this kind of incident happens, we have an investigation, and then there is a court decision as to what the penalty is going to be.

Mr. Nathaniel Erskine-Smith: It depends upon the seriousness of the misconduct. Okay.

Our Privacy Commissioner recently commented in the media in relation to worries about digital government services, but it seemed that his primary concern—we'll have him here at a later date—was the government collecting public information about citizens, whether it be on Facebook or otherwise.

Does Estonia engage in these practices? Is this part of digital government?

Mr. Raul Rikk: Our government doesn't collect data from Facebook. The only data that our government collects is as Liia has mentioned, according to the legislation directly from the data owners, the citizens.

Mr. Nathaniel Erskine-Smith: Great.

I can imagine that some senior citizens in my riding, who perhaps don't use the Internet as much as I or others might, would have some concerns about customer service moving to being completely digital and about how they would lose the services that they have or about not being able to get someone on the phone to have the ancillary services to support their access to the digital environment.

What is the Estonian experience? If I'm having difficulties with digital government service, who do I turn to?

Mr. Raul Rikk: If you have difficulty, you can always go to the government service centre and get help there, but the digital solutions or services scheme is that if I want to do it over the Internet, I don't need to go to the government service centre. I can do all my digital operations or interaction with the government wherever I am—in Canada, Australia, or New Zealand. It doesn't matter. As long as I have Internet connectivity, I can use all services that are available.

Mr. Nathaniel Erskine-Smith: We haven't discussed this. We've seen X-Road. We've seen the no-overlap concept in databases. We have your list of various ways that security and privacy are protected. How is blockchain used in protecting the privacy of Estonian citizens?

Mr. Raul Rikk: That's a very good question, because there has been a lot of hype about blockchain in recent years. Everybody talks about it, but we use it to make digital signatures secure. We started to use blockchain logic before the name was even invented. Once we issued the first ID card in 2002, blockchain logic was already implemented in the system.

What we basically do is to put the old digital signature or the fingerprints of the digital signatures onto the new digital signature. Basically, we link different digital signatures to each other so that whatever happens with encryption in the future, we can still have the secure link of the digital signatures.

Mr. Nathaniel Erskine-Smith: With regard to other countries adopting more digital government, Finland, I've read, is straight up wanting to use X-Road. Other countries are developing their own systems.

Is Finland the only country looking to use the same technology that Estonian digital services are based on? Are other countries doing the same? How is that working?

Mr. Raul Rikk: That's what we are working with on a daily basis. Finland is one country. We have done this in other countries as well, although not so much in Europe, but it depends on different countries' approaches to the data exchange. We believe it is the best solution to how you can connect different databases. None of the organizations need to change what they already have; they just implement the security layer onto the existing systems.

I don't have the answer to why most of the countries have not started to use it.

Mr. Nathaniel Erskine-Smith: We haven't really discussed private sector collaboration. Perhaps you can explain. I see in the chart that the citizen is beside the government is beside business.

How is individual private and personal information shared with businesses in the private sector in this context? What different sectors have access to this information through digital government services? What best practices preserve people's privacy?

● (1020)

Mr. Raul Rikk: Each time the private sector wants to use personal data or they want to get connectivity to the X-Road environment, they have to prove their need to the data protection inspectorate. They have to justify why they need it. The data protection inspectorate allows them to use the personal data. Mostly the private sector provides service. They have certain data about citizens and they provide this data for the government service.

For example, there's the electronic tax declaration. The banks have information about personal incomes. Banks create the reports. I can go to the banking service and allow my bank to send this data to the Estonian tax board, which can take this information and put it on my tax declaration. I don't need to do that. That's how it works. The private sector generates certain information, and they can provide it to the government through the secure X-Road.

The Chair: Thank you.

Mr. Cullen is next up.

Mr. Nathan Cullen: Thanks.

I'm wondering if there are any prescriptions in the law about where the servers must be located. Do they all have to be based within the boundaries of Estonia, or do you have a scenario in which some of the private sector partners that you have or government services can be located outside the country?

Mr. Raul Rikk: There are limitations concerning the critical or essential services. Banking systems are one of them. For example, after the 2007 attacks, some Swedish banks wanted to take the data from Estonia and keep it in Sweden. The Estonian Parliament regulated that the data concerning banking information must also be located in Estonia. They can keep it in Sweden or other countries if they want to, of course in an encrypted way, but it must also be in Estonia so that if something happens with Internet connectivity, it doesn't affect the provision of service.

Mr. Nathan Cullen: You may have covered this already. I was just reading through the history of why Estonia has come so far on electronic government services. It has been referred to a few times, but I still don't understand the e-minded coalition government in 2001. Was there an election in 2001?

We're in politics; people can say “blockchain”, and I can nod, but I really have no idea of what we're talking about. I can read it six times and still not fully understand what we're talking about. In any case, there was some political energy at the turn of the last century to bring Estonia down this path. Was there a political event, an economic crisis? Did something precipitate this sort of political consensus to take such a long and relatively bold step?

Ms. Liia Hänni: It started earlier. It was a part of Estonian state-building from scratch, actually, after the Soviet occupation. We had this vision and strong political will to build up a modern state and our technology. We had some technologically knowledgeable people, and also politicians who believed that technology could support us in these efforts to modernize and build a really modern state. There was no political opposition to the use of technology.

There was opposition when we introduced digital identity cards in 2001. There was debate in the constitutional committee. Some members of the committee asked why we needed this digital identity, what kinds of services the government would offer. It was difficult to explain at that time what exactly we would do with this digital identity, but we still had some vision that digitalization would go on and that sooner or later we'd need to have the opportunity to identify ourselves in the digital world. We made this very correct decision not to make our identity card for digital identity a voluntary action. You are obliged in Estonia to have a digital ID card. All citizens and residents of Estonia must have it.

● (1025)

Mr. Nathan Cullen: I understand. I want to to thank you for that.

I want to turn back to the question of a government doing any data mining outside of just direct government services.

I can see the rationalization of a government's saying that in order to understand the impacts of a vaccination program or an economic program that it is running, one of the great datasets out there for how people are talking about a program or a service or a certain government policy is social media. As a government, we do polling all the time, but we also know that polling is limited in terms of its understanding. Many people are spending more and more time online, and more people are having their political or just their local discussions in social media environments.

You said earlier that the government doesn't do any data mining off the Facebook social media site. There are many others, and there are others that are more popular in Estonia. Why not? Why wouldn't...? Understanding the good-intentioned motivations—not even nefarious motivations—of a government to do this, and with the breaches just within Facebook itself, one could imagine a government having a contract whereby it would understand our latest child care policy and whether it's having any effect by mining data and finding out what people are saying about it on Facebook, Twitter, or Instagram.

Ms. Liia Hänni: In Estonia, social media are still very much used in the public sector, but that's basically for communication with citizens. It's not exactly necessary to take from Facebook this information on what people think about the government and government services. We are quite open to direct co-operation with our government, rather than through Facebook.

Definitely there is a lot of information in Facebook. I'm not speaking against this opportunity to use this information to improve services, for example, or to better understand political processes, but definitely not to profile our citizens in order to get some more political power and political interest. I think this is what you are talking about.

Mr. Raul Rikk: Profiling is not allowed according to the new EU data protection regulation. It is prohibited, basically.

Mr. Nathan Cullen: I'm sorry. I missed the first part of your sentence. What is prohibited in the new EU regulation?

Ms. Liia Hänni: Profiling.

Mr. Raul Rikk: Profiling persons.

Mr. Nathan Cullen: Profiling persons is prohibited in the EU regulation by governments. Sorry, just to be clear, has it been made illegal for governments to profile their citizens?

Mr. Raul Rikk: Yes. Basically, you cannot profile persons through the social media.

Mr. Nathan Cullen: It would be helpful for the committee if you have that regulation handy, because I don't. I don't know if other committee members follow EU Internet regulation guidelines, but if your government were able to provide that to us, that would be something I would be personally interested in.

Thank you, Mr. Chair.

The Chair: Thank you, gentlemen.

Next we have Ms. Vandenbeld and then Ms. Murray.

We are a little tight for time. We still have five minutes of committee business to deal with, so I have to cut things off at that point.

Go ahead, Ms. Vandenbeld.

Ms. Anita Vandenbeld: Liia, you mentioned that this is part of state-building in Estonia. This is something that goes back a few decades now, and from the very beginning it was imagined that you would get to where you are today.

If you have existing very sophisticated architectures that weren't conceived and built bit by bit in that direction, is it harder to take existing architectures and then apply this than it would be, for instance, to go into an emerging democracy and start from scratch? Are there are challenges that come with the fact that you already have government services and digitization in various departments that are already centralized? Looking at the fact that we're already very sophisticated, how difficult would it be to do what Estonia did?

● (1030)

Ms. Liia Hänni: Sometimes I think it was easier for us to build a system by seeing technology as a facilitator. In many democratic governments or democracies, governments are already working very well, so there is no pressure to change the state processes and to use new technology, but I think that because development will go on and the use of technology by citizens will go on, the government therefore also needs to understand that it is time to reconsider how government is operating.

It's hard, because you have this system that is working well, so why should you make another plan for government development? I think it is necessary, but it needs a lot of political energy, understanding, and strategizing to have some new goals in terms of how countries should meet this 21st century. This is actually very interesting work for the politicians of the world in terms of understanding these opportunities to pick a wide national consensus about the direction that the country would like to take. This is why I congratulate you. You have this opportunity now.

Mr. Raul Rikk: If I may add to that, the process is still going on. I've put up one slide that shows the main regulations in the EU. The same thing that has happened in Estonia is now happening in the EU states. The first directive, the EU data regulation, is all about electronic identity and providing digital trust services. The second directive is about how to manage incidents. The third one is about data protection.

Now the EU wants to take on the same logic at the EU level. In the last five to 10 years, the EU has made significant efforts to put forth and agree on these regulations and directives, so now this will be even bigger.

Ms. Anita Vandenbeld: In terms of compelling reasons, I think 2% of GDP saved is a very compelling reason.

I'll go back to the trust issue, because of course we're in a very different environment today than we were in the 1990s or the 2000s in terms of the level of trust that citizens have in digital data and also in government.

Ms. Hänni, could you talk about what the level of trust was in government when you embarked on this, as opposed to, for instance, the fear there is if you're sharing information between departments? I know we've had concerns in Canada that certain information is being shared with security services, or that we have health information or tax information being shared with other departments.

How do you protect against this? What would you see as the level of trust that citizens had in government generally and in the Internet and how it might be different today, and how would we overcome that?

Ms. Liia Hänni: How to build trust I think is your basic question.

It depends on the situation you have in your country. In Estonia, coming from this totalitarian system where Big Brother was watching us all the time, and our own government, it was such a different situation that we didn't even ask if we should be concerned that our own government would misuse our data. This problem of non-trust has been so strong in Estonia, as I understand it, but still people should know how a system works. With their having this concern, government should be able to explain what is behind this data exchange and how citizens' data is protected. There is lots of work there, and there is a rising need for that.

However, once again, paper documents are much more unsecure than digital information.

● (1035)

Ms. Anita Vandenbeld: I have one other quick question. It's about age. At what age do you start collecting the data? Is it at birth? Is it when people first get a driver's licence? At what age would the citizens themselves be able to access and have control over their data?

Ms. Liia Hänni: Actually, the first digital data will appear in our system when a baby is born. Already then, as I said, they're a digital citizen of Estonia with a personal identification code, with even a digital ID card, because it can be used for travelling. Parents, of course, are responsible for the data on their babies and can also access their babies' data—for example, medical data—but we have no time to speak about these medical records, the medical systems we have.

Yes, collection of data starts from birth, actually, but again government can collect data only when there is a legal power given to the government to ask for the data. This is very important to understand. It is not up to the different government agencies to ask for my data if they have no legal grounds for it. This kind of authorization of data usage by different agencies is based on law. When public servants want to go into the system, they need to have this authority—

The Chair: I'm sorry, Ms. Hänni, but we have one last question and we only have about two minutes left.

Sorry, Ms. Murray; we have approximately four minutes or less.

Ms. Joyce Murray (Vancouver Quadra, Lib.): Thank you very much. I just want to thank you for your country's leadership on digital government. I had the pleasure of spending time with Siim Sikkut, your CIO, in Wellington for the signing of the Digital 7. Estonia clearly is positioned as a leader in the international community, so congratulations.

I wanted to ask about watchdog functions. If someone has a complaint around a breach of privacy or perceived breach of privacy of data, is there a watchdog?

In our country we have a commissioner with respect to privacy. We also have a commissioner whose job it is to deal with complaints and do investigations. They have order-making power with respect to access to government information by citizens. I'm interested in Estonia's structure of compliance and oversight. Specifically, I'm very interested in whether the privacy oversight is combined with the access to information oversight, as it is in New Zealand and in many of the other leaders I spoke with in Wellington. We have separated those functions, and I'm interested in Estonia's approach.

The Chair: Thank you, Ms. Murray.

I'm sorry, Ms. Hänni and Mr. Rikk, but could we get a written response to Ms. Murray's question? Can you respond that way? We're out of time, unfortunately.

I want to thank you again for presenting to us in Canada. I appreciate your time and all the patience in working out our technical difficulties. It's much appreciated.

Thank you for your leadership on digital governance.

We're going to suspend and go in camera to deal with committee business.

[*Proceedings continue in camera*]

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

SPEAKER'S PERMISSION

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

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

PERMISSION DU PRÉSIDENT

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