House of Commons
Chambre des communes
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 097 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, March 27, 2018

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, March 27, 2018

● (0845)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): I call to order meeting number 97 of the Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3)(h)(vii), we are studying privacy of digital government services.

Today we have with us Jerry Fishenden, a technologist and government adviser, as an individual.

Go ahead, Mr. Angus.

Mr. Charlie Angus (Timmins—James Bay, NDP): I know we're later going to be discussing the witness list for the study of the growing Facebook scandal. I am concerned, and want to put it on the record for my colleagues to think about it. Right now in the United Kingdom, the question of whether the Facebook platform was used illegally to undermine the Brexit vote, and possibly change the Brexit vote, may have a direct Canadian link to Jeff Silvester and the work that AIQ did. It's my understanding that Mr. Silvester, because of jurisdictional limitations, is refusing to testify before the U.K. committee.

However, it would be well within the mandate of our committee to call Mr. Silvester to testify because of the power of the third party operators to misuse personal data and possibly undermine the Brexit leave vote. To that end, if we agree to bring him to testify, which we could by subpoena if necessary, we should make the U.K. committee aware of our work so that the U.K. committee, if it has questions about how the referendum was undermined by this misuse of the Facebook platform, could provide us with briefing notes as well, so that we could get this thing done.

We're talking about something that's much broader in terms of potential impact on the democratic process than we've looked at in the past. There would be an urgency to it, and I would certainly be looking to my colleagues to say it would be well worth our while to reach out to the U.K. committee at this time.

The Chair: Mr. Angus, are you making a motion to that effect, or are you just making the request to the chair that I look into it?

Mr. Charlie Angus: We can handle this a number of ways. I could do it as a motion now. We could do it in camera, but we have to apprise ourselves of the seriousness of this situation, because the United States is looking at it. The U.K. is looking at it, and two of the main players are Canadian. We should be taking account of the seriousness of this situation and making it clear that we will address it.

I know there are a number of witnesses we are going to talk about and I don't want to take time out from the witness that we have, but in the case of Mr. Silvester, we should say he is definitely someone who's going to be appearing before our committee.

The Chair: Would you like to open up the discussion now, or would you like to talk about it?

Mr. Charlie Angus: I'll turn it over to Mr. Erskine-Smith and see what he thinks.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): I'm certainly open to this conversation, but we should have a conversation later after our witness has presented. Obviously the analysts prepared a briefing note, and this was not in the briefing note.

I listened with interest to Chris Wylie's testimony at the U.K. committee this morning, so I am open to all potential witnesses and the conversation to that end. We're going to deal with this, as I understood it, after we hear from this witness, and we're going to be dealing with this as we ordinarily do, dealing with potential witnesses after our committee business. Let's have this discussion at that time.

The Chair: I watched the testimony this morning with interest as well, so we'll do that following this testimony.

Go ahead, Mr. Fishenden.

Dr. Jerry Fishenden (Technologist and Government Advisor, As an Individual): Good morning. Thank you for the opportunity to provide evidence. I'm doing so in a personal capacity, as you've mentioned.

Consumer and citizen trust is essential if governments and businesses alike are to use technology to the benefit of us all, yet all too often we are seeing personal data being taken and misused. It's either by intent or as a consequence of poor security and privacy. Topically, the Facebook and Cambridge Analytica revelations are obviously highly pertinent to that.

We need to improve the general level of understanding about data and computing. Equally clear, there is a need to increase the understanding of the important difference between public or open data and private or personal data, which citizens wish to see better protected. In particular, we need to ensure that sensitive data, which covers everyone from vulnerable children to undercover law enforcement, is much better protected.

Much government data quality is often poor, since many people only deal with central government occasionally. It's also duplicated in many places. Government generally lacks well-developed data architectures. There's a need to map and better understand the use of data and stop believing that data sharing is a way to fix poor design.

In computing, we already have better approaches that can be used, such as zero knowledge proof, use of interfaces, encryption, authentication and authorization, and attribute or claim confirmation. Zero knowledge proof, for example, enables one party to prove to another party that a given statement is true without conveying any information apart from the fact that the statement is indeed true—for example, that I am over 21 or that I'm entitled to a particular welfare benefit.

Such computational techniques need to be embedded in the way we design systems. If they're not, the more the paper age data-sharing legacy persists in an age where computer systems operate on a scale and at a pace previously unknown, the quicker security, privacy, and trust will be degraded and fraud increased. The human and financial suffering data misuse causes is only likely to increase unless governments adopt stronger legal and technical means of protection.

One country in particular that the U.K. has looked to and learned from is Estonia. They have a good set of principles, particularly in terms of putting the citizen at the centre and organizing around them, even to the extent that citizens can see which officials have had access to their data. Transparency is I think essential to help build and maintain public trust.

In 2011 Francis Maude, MP, the then Minister for the Cabinet Office in the U.K., established the Privacy and Consumer Advisory Group. It comprised academics, privacy and security advocates, and representatives of consumer groups. Its remit was to ensure that government programs address citizen privacy, trust, and confidence, from initial policy planning to requirement specifications and through to delivery.

The group worked very well when it had the direct backing of a strong minister like Francis Maude, but after his departure some officials no longer responded to or attended the group. My recommendation would be to establish a similar expert group but have it report directly to Parliament, perhaps via a committee such as yours, so that it cannot be marginalized or ignored.

The Government Digital Service—GDS—technology code of practice is important. They set out criteria to help government design, build, and buy better technology, and it emphasizes privacy in particular, including explicitly that citizens should have access to and control over their personal data. The code still has a principle that privacy should be integral.

The prevention of cyber-attacks and the protection of data is a constant challenge, from external attacks to insider abuse, whether that's an official inappropriately accessing or using data or indeed a developer putting in place rogue code that can later be exploited. The U.K. has expert help and guidance in this regard from the National Cyber Security Centre, which is part of GCHQ.

I do have, however, a concern about inadequate privacy by design and security engineering.

● (0850)

Many government departments and agencies have set up their own bespoke development programs using web developers, many of whom are not trained or experienced in writing secure code. The requirement of minimal standards for software engineering quality should be considered, such as the ISO standards, the application of the Consortium for IT Software Quality, and specialist advice such as that available from the NCSC.

At the infrastructure level, there is better practice around the protection of data, both in motion and at rest. There are also strong access controls and auditing, including protective monitoring of the most sensitive systems.

A lack of understanding of technology, both the good and the bad, at the most senior levels can create gaps in policy and between intent, outcome, and legislation. Sometimes existing legislation can be a blocker to effective improvements in services and their outcomes. It's important to have a process for highlighting where legislation needs to be simplified or updated.

There can be a naive tendency amongst some politicians and officials to assume that technology can somehow magically solve complex policy or socio-economic problems. I wish that were true. The idea that technology can be a solution for everything does need to be challenged. It must never be about websites and online services, but how better digital infrastructure helps those who need face-to-face services too, and those who don't have access to modern technology.

Government can lead by example in the secure, consent-based use of data and the establishment of principles to be applied to the ethical use of data and software that acquires, processes, and utilizes it.

One of the key issues on which government should be playing a leading role is user consent: engaging and educating users to ensure their consensual participation and understanding, including of the data they are revealing, what's being done with that data, and how they can provide or indeed revoke consent.

Another key role is in the legal aspects, by ensuring legislation is adequate or by identifying work that needs to be updated to keep pace with changing technology.

Government can also play a role on the economic issues, meaning understanding the impact that better use of data and techniques such as artificial intelligence and machine learning are likely to have, both at microeconomic and macroeconomic levels, including on the potential future configuration of public services as the Internet of things and embedded health sensors become more ubiquitous.

Then there are the access and control issues of establishing a trust framework, one that spans anonymization, pseudonymization, and strong identity proofing.

I've already mentioned data quality. It's to ensure data is of sufficient accuracy and veracity to ensure that resulting decisions are coherent, particularly before building analytics and machine learning on top of unknown data quality. Users need to be provided with access to their own data to ensure their records are accurate.

Data de-identification and anonymity are known problems that already exist with anonymizing personal data successfully. This is becoming an increasingly significant and complex issue. De-identification is not the same as anonymization, and more research is needed in this area.

On data access, we need to ensure that appropriate control mechanisms for public, private, or personal data accessed by systems are in place. This includes appropriate protections ranging across security, privacy, audit, accountability, and protective monitoring.

On data veracity and integrity, how do we know that data being used by such systems can be trusted? How do we know all data have been released from the systems when we attempt to regulate or ensure they're compliant with laws of non-discrimination?

Concerning code jurisdiction, code and data are increasingly operating in the cloud or serverless environment in systems scattered across the planet. There is a need to clarify how they meet the standards required—for example, not exhibiting biased, illegal, or discriminatory behaviour or being compromised by hostile actors.

Finally, on resilience, as many services become ever more reliant upon the new generation of interconnected systems, the potential resilience to failure, whether that's caused by accidental or malicious purposes, is a significant issue. More research is required into the potential interactions, vulnerabilities, and risks of the emergent systems of systems.

If the best legal, ethical, and trust frameworks are not in place, the poorly designed acquisition and use of personal data will be discriminatory, wrong or inaccurate, biased, unaccountable, manipulative, and they will create significant security, privacy, legal, and trust issues.

● (0855)

However, if well applied, there is certainly an upside, which is that they can help support better policy-making, health care, education, and transport, for example, through responsive and more efficient systems.

Consistent standards of security, privacy, and software engineering, together with transparency, are required. To be successful, any digital or e-government initiative first needs to determine what it wants to achieve by going digital. Is it simply to automate existing services, or is it optimization, re-engineering, or transformation? Is it about moving resources towards the front line by taking cost out of internal operations by helping to streamline and simplify them? There needs to be clarity about exactly what the design outcomes and benefits are, rather than a simple assumption that this is something we need to do in the digital age.

I think that government can play a significant and positive role in showing how we can enjoy the upside of our digital age, rather than the downside. Rather than simply following the model of the worst of the private sector, misusing and abusing data without users' meaningful consent, government should look to raise standards. There is a chance to lead by example.

I would be happy to provide more detailed links and references after today's session if that would be useful. Thank you for taking the time to listen to me this morning.

● (0900)

The Chair: Thanks once again, Mr. Fishenden.

We'll go first of all to Mr. Nathaniel Erskine-Smith. You have seven minutes.

Mr. Nathaniel Erskine-Smith: Thanks very much.

With this study, we're looking at how digital government can improve services for Canadians while also protecting their privacy and security. Do you have an ideal case, an example that we could specifically point to and say, “Here's an initiative that has done just that”?

Dr. Jerry Fishenden: I think there have been several initiatives in which privacy has been very much at the core of the program. I think some of the programs have struggled. One of the particular ones that comes to mind is the GOV.UK Verify program, which looks at identity. It's based on a very sound set of privacy principles, and it was designed from the ground up to ensure adherence to those and to take account of upcoming legislation, such as the European Union's General Data Protection Regulation. However, I think that for other reasons, this program has struggled to deliver the outcome it once set out to achieve.

Other areas that I've been involved with include some of the police national systems, where the thing is generally very well designed in terms of data protection of the citizens involved and has protective monitoring. Unfortunately, there have been one or two cases that have proved the value of the protective monitoring in terms of officers being belatedly identified as having abused the trust with access to those systems. I think we need to look at ways to have more proactive monitoring on systems so that if there is potential abuse by an insider such as in those cases, or indeed by a hostile player from outside, we're much more timely in the way we respond to those incidents.

Mr. Nathaniel Erskine-Smith: In terms of ideal cases, though.... I mean, in your comments, you indicated that the U.K. looked to Estonia. We had Estonian officials before us last week, and they spoke very highly of their system. It has improved services. They've reduced costs—2% of GDP. There has been no identity theft with regard to their digital ID. Is that, in your view, if you look internationally, the model?

Dr. Jerry Fishenden: I have a lot of respect for the Estonian approach, and I've spent time with their officials and politicians as well.

I think one of the things, to be frank, that we struggled with in the U.K. is that theirs obviously relies on quite a different approach to identity than the one the U.K. has adopted. That forms the core of the system. To be frank, we are still struggling in the U.K. with adopting a reliable and consistent identity framework that would enable citizens not only to easily prove who they are when they're online, but also to prove that a particular dataset belongs to them, which is a much more complex issue. Even if I've proved who I am to a third party, when I turn up at the front door of the National Health Service or the welfare office and try to claim access to a particular record, there's still a need to associate my identity with the particular data held in different data silos across government, and that's proving also to be quite a complex challenge.

Mr. Nathaniel Erskine-Smith: That's an interesting point, because when the Estonian officials were before us last week, my colleague Mr. Baylis asked them to walk us through the building blocks, the starting point of where we should begin. They said that the starting point has to be the digital ID. They noted that their digital ID is itself an encryption device, which is why they haven't had the identity theft issues that we've had here without having digital ID.

You've criticized the U.K.'s digital assurance program to date. Is what Estonia did...? The question, fundamentally, is this: why not do exactly what Estonia did?

Dr. Jerry Fishenden: That's a good question, and it spills over into the realm of politics. The current identity assurance program, Verify, was created after the incoming government of 2010 abolished the U.K. ID cards program, which had been a political commitment by the coalition government, the Liberal Democrat-Conservative government. They were very keen to find a method of achieving a similar outcome, but one that did not mandate that every U.K. citizen needed to go and register their biometrics on a national identity register. This was an attempt to find a middle ground.

I think, partly, there's also been a change in that we have an initiative such as open banking, which started recently in the U.K., under which you can go online and prove who you are using your bank as the backstop in terms of confirming your online identity and then confirming through a third party that you are who you say you are. I think there's currently a desire to have a look at what the government originally wanted to achieve, which was effectively a marketplace of trusted identity providers working within a framework that government trusted and ultimately could regulate if necessary, and whether that can now be achieved by changes that are happening in the marketplace anyway.

The one missing thing, to me, is still this link between a proven identity and the various silos of data that relate or belong to me sitting in the different government departments. There needs to be more discussion about the process that's going to bind my identity to those different multiple datasets in a way that people can—

● (0905)

Mr. Nathaniel Erskine-Smith: To that end, you mentioned that politics sort of got in the way, to some degree. Assuming we remove politics from the equation, then would the best policy answer be to adopt what Estonia did with the digital ID in their encryption device, or would you say there are ways to improve upon the Estonian experience?

Dr. Jerry Fishenden: I think if you're starting out, you could follow a track very similar to the Estonia approach. Most people now carry mobile phones or mobile devices around with them. I'm thinking of a principle of using those mobile devices as the core means of proving identity. I use that approach with a lot of my online commercial services. I have two-factor authentication or two-factor verification set up so that when I try to log in online, I get either a time-based code I can read from my phone or a text message is sent to me, which is obviously less secure. I think government could take advantage of the technology enhancements that have happened since the Estonians developed their model to come up with a solution oriented around mobile devices that's probably more amenable to trust.

I think the issue in the U.K. was partly the fact that the Home Office was seen as the arbiter at the national identity register and the feeling that people were going to have to store all of their biometrics and personal data with one single government department. I think that now there would be more effective ways of linking one proven identity to the different data silos or lockers so that I could prove who I was to the NHS, the National Health Service, and prove the link to my health records without necessarily exposing that linkage to perhaps the taxation department or the welfare department, if it were not appropriate for me to do so or there was not a regulatory reason that I needed to do so.

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

Next up is Mr. Gourde.

[*Translation*]

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

I'd like to get back to the numerical data concerning Canadian citizens, and perhaps to data pertaining to citizens of other countries as well, which are sent to various departments, where people work in isolation.

In my 12 years as an MP, I have come to realize that when they come to me for help, some of my fellow citizens' problems are due to the fact that there is erroneous data, and it differs from one department to the next. This causes problems for them. We then have to do a search with them to help them reestablish the accuracy of information. For instance, it's often an address that differs from one department to another, quite simply. This means that citizens lose rights or services, among other things.

In order to get around the issue of work done in isolation, could we not create a personal digital file for every individual? Everyone would have the right to his or her file, which would belong to them, and they could correct it themselves so that the data would be real, accurate and in real time? It could be the individual's responsibility to see to it that his file is always up to date.

[*English*]

Dr. Jerry Fishenden: You paint a picture I recognize. It sounds very similar to the United Kingdom model, with data held in multiple places, often with conflicting information.

I'm very much a believer in the citizen having access to their data and control over it precisely for that reason. I think the citizen is the ultimate arbiter of their own data, subject to some validation, obviously, where necessary, by the government. Maintaining their own records would be a good way to do it, as we do with commercial organizations when we log in and update our credit card details or our address records.

Some of the U.K. has started to do that. We now have a single tax portal. When I log in, it not only shows me my current tax position but also my state pension position, even though that data is coming from a separate department. It enables me to see in one place data that spans more than one government silo.

I don't think necessarily that enabling citizens to access and maintain their own records means you have to pull all the data into a single database. The fear is always that if it's all in one place, a potential compromise will mean that all of that citizen's data is compromised at the same time. I think there can be good justification for silos if that is done as a design intent and if the user, the citizen, can still maintain their data through a single online service, even if the data that's updated then goes back into perhaps....

I'm thinking about areas like health, where citizens are particularly sensitive about their records potentially being made available to others. I think that in some sense, just having a silo by design around health records can be a good thing, but enabling the citizen to still update the common aspects of that record, such as addresses, across multiple government agencies could still be achieved through a single portal.

To me, it comes back to the identity issue, which really does need to be cracked first. You need to know which citizen it is and then to establish that they really are the citizen who owns those different data records. Then I agree entirely that the citizen is well placed to look at the data and to either directly make amendments and corrections or to request the appropriate corrections and amendments by the owning department.

● (0910)

[*Translation*]

Mr. Jacques Gourde: A central file would no doubt allow citizens to be informed of the fact that this or that department or organization is using their data, if they were asked for that authorization in order to provide services. For instance, the Canada Revenue Agency could ask for the authorization to access a person's central digital file to solve a problem. Currently, Canadian citizens do not know which departments consult their existing digital data.

I believe that this data belongs to individuals and that they should be aware of the fact that an organization is doing research on them.

Do you think it would be legitimate that the individuals in question ask to be kept abreast of the fact that a department is examining their digital data?

[*English*]

Dr. Jerry Fishenden: Yes, I think the principle is very sound. Obviously there are occasions when the state needs make investigations in the background to which it would not be appropriate to alert the citizen, such as cases of fraud or crime, but as a general principle I think it's right.

That's partly why I like the Estonian system. Estonian citizens can see which departments and officials have been accessing their records, and if they feel that wasn't appropriate, they can request an explanation as to why their records have been accessed by either a particular official or by a government department. I certainly believe that would be a very good way to go.

[*Translation*]

Mr. Jacques Gourde: On the health front, that's really very interesting.

When you go to the hospital, there is a file about you on site. That file is shared, or it is not. If you change physicians during your life, it unfortunately happens that files are not transmitted in their entirety, or that the information they contain is not sufficient.

Digital health data should be compiled in a file that would follow us all our lives. It would be more practical and safer for people. What do you think?

● (0915)

[*English*]

Dr. Jerry Fishenden: It would ideal if we had a composite health record.

I'm also very conscious, with the growing use of wearable devices, that our health information now spans far wider than it did in the past. For example, I'm wearing a device that measures my heart rate periodically, and my exercising. It would be good if it could all be consolidated into a single place, so that when I go to see my doctor, they're aware not only of the health service interventions in my life but also of my lifestyle.

Again, I think it's making the citizen the custodian, or at least having the citizen have access and control so they can decide what they want to share among different officials. I would happily share any medical data from my wearable devices with my doctor. When I go to see them, they can either validate whether I'm telling the truth about how much I exercise or at least get insight into some of my lifestyle that would enable them to provide better health care to me.

I think it's an important point that's sometimes missed, particularly with the system we have in the U.K. at the moment, that more and more health data is no longer held exclusively within the health care system. As consumers and citizens, we're going to be generating quite a lot of useful medical information that also needs to come into those records.

I'm basically agreeing that it would be nice if there were a very highly trusted place where we could store both the medical service data and our own personal health acquired data, so that there would be a single health data repository that would enable medical professionals to give us the best possible care.

The Chair: Thank you.

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

Mr. Charlie Angus: Thank you. This has been a fascinating discussion.

One thing I've learned in my many years in Parliament is that I've become very mistrustful of government saying they're going to come up with a great new app that's going to make everything easy and cheap, because whenever it comes to the issue of privacy, it doesn't seem to be within the operating culture.

For example, this past week I learned that the government had 250,000 breaches of private information of citizens, including their tax records, health records—all manner of other records. That was down from 2013, when there were a million breaches of personal information, which included 583,000 records of financial information on student loans.

Through each of these cases, year in and year out, the reporting rate of government officials to the Privacy Commissioner.... In Canada, if there's a major breach of privacy, you're to report it to the Privacy Commissioner, who then investigates to determine if there's been a threat to personal data. The government rate of reporting is 4% in these breaches. That suggests that when it comes to deciding the priority, it's always to protect the rear end of the minister and try to keep it out of the public eye, rather than the primacy of privacy.

From your experience with the U.K., how do we ensure that we have a government that puts privacy above sometimes protecting departments and protecting mistakes? These breaches happen year in and year out, and they're very serious.

Dr. Jerry Fishenden: That's a good question.

I think part of it comes back to my concern around the issue of privacy engineering and security engineering. There could be an extent to which breaches at the technical level could be automatically reported and made visible without any human interpretation or obfuscation in the process. I'm trying to find polite ways of putting it.

Equally, I think we need to be wary of the idea that technology alone can provide the answer. I think it could certainly help. It could certainly enable us as citizens to see where, as in Estonia, records have perhaps been inappropriately accessed. It could also identify where that might be happening at scale. For example, if somebody, either an insider or an external agent, has tried to farm multiple records in rapid time, that type of thing should be caught quite quickly by a good computer system.

However, it seems that most of the breaches that come to light in the U.K. often involve insiders who have executed social engineering attacks. Even though the system has been well designed, if they bring up people's records on a screen and use analog attack methods, such as either writing down the details or taking a photograph of the screen, it's very difficult for the system alone to catch those types of things. You can spot patterns of behaviour over time, but if an official only does it as a one-off, it's going to be very hard to know.

I think there's also a disincentive in the system currently, in that the more honest the departments are, the worse they look on the leaked tables. They're seen as the departments with the biggest problem, whereas they may be the departments actually being the most honest with us.

● (0920)

Mr. Charlie Angus: I guess that's what my concern is. We can create the most perfect technological system that will always get rave reviews, but it depends on the human factor. The human factor in politics is always defined by politics and political pressure. In our country, certainly the tax department has multiple breaches year in and year out, with lost hard drives and USB sticks. Maybe, as we move more toward the cloud, we won't lose as many USB sticks full of financial information.

We have had cases of people inappropriately accessing their ex or their spouse. Those things will happen in departments, I guess, but how do we build a culture of accountability within government to ensure that the privacy of individual information is first and foremost? Without that trust, citizens have no reason to believe that this great new app that we're going to create is going to protect them.

Dr. Jerry Fishenden: I agree. I think there are probably multiple solutions here. One is improving the quality of the training and awareness available to officials. The second is improving the design of some of the systems. For example, why do so many screens, when officials access them, reveal in plain text everything about an individual? If they need to know whether somebody's in receipt of a particular benefit or over a certain age, why reveal the person's date of birth or the particular benefits they're receiving? You could just have a confirmation flag showing on the screen, which would prevent an amount of data from being leaked.

Ultimately I guess you need stronger sanctions, such that when these things happen, people are held to account. It sounds as though you have a situation in Canada that's similar to ours in the U.K. Very, very rarely does anyone personally or individually seem to be held to account.

Worse sometimes, in my opinion, is that we see organizations fined that are part of the public sector. Let's say a health trust has had a breach; they may have a fine of several million pounds imposed on them for the breach. That seems to me like a double punishment to the innocent, because that fine will directly impact the rest of us, the people relying on medical services from that trust. It also ultimately avoids the issue of finding out who was accountable for that breach. It's as if a mysterious faceless entity was responsible.

Also, at the senior level here, we rarely have the right accountability, at the senior board or executive team level, of somebody who owns it, so that you can say, “It stops with them. They are accountable for that.” Maybe if we had greater clarity that a particular named official would be held to account and we could move away in the U.K. from the culture of fining rather than looking to see who was responsible for ensuring all of those aspects we're talking about—making sure the culture of the organization is right and the systems are well designed—people would be held to account when things went wrong and would fix them.

Ultimately, if they haven't managed to fix all those things over an agreed period, then they should be held accountable.

Mr. Charlie Angus: Thank you very much.

The Chair: Thank you, Mr. Angus.

Mr. Baylis, you have seven minutes.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Good morning —or I guess for you, Mr. Fishenden, it's good afternoon.

One of the important points you made is that the core of the system is the identity framework. Estonia has an 11-digit number. You also mentioned that in the United Kingdom, you looked at an ID card program in 2010. I got the impression from what you said that it didn't work.

Can you explain what the ID card program was and why it didn't work, or what happened to it?

Dr. Jerry Fishenden: Just to clarify, the ID card program was terminated in 2010 with a new incoming government. It started in around 2005 or 2006.

It was effectively in two parts. One was a national identity registry, which was going to contain 140-something pieces of personal information, both biographics and biometrics. The idea was that citizens would have to enrol by providing their fingerprints, iris scans, and photos and things.

The card was going to be the physical manifestation of that register. Effectively, U.K. citizens would carry it around, and if they were challenged, the card could be checked. It could also talk to the central register and, if need be, bring back fingerprints and things, which would enable a law enforcement officer or whomever appropriate to validate that the individual in front of them was the same person who'd originally had the card issued to them.

● (0925)

Mr. Frank Baylis: If that had not been terminated, it could have been the core identity for moving toward a digital economy. Why was it terminated?

Dr. Jerry Fishenden: There were a variety of reasons. Some of them were around civil liberties. It was seen as a single database register of every single U.K. citizen, which is alien to U.K. culture, apart from during the Second World War when people had identity cards, which finished sometime soon after the war.

There were also technical issues with the design, partly reflected in the recent discussion about whether you build one big database into which you'd put all this quite sensitive data and then run the risk of it being breached. That would cause a bigger problem.

Mr. Frank Baylis: That approach is somewhat different from, say, the Estonian approach, where they said they would give you an 11-digit number. That number, through what they call this “exit data”, can go and fish out this piece of information from this database, or it can go over there and fish it out, but it's not all tied to it. The people who have one pocket of data over there can't themselves go and look in other parts of the government to get that data. You're saying one approach that got people nervous was this one card, and putting everything onto it together. That approach actually made civil liberties people very uneasy. I could understand that. Is that right?

Dr. Jerry Fishenden: Yes, exactly. It made the fundamental error of assuming that having a single identity number for everything would be a good thing in a highly computerized age, whereas the Estonian model, which is based around a unique ID but keeps your data segmented, if you like, logically where it makes sense to do so on the state's behalf—so maybe health, taxation, welfare, education and other pockets—means that citizens still feel that they're in control of their identity rather than the state being in control.

Mr. Frank Baylis: We have in Canada something called a SIN number, a social insurance number, which is a nine-digit unique identifier. Every citizen has one, but it is primarily used for Revenue Canada, our taxation net. Is there such a number that exists in the United Kingdom that every citizen has?

Dr. Jerry Fishenden: We have multiple numbers. We have a national insurance number, which is issued by the Department for Work and Pensions, which is used by them primarily. We have unique tax reference numbers used by the taxation department, Her Majesty's Revenue and Customs. We have NHS, National Health Service numbers, and most other departments do have their own unique identifiers for people.

Going back to my original comment, that needn't necessarily be a problem, because there is no reason you couldn't have a number, as in Estonia, that potentially is a super-set of those to enable me to prove who I am to each of those different indexing systems, if you like, but without necessarily their being able to see across my proper identity file.

Mr. Frank Baylis: Yes, to your point, we also each have our own medical identity number. The challenge we have is that this is provincial. It's a different jurisdiction, but on the federal level—and we are the federal government talking to you right now—we have that SIN number, which is nine digits. Are any of these, the national insurance, the unique tax reference...? I'm asking a technical question about how big are those numbers. Are they alphanumerics? They're all unique identifiers. Is that fair to say?

Dr. Jerry Fishenden: Yes, most of them are an alphanumeric mix. The NHS number might be purely numeric, but the others are an alphanumeric mix. I'm trying to think. My national insurance number is 10 digits altogether. It's a grouping of five two-digit—

Mr. Frank Baylis: You also mentioned that some people conceivably think of using bank confirmation. Basically the bank confirmation is just your bank account number.

I want to get your viewpoint on this from the U.K. You need a unique identifier. You need to choose some number or alphanumeric mix. That's going to be linked to it. The approach the U.K. took, which seemed too intrusive, is that everything was in one database and on that one number, and people said that it was starting to sound like an attack on their civil liberties. This was opposed to saying, in the Estonian way, “This is your number. This number can link you into any department and give you access to any data of that department, but those departments can't use that number to access your data, to go through the system.” It is unique to you, and there is a very strong concept that you own the data and you control it and you see when your data is used.

Would that have helped? I know you've had frustrations in the U. K., so maybe you can expand on that. Would that have helped? Would that be the right way to go if we're looking at doing something in Canada?

● (0930)

Dr. Jerry Fishenden: Yes, I think that approach would potentially work in a way the U.K. one didn't. I think it also tackles the other issue of how to find the data about me in different silos and link it back to an identity. You issue the identity. I could turn up somewhere and prove who I am, using a passport or maybe facial recognition and things, but that still doesn't prove I own my national insurance record or my health record.

The ideal way to do this would be that the next time I see my doctor or a consultant, I can prove who I am to them and then have that linked back to that proven identity. Within a short space of time, I could have both my controlled identity, if you like, and by my actions and trusted relationship with the people who issue the other numbers, I could prove that I am the person to whom those other pieces of data relate.

We end up in a place where we need to be if we're going to enable better citizen access and control over their own data, which is both the trusted identity and the linkage between that identity and these potentially sensitive data records.

The Chair: Thank you, Mr. Baylis.

Next up, for five minutes, is Mr. Aboultaif. Welcome.

Mr. Ziad Aboultaif (Edmonton Manning, CPC): Thank you.

Good afternoon.

Estonia has been mentioned in many places. None of the G20 or G7 countries, supposedly, have a system or an example that we can look at. My understanding is that the witness from Estonia appeared before committee here and mentioned that in their experience they've never had an example of a breach.

Is it reasonable, in your opinion, to believe that they've never had a breach? Otherwise, they could have been hacked and they didn't know it. Can you comment on that?

Dr. Jerry Fishenden: That's a very difficult question. It's the nature of computer security and systems that you only discover years later you were breached.

Based on the calibre of the people I've met and what I know of their system, they have as good a series of protections as you could possibly have on any computer system to protect what they're doing. As to whether it could turn out at some point that there's been some malicious piece of code or some compromise running somewhere in there, it's almost impossible to say.

I think they're very savvy, very aware in monitoring their own environments and looking for patterns of strange behaviour that lie outside the norms. This is a pattern we're beginning to see elsewhere, with both the online banks and insurance companies in the U.K., but also with our taxation departments.

Even when I'm logged in to my tax account, despite the fact they've accepted proof of who I am by my logging in, they are running behavioural analytics in the background to see how I behave when I'm on their website. For 15 years I've been logging in and using my tax account. They probably have a pattern of behaviour they expect to see from me. If they see something different going on, that can automatically raise flags that perhaps somebody has hacked into my account, and they can close down access.

Mr. Ziad Aboultaif: The most successful example right now is Estonia. How long have they been using this system? Do you have any idea?

● (0935)

Dr. Jerry Fishenden: They first started building it back in the early 2000s, I think. I'm not sure when it reached maturity. I believe they have continued to enhance it. They added some of the secure SIMs in the mobile phones more recently, so it has been an evolving program.

You're probably best to direct this back to them for specific facts.

Mr. Ziad Aboultaif: The risk that any government can take in trying to implement something like this is to do a complete revolution in the way things are done. Then to try to embed everything in one area is heaven for hackers, in a way, who can get all the information they need from one place. The moment they break into the system, everything is beyond cost or beyond any economic measure that you can ever put there.

From your information—I read your opening statement, and I listened to it—are there any concrete examples to indicate that the proposed system is superior to what we or other countries use at the moment? Is there any evidence that going that route is better, rather than staying with the current system?

Dr. Jerry Fishenden: I take your point about everything being in one place. Everything keeps coming back almost to Facebook and Cambridge Analytica at the moment, because it's a great example of what happens when somebody gets access to all of your data in one place, impacting not only you but potentially your whole circle of acquaintances as well.

When I look at the Estonia model, I think you could take what they've done together with what your colleague was talking about, which is looking at how you put citizens in control of a particular method of proving identity and then enabling them to link back to their other pockets of services and data so they become the trusted pivot point. A lot of this is about trust and about citizens trusting not only the intent of government but also the technology. I do worry that the more they see what some in the private sector are doing with technology, the more they will worry about government's intent in using data.

The other thing is the government's appetite for risk. If we look at how things are currently done in the paper world or have been done in the paper world, and the level of risk and the risk mitigation that was done there, we might then ask if we are sometimes expecting too much of technology, or overloading it, because we think it can do a better job.

In the past, whenever I signed the document for the tax office, it always amused me that they obviously never asked me for a copy of my signature when I first started doing tax, so quite what my signing a document proved to them I don't know. However, when we moved to the digital domain, suddenly people talked about digital signatures or electronic signatures. That may be appropriate depending on the financial risk or exposure of a government department, but there may be many services for which the appropriate risk model would be to say that we understand the risks and we have appropriate mechanisms for dealing with them that don't require the very highest level of citizen identity to be used.

The Chair: Thank you.

Thank you, Ziad.

Next up is Ms. Fortier. You have five minutes.

[*Translation*]

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

Good morning. I thank you for being here today.

You had already begun to address the topic of cyber attacks. I would like to know if the British model currently prevents cyber attacks? Does it deal with specific security issues you could share?

[*English*]

Dr. Jerry Fishenden: Thank you.

It's difficult to know how much I can say on the cyber-attacks. Government departments are under constant attack by automated bots and agents all the time. We've also had distributed denial of service attacks. We're constantly looking at ways to engineer our way around those.

We are fortunate that we have GCHQ and the National Cyber Security Centre, which are very capable in anticipating and warning against attacks as well as advising not only government but also business in the U.K. of potential mitigation. Also, if there is a cyber-attack or if something is compromised, they are very capable in advising on how to quickly recover from it so that it doesn't cause any lasting damage.

I'm finding it difficult to be specific. I suspect you might need a closed session with a representative from the National Cyber Security Centre in the U.K. I do know more; I'm just conscious, particularly in a personal capacity, of what is appropriate for me to share.

● (0940)

[*Translation*]

Mrs. Mona Fortier: I understand, and I respect that. It was important to point it out. This concerns us at this time because it is a part of the analyses we are doing in view of transforming the system.

We are faced with the fact that the advent of digital government services is inevitable. Canadian men and women increasingly want digital services—if we understand the will to deal with the various governments properly. As we mentioned earlier, there are three levels of government the citizens may address, and they are the federal level, the provincial and territorial level and the municipal one. We have to take that complexity into account.

You have already shared various ideas with us, but one of the questions I want to ask you concerns the advice you could provide to the Government of Canada in its efforts to digitize its services. Do you have any other advice to give us this morning?

[*English*]

Dr. Jerry Fishenden: Thank you.

I think that goes back to the first question of my opening statement: what are you trying to achieve by going digital? Is it purely moving more services online and effectively still operating in a forms world, where it's not paper forms anymore but forms on a computer screen, or is it about looking at how the operating model of government itself can be improved to enable services to be redesigned, really?

If we have better data in government, why do we ask citizens to constantly tell us something that government already knows, such as where we live, how much we're earning, how many children we have, and whether we're married? Why don't we move much more to data-driven services and push services to people, rather than asking people to fill in forms all the time?

I'm aware that the focus seems to have gone at my end....

[*Translation*]

Mrs. Mona Fortier: Over the next 20 or 30 years, digitization will be inevitable. We're talking about a transformation. We have to be able to provide services to Canadians more quickly and in a secure manner. We have studied models that exist in Europe, such as in Estonia, as well as in Australia.

What would be the most important piece of advice you could give us, since we really have to undertake this transformation?

[*English*]

Dr. Jerry Fishenden: I think that in an ideal world I would take the time to step back and ask, “How do we want our public services to be working and engaging with citizens in the next five to 10 years?” I would be just taking the time to look at everything that's going on.

I've mentioned that people are going to be wearing more monitoring devices in health and that the Internet of things is going to be in people's homes more and constantly interacting with them. There's going to be a whole series of changes coming. I worry that government will always be behind the curve. If today it's still thinking about moving things onto websites just as the rest of the world is moving to the Internet of things and devices, the whole world will have moved on again just as government manages to catch up with the web.

I think there's an opportunity to look back. We have a very similar problem in the U.K. between central government and local government, and we have multiple tiers of administration. There is an enormous opportunity to take a lot of the complexity out of the internal operations across both local and central government and to potentially put more resources back into front-line services.

My worry is that we talk too much about online services, rather than thinking about digital in terms of how government itself reorganizes and restructures its own operations to remove a lot of the complexity in process, function, and administration in order to simplify and streamline front-line services, whether they're delivered face to face or through a gadget of some kind. By making better use of technology within government itself, potentially there's an upside of enabling more resources to go towards the front-line services that maybe can't be automated.

● (0945)

The Chair: Thanks, Mr. Fishenden.

I'm going to ask the committee for a bit of indulgence. We're at our time right now, at 9:45, but there are still two people left to ask questions, and it's a great conversation. We did have some earlier time taken up with a motion or discussion. Is it okay if we go another 10 minutes and finish up the questions?

Mr. Nathaniel Erskine-Smith: For at least another round.

The Chair: Mr. Fishenden, are you able to stay for another 10 minutes?

Dr. Jerry Fishenden: Yes, of course.

The Chair: We'll proceed with Monsieur Picard.

Yes, Mr. Angus?

Mr. Charlie Angus: Well, I'm open to this, but I want to know that we're going to get to the witness list and net neutrality, because we have to come out today with a decision for the witness list.

The Chair: Yes, we will.

Go ahead, Monsieur Picard, for five minutes.

[*Translation*]

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

Good morning. My first question is very general and concerns transparency.

It seems that all of those who want modern procedures or a modern administration talk about the importance of government transparency. It is a “cliché” that no one defines specifically. If for reasons of transparency I obtain financial information from the Department of Finance, I could influence the market in an inappropriate way. Access to security information could facilitate terrorist acts.

In the search for greater transparency in a digital government, what is your understanding of what a transparent government should look like?

[*English*]

Dr. Jerry Fishenden: Thank you.

I think there are possibly several layers to that. One is the Estonian type of approach that we have mentioned, whereby citizens can at least see who has had access to or made use of their data. Then there is a bigger question about how much appetite government has to reveal much more financial data about its internal operations. You mentioned the possible threat that if it does so, people might try to effectively game the system and manipulate the market. On the other hand, it might enable us to get better insight into where the public sector is doing a very good job and where other parts of the public sector could follow a particular organization's model because it's been very financially efficient in the way it operates. It might also enable us to see where other parts of the public sector are not functioning so well and could work together to help improve those areas.

Also, in the computer age, there is a potential level of transparency about algorithms and processes. For example, regarding welfare calculations, does government keep those processes entirely within itself, or does it enable third parties to potentially run my financial affairs against a welfare calculation system? There could be big benefits to citizens if they could share their financial details with a financial adviser. If a financial adviser could model my circumstances against government rules and calculations, they might be able to determine whether I could apply for benefits or whether I'm due a tax rebate or something.

There are many levels of transparency. I think it's a good question, because I don't think that I've seen anyone answer the question. How open does this government want to be in the digital age in terms of the type of information it makes available? As well, how open does it make some of its systems to allow for others to potentially come along and help government innovate and improve upon its services?

● (0950)

[*Translation*]

Mr. Michel Picard: Let's compare our systems to the Estonian ones, for example. We praise the merits of extremely sophisticated systems that tend to guarantee that they are 100% safe or almost, and that the information provided is accurate, thanks to verifications and multiple cross-checks. Personally, I think that this is not a point that should be touted. It's the minimum we should expect given the current state of technology.

Systems are going to continue to evolve, but efficient systems currently exist that have the best safeguards in the world against external attacks. However, none of the presentations on effective digital systems, including those of the Estonian representatives who testified last week, spoke about the only uncontrollable risk: the human element. I don't have an answer to that one either. Systems are more and more complex, and the risk tends to come increasingly from the inside, and not from the outside. However, despite the development of sweeping technological procedures, no procedure has been raised or mentioned to deal with the risks posed by human resources.

[*English*]

Dr. Jerry Fishenden: I agree that humans remain a weak point in many of these systems. I mentioned earlier some of the social engineering we've seen when very sensitive computer systems in the U.K. have been inappropriately accessed. While they do have protective monitoring on those systems that raises alerts when inappropriate access is made, the time delay between the access being made and the human being found, tracked down, and held to account has unfortunately been tragically slow on occasion, and I do mean literally “tragically slow” in at least one case.

The risk appetite comes back into this discussion, along with everything involved in the software engineering. How do we trust the code that a human being has written, all the way through the system to the operator of that system? Given that this can be a weak point, how do we ensure that as little unnecessary data as possible is displayed to users when they look at a screen in the future, instead of enabling them to bring up somebody's entire record on a single screen to look at all at once?

You're right that all those things should be looked at in designing these systems, but ultimately there's always going to be a risk in these systems. Where are you on that risk appetite, in terms of the cost and the mitigation you're prepared to take in different systems?

The Chair: Thank you, Mr. Picard.

Mr. Angus, you have two minutes to finish up.

Mr. Charlie Angus: It's okay.

The Chair: Thanks, everybody, for attending, and especially to Mr. Fishenden from the U.K. Thanks for your testimony. We look forward to more discussions in the future.

We'll suspend until we go in camera.

[*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