HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 135 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, February 7, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 7, 2019

● (1530)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): We'll call to order meeting 135 of the Standing Committee on Access to Information, Privacy and Ethics, pursuant to Standing Order 108(3)(h)(vii), on the study of the privacy of digital government services.

Today we have witnesses as individuals. We have Jeffrey Roy, Professor, School of Public Administration, Dalhousie University; David Eaves, Lecturer in Public Policy, Digital HKS, Harvard Kennedy School; and last but not least, Amanda Clarke, Assistant Professor, Carleton University.

Before we get into it, I wanted to say that most of you have seen by now the release about the International Grand Committee. It was sent out at noon today. This morning I spoke with Damian Collins, the U.K. chair, as well. It's going to be a developing story as things roll out. We'll send out requests for groups to appear. Likewise, we'll be adding countries to those that we already have. That will be forthcoming. If you want any further information, feel free to ask.

Madame Fortier had submitted a witness. I just wanted to say, for the record, that you can submit witnesses at any point. We had a deadline just because we needed an initial number to get going. If you have a witness who you think would benefit the committee, send the name to the clerk or to my office and we'll make sure it gets put on the list. That said, I do want to get the witness list to you—where we stand right now—so you know where your witness is in the queue.

I have a question from Charlie.

Mr. Charlie Angus (Timmins—James Bay, NDP): I have two points. One is that I'd like us to look at a witness list. So far, we haven't done what is normally done on committee, which is to say how many meetings we'll have and then break down witnesses and decide whether we need them all. I'd like to do that.

I don't want to take any time from our wonderful, astute witnesses, but we're going into a week break and I would like to put out for attention that, given the Globe and Mail article on the allegations about SNC-Lavalin, and given what's being posted about the lobbying that was done, it will fall to Ethics to start to look at this, particularly the question of what kind of lobbying was being done by SNC-Lavalin.

I will be bringing a motion for discussion, because our committee will be expected to look at anything that has to do with allegations about improper lobbying that may have changed the direction of any kind of policy. I'll be bringing that forward at our next meeting.

The Chair: Thank you, Mr. Angus. Are there any further comments?

Okay, we'll get going. To all the witnesses today, thank you for appearing. You have 10 minutes.

We'll start with Ms. Clarke—ladies first.

Dr. Amanda Clarke (Assistant Professor and Public Affairs Research Excellence Chair, School of Public Policy and Administration, Carleton University, As an Individual): Thank you very much.

My name is Amanda Clarke. I'm an Assistant Professor at Carleton University's School of Public Policy and Administration, here in Ottawa, where I hold the public affairs research excellence chair.

I've been researching and advising governments on digital government for the past 10 years. This work actually first began here. I used to be an analyst with the Library of Parliament, and I was on the scene when parliamentarians first started asking us questions about things like Twitter, Facebook and open data. It's very interesting to be back here speaking on some of these topics again.

My work in this field continued with doctoral studies at the Oxford Internet Institute at the University of Oxford, where I completed a Ph.D. study comparing digital government reforms in Canada and the United Kingdom. The U.K. portions of that research looked quite a bit at the “government as a platform” model that the U.K. government has instituted. You've talked a little bit about that and the Government Digital Service, so I'll be happy to speak to that in the questions.

The Canadian portions of that research most recently have been published in a book laying out the history and the trajectory of digital government in Canada, where I focus in particular on the tensions between some of the demands of digital government and our tradition of Westminster government in Canada.

I'm currently leading a research project on civic technologies and data governance. In particular, this work is unpacking the role that private actors play in digital government service delivery. It explores governance mechanisms that can be used to ensure more accountable and equitable stewardship of personal and public data.

I'm really grateful for the opportunity to speak to the committee today. I applaud you for putting what I think is a really important issue on the parliamentary agenda.

I'm going to focus on three topics. The first is the tensions and the complementarities between digital government services and privacy and security. Second, I want to look at data governance and the privatization of digital government services. Third, I'll talk very briefly about indigenous data governance.

On the first theme, the committee's study really aims to promote effective digital government services, while also protecting Canadians' privacy and the related issue of security. I think you're right to identify these objectives as potentially being in competition and to try to seek a balance between those priorities.

In discussing this balance, the committee and earlier witnesses have identified a number of ways in which it appears that federal public servants in particular are too lax in regard to the privacy imperative. There has been discussion about lost hard drives containing user data and about withholding information from the Privacy Commissioner regarding data breaches, for example. At the same time, in my research with federal civil servants, I regularly—

● (1535)

The Chair: Ms. Clarke, our interpreters are having a hard time keeping up with you. Can you just slow it down a little bit? Thank you.

Dr. Amanda Clarke: Fair enough. I did have a coffee right before I came here.

Voices: Oh, oh!

Dr. Amanda Clarke: My students complain of the same thing. I'm sorry.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): We all do it. Don't worry.

Dr. Amanda Clarke: Okay.

All right. I'll take a breath.

The committee seems to be under.... I mean, there was a lot of discussion about the federal civil service not having an appropriately robust appreciation for privacy. At the same time, in my research with federal civil servants, I regularly hear an alternative narrative. That narrative presents public servants as, in some cases, overly zealous in their concerns over privacy and the related question of cybersecurity.

Now, many of you might respond with, "How can governments be overly careful when it comes to privacy and security? Shouldn't that always be top of mind?" But that view, if you buy into it, essentially allows those concerns to be a trump card. In many instances, that can directly undercut scope for much-needed innovation and improvements to the services that governments provide to Canadians. It can also really undermine the efficiency and effectiveness of the daily operations of the government, in particular when it comes to policy analysis. Oftentimes, this overzealous concern for privacy and security doesn't even really address real privacy and security questions.

There are three concrete examples. Many government offices don't have Wi-Fi, in part because overly risk-averse managers have decided that the risk to security and privacy is simply too high. Many government officials similarly can't download the tools they need to do their work, such as free software online that would allow them to do sophisticated data analysis, or even really simple data analysis. They're often banned from accessing websites with really pertinent information to their policy work—websites that are regularly used by stakeholders and by service users.

Perhaps more significantly, in part due to privacy concerns, current legislation, vertical accountability regimes, and corporate information management strategies favour the siloing of data in the civil service. This approach really undermines the potential to produce important improvements, not only in service delivery but also in allowing for policy analysts to work with data across many different policy areas. That kind of crosscutting policy analysis that draws on data from multiple departments is increasingly important as we acknowledge that the policy challenges of today don't sit nicely into departmental silos. They are inherently crosscutting. They don't respect departmental boundaries.

In these instances, civil servants—this is a regular, daily complaint—really can't access the tools, data and people they need to do their jobs well. This creates work environments that are reinforcing the stereotype of government as being out of touch and not being innovative, which certainly does very little for the recruitment efforts of our current public service. More significantly, it ensures that we're going to continue to see substandard and failing government services that reinforce Canadians' already low levels of trust in the state.

To be clear, I'm not advocating that the government cast aside a concern for security and privacy. Rather, I'm suggesting that the approach the committee should be advancing is one that accounts for the trade-offs and costs to the efficiency and effectiveness that can come from overly prioritizing privacy and security without taking a more balanced approach. Here I'm advocating for permissive, flexible frameworks. What would those look like in practice? We can actually look to some current efforts already under way in the federal government that show there are some really promising efforts being taken by civil servants to strike the balance the committee is seeking. I'll just name a few for you.

First, the Government of Canada recently introduced a digital service standard that prioritizes privacy and security but provides means of upholding those principles while also developing services that meet users' needs. In addition, Canada has actually recently emerged as a global leader in developing very progressive frameworks on the responsible use of artificial intelligence in government. This work is attempting to balance, again, those imperatives of respecting principles of equity, democratic representation, transparency, and privacy and security while also being very innovative in how we use data to improve government services and develop more robust policy solutions.

Importantly, this work on responsible artificial intelligence was done in the open. It was developed with stakeholders and experts through a Google doc, giving it a degree of legitimacy but also adding an important level of transparency that I think we should be applauding.

Last, I'd point to the Canadian digital service housed in Treasury Board Secretariat. It was created in the 2017 budget. This is another place where the government is recruiting a fleet of talent with a lot of technological expertise but also bringing in some really sharp policy minds in order to balance the imperative of improving government services while also upholding principles of privacy and security. Here I mean top-of-class, best industry standard privacy and security that I think are really pushing some great innovations in government.

● (1540)

I think, then, that we actually face a very promising landscape, and the takeaway for this committee should be the need to keep reinforcing that work. This demands funding to enable hires and to build up staffing in these areas. It also means giving some of the existing units leading this work the legislative, policy and administrative levers they need to scale their work across the bureaucracy. While these are promising efforts, they really are just the beginning, and they're largely housed at the centre of government right now.

I have only a few minutes left, so I'll move to the second point that I wanted to discuss, which is on data governance issues that arise in the privatization of digital government services.

What I really want to hit home here is that it's important for the committee to acknowledge that many digital government services are not actually delivered by the state directly or at all. This was the early hope of digital government, in fact, that governments would release their data and others would use it to innovate.

That narrative has been nuanced quite a bit, and I think governments are much more realistic about this now. Nonetheless, there are many federal government services that we access through platforms the government doesn't own. I would turn you to the example of the TurboTax software, which, since 2012, more than 12 million Canadians have used to file their taxes, or something such as CANImmunize, an app developed in partnership with hospitals, but also partially funded and endorsed by a number of governments. This is a mobile application to keep track of vaccinations.

There are also countless other digital interfaces that we use to access government services. Some are directly procured by government; others aren't, but are endorsed by government, and some are independently run.

I think the important question to ask here is, when those digital interfaces not managed by government—and thus privately owned—become the only or the easiest way of accessing government services, what is the role of government and how can government ensure that the data those interfaces collect respects privacy concerns and also adheres to other principles of good data governance? When they are contracting private actors, let's say, to deliver digital services, governments need to be very aggressive in defining what data can be collected, how such data can be used and monetized, and who would benefit from that monetization.

We also need to be very realistic about citizens' capacity to give informed consent to some of these private services. One recent New York Times editorial calculated that if the average person were to read all the digital privacy policies they agreed to in a year, it would take 76 working days. I think that in our models of consent for some of these private services, we need to be a bit more thoughtful about this matter as well.

● (1545)

The Chair: Thank you, Ms. Clarke.

Dr. Amanda Clarke: Can I just put in the last one, which I really think we need to get on the agenda?

The Chair: You're a minute over already. If you can do it in 10 seconds, go ahead.

Dr. Amanda Clarke: It's just a quick last point. I haven't seen it yet in the discussions, but some of the discussions the committee has had haven't been made public yet, so maybe it has been on the agenda.

I would like to point the committee to specifically approach the issue of indigenous data sovereignty in its work. I'm not an expert on this, but I can suggest others you should speak to. There are very unique concerns at play here concerning the way the Government of Canada collects and uses data relating to indigenous people, and in particular the way services are delivered to those communities. Given ongoing ways in which that data has been used to marginalize and oppress indigenous peoples, I think it's really incumbent upon this committee to particularly carve out some space for that issue.

Thank you.

The Chair: Thank you, Ms. Clarke.

Next up is Jeffrey Roy, for 10 minutes.

Dr. Jeffrey Roy (Professor, School of Public Administration, Dalhousie University, As an Individual): Thank you very much.

I'm just going to read a brief opening statement, in order to discipline myself to stay within our time limits today.

Good afternoon, Chair, members of the committee and esteemed colleagues. I wish to thank the committee for this opportunity today. I am pleased to participate in this discussion on such an important topic, namely how governments can both expand and improve digital service capacities, while protecting the privacy and security of citizens and all stakeholders.

I will begin by building upon a few of the comments made by the Privacy Commissioner in his thoughtful remarks to the committee last week. Three points stood out for me, in particular: first, the importance of the Government of Canada's data strategy road map; second, notions of barriers versus safeguards; and third, the Estonian model, as a comparator for Canada and other countries.

In my view, the data strategy road map is an important reference point in this debate, as the Privacy Commissioner observed. It is a comprehensive discussion of both opportunities and challenges, based on the cumulative efforts of both Liberal and Conservative-led governments over the past decade, as well as like-minded efforts across all government levels and the private and non-profit sectors.

Data-driven capabilities are now widely regarded as critical enablers of service innovation in today's digital age. Such capabilities often imply, and even necessitate, data sharing across multiple government entities, yet the road map aptly describes a fragmented public sector environment, often more vertical than horizontal, as Amanda noted, with a host of legislative and cultural barriers impeding a whole-of-government approach.

From his vantage point, the Privacy Commissioner observes that "what is a legal barrier to some may been seen as a privacy safeguard by others." In my view, the essential task of this committee is to reconcile the inherent tensions embedded within this prescient observation with the shifting realities of today's society and the emerging opportunities presented by digitization. While I laud the critical efforts of the Privacy Commissioner to safeguard and enforce privacy rights, it is also the case that many legislative, organizational and political barriers do inhibit greater innovation through information and data sharing.

Several pilot initiatives across the country, across all government levels and often encompassing more than one government level, have demonstrated how information and data can be shared without sacrificing privacy. Nonetheless, such pilots all too often flow against the currents of traditional public administration and proprietary notions of protection and control.

In an era where openness and engagement are drivers of networked and agile governance models that challenge traditional hierarchies, privacy is bound to be a contested notion. While a large segment of society remains deeply concerned about privacy, others have simply written off the concept as dated and unrealistic. Bridging this widening cleavage requires trust in public and collective governance mechanisms, and key enablers of such trust are openness and dialogue stemming from political institutions, in large part.

In this regard, and to your point, Estonia is an enlightened example of a country embracing open-source technologies and leading-edge solutions for more integrated and online services. Central to that country's widely recognized success in this regard is the sustained and transpartisan political commitment to making digital transformation a societal project in the aftermath of the collapsed Soviet Union.

In terms of political history and institutional structures, a closer comparator to Canada is Australia, which also presents a compelling case study. Despite widely reported digital failures and privacy breaches, which all countries experience, Australia has steadily climbed to the upper echelon of the United Nations global e-government surveys over the past decade—which is inversely correlated to Canada's performance—partly due to a robust political dialogue and strong engagement on digital matters by elected officials from both the House and the Senate.

Such political literacy helps to facilitate digital literacy across society at large. Australia has also recently created a new national agency, with both federal and state-level involvement, devoted to e-health solutions and, by extension, reconciling privacy and sharing in that critical space. While I have great respect for the boundaries and benefits of federalism, an important lesson for Canada in health care reform is the need for greater intergovernmental collaboration in devising new digital frameworks for shared policies and more virtual forms of delivery.

● (1550)

More broadly, in this country, the absence of more robust collaboration, particularly with respect to financing and shared political accountability, is a major inhibitor of greater progress in digital service innovation. The plethora of public sector service centres in large and medium-sized cities merely underscores this point, further encouraging each government level to focus on its own service apparatus in largely separate manners.

Canada is not alone in facing such struggles, of course. I am presently engaged as a consultant to the OECD, assisting in a groundbreaking study examining digital government from subnational and interjurisdictional perspectives. An emerging theme from this project is the essential role of a holistic governance architecture for the public sector as a whole.

I would offer two final observations. First, privacy in a digital era should not be framed solely or even predominantly as a matter of rights. Citizens, too, have responsibilities in becoming “data activists,” to quote CBC journalist Nora Young in her book entitled *The Virtual Self.*

A new social contract for the digital era cannot be predicated upon unrealistic promises for unfettered privacy rights, especially in a world where governments must themselves challenge such rights for a host of reasons. Of course, the private sector also carries important responsibilities to customers and to all stakeholders. A more sophisticated dialogue is essential as a basis for public education and collective action. As well, in my view, new forms of more direct public engagement in devising digital service solutions are also warranted.

The final observation I would make is the essential role within the legislative branch for what I would call anticipatory capacities to better understand the challenges and the risks that lie ahead. The committee has undoubtedly heard experts discuss the potential of blockchain technologies, which some might associate with cryptocurrencies such as Bitcoin.

Beyond Estonia's widespread adoption of blockchain, Finland is deploying such technologies to deliver support services to refugees, while a separate Finnish pilot enjoins agriculture producers and local governments in a shared effort to improve employment services in rural communities. The European Union has funded several like-minded blockchain pilots, and it is notable here that the European Parliament has appointed a special adviser on blockchain to facilitate collective learning.

In closing, I would commend this committee for its efforts as an important enabler of strengthened digital innovation in the delivery of public services, and I look forward to your questions.

The Chair: Thank you once again.

Our last witness for today is Mr. Eaves, for 10 minutes.

Mr. David Eaves (Lecturer in Public Policy, Digital HKS, Harvard Kennedy School, As an Individual): Thank you.

Good evening, everybody.

My name is David Eaves. I'm a lecturer here at Harvard University. I teach technology in government and digital transformation at the Harvard Kennedy School. That said, I was born and raised in Vancouver Quadra, so I know Ms. Murray, who may be in attendance. I used to live in her riding until a few years ago.

I have also been advising on and thinking about transformation for about 15 years now. In fact, I appeared twice before the ETHI committee to talk about open data and my framework around open data, open information and open dialogue. It kind of turned into the policy framework that I think is still broadly used to organize transparency in government.

Today I want to talk a little bit about digital transformation and its impact on privacy. Particularly, I'm concerned with issues of governance and trust. One thing that the chair may, if he is so inclined.... Just today, I published an article in Policy Options about lessons from Estonia. It deals with some of the governance issues that I think are particularly pressing, questions that need to be asked. If it is of interest, it might be worth translating so that the committee can share it with all its members.

First, I just want to level set about what we're actually talking about when we're talking about Estonia, and what Estonia has done that makes it unique and worth talking about. There are really three things I think the members need to take away about what Estonia has done.

The first is that it has created a set of what we would call canonical databases, where it stores information about its citizens—that is, where you live, what your driver's licence number is and so on. All these things are being stored in databases, but they're being stored in a single database. There's only one database for addresses, one for drivers' licences, one for something else and one for something else.

The second is that the information in these databases is linked together because every citizen has a unique identifying ID. Everybody has their own number. The number gets attached to that information in those various databases, so it's easy to pull disparate information about a citizen all together to get a very clear view about who that person is, and then to offer that information to different parts of government as it's trying to do its service. This is a very different model from what you would find in most countries, including Canada, where these databases tend to be what my colleagues refer to as siloed. The information is actually stored in several places. It doesn't get shared. It's hard to get a full picture, and it's hard to grab all the information you have about someone, and that's why you have to keep collecting it over and over again.

Finally, the third big piece the Estonians have done is that they've gathered information, connected it to individuals through unique IDs and then made those databases—what I want to call “core infrastructure”—available to anybody who works in government, across all government agencies, so they can then leverage it to build new services or improve the services they already offer.

Those three innovations, for me, are at the core of what we're talking about, and if you don't understand those, then it's very hard to talk about the innovations or the costs or the dangers that are facing us if we want to go down that path. First, I just want to level set the committee around understanding those core issues.

Why does this matter? Just speaking a little bit to my predecessor Amanda Clarke's point, once you have this infrastructure in place, it's much easier to innovate and build new services. The core promise that the Estonian government makes to its people is that, by law, it will only ever ask for a piece of information from you once. If, say, the Canada Revenue Agency asks for your address, that means that if you go to the passport office, they'll already have your address on file and you won't have to give it to them again. The advantage of this is that, as you're building services as a government, you don't have to re-collect and re-store all this information. You have it in a single place, so you can leverage it when you build a new service and not have to ask for that information again, nor do you have to build all the infrastructure in that service to store and manage that information.

There are three key questions I would really like the committee to think about.

The first is that, as you're thinking about privacy information, I would love for you to be at least asking this question: What is the threat model that we're trying to protect ourselves against? There are predominantly two types of concerns people have about privacy, particularly in government. One is that they're worried about an external actor attacking the system and gaining access to data that the government stores about people. This is typically a foreign power. The fear is that it will then use that information to undermine the government or possibly even collapse confidence in government institutions and thereby cause people not to want to access information or not to trust the government.

The other core threat model that I hope a lot of time is actually spent thinking about is the internal threat model. I'm actually much more concerned about what my own government can do to me than I am concerned about what a foreign government might do to me. I'm significantly more concerned about what my own government can do to me than what a private actor might be able to do to me. In this particular example, this can range from a government engaged in surveillance to relatively narrow activities.

● (1555)

I'm particularly concerned about perhaps the ex-husbands of women using their access to government information to track where their former spouses are living and what they are doing. We certainly have ample history of that happening in all sorts of places, particularly in police forces, but in other places as well.

Even in small ways, this happens and comes up on our radar. People may remember that when Rob Ford went to the hospital, his records were illegally looked at by multiple people within the hospital records system, and relatively recently, two of those people were charged and fined. That type of access, what you can do with someone's personal information and the way you can share it as an internal actor, in some ways, concerns me more than what an external actor can do. Who we are worried about matters a lot here.

The second piece is that, while I am concerned about internal actors, this does not mean I want to create so many burdens for them in using these types of systems or gaining access to them. I very much want to echo Professor Clarke's points about how increasing security can be good, but if it comes at the cost of usability, then you create a system that's highly secure that no one can access or use. I have students who work in the military here who talk to me about their laptops that take 45 minutes to boot for them to access because they have so much security on them. As a result, people don't tend to use their laptops. I'm not sure we want a system that's so secure that nobody will end up using it.

The third is that privacy is not actually absolute. We want some flexibility. I may not want you to be able to look at my health care records at any point, but if I'm dying in the street, as my colleague Jim Waldo says, I definitely want you to have access to my health care records, and I might not be in a place where I'm able to give you permission to do that. We need a system that, while secure, provides some flexibility.

My key recommendations on this particular piece are.... Before any technical work happened on their systems, the Estonians did a lot of work of really updating their privacy laws for the 21st century and, more importantly, creating systems of logs and audits, so individual citizens could see who was accessing their data, and they could pose questions about whether said access was legitimate or not, and challenge authorities accordingly.

The second thing that I'm particularly concerned about is whether building this type of infrastructure might break the social contract that government has with its citizens. This may be humorous to hear, but most people are often quite comfortable giving information to their government because they believe their government does not have the capability to actually use that information to know very much about them. They're willing to hand information over because they don't actually think government has the competency to weave information together to create a story about them.

In the type of world that the Estonian government has created, this is simply not true anymore. The government's ability to pull together information about someone and actually really understand the totality of that person's life is vastly increased. Estonia has a very specific history and context that allowed that to happen. It's not clear to me that this exists in Canada, so I would strongly encourage the committee to do outreach to the Canadian public to understand how much comfort there is in the public for them to have that type of experience, what they want the government to know about them and what they want the government to be able to do with it.

The particularly large challenge I think you will have is that the citizens will tell you they want two things simultaneously. They will want you to treat them as Amazon does, which means they will want you to recommend new services to them, and they will want customized experiences. They will not want to have to re-enter their information over and over again, but they will say, “Don't you dare use my data to figure out that I have not been filling out my tax forms correctly, or that I actually owe money to the government for this other reason, and I don't want you to invade my life in ways that will make me unhappy.” It's not clear to me that you can have one without the other, or if you can, it's going to require a fair amount of rule thinking in order to get to that place. I don't think we've even begun to have the public conversation to engage and educate the public about how to get to that place and rate what their comfort levels are about such a possible future.

Finally, I'm very concerned about who's going to end up building —and more importantly, controlling—the infrastructure that Estonia has built. These database systems and the unique identifiers that come with them.... I wrote a case recently about a similar system in India, and I went in thinking there was a way to build this infrastructure to prevent a future political actor or a future actor from abusing this infrastructure, and the short answer is that there is not. There is not going to be a technology solution to the types of problems of privacy that we're talking about. There may be technology that can help, but ultimately, we're going to be relying on governance solutions. What is the governance that's going to protect the public from current actors and from future actors?

There are three futures that I can imagine for us. One is that we decide that building this infrastructure is simply too scary, that a government that knows this much is not one that we're comfortable with.

There's a second model, which is that we build it the way the Estonians did: highly distributed, so different ministries own different parts of this core infrastructure and they're sharing their databases with other ministries. The dangerous piece about this is that I actually think the governance in some ways is quite weak; ministries may be unwilling to cut off other ministries' access to data if they're doing something inappropriate, because they fear retaliation from that ministry cutting them off.

● (1600)

Finally, the third option might be that we build it in a way that's highly centralized, where there may be new governance models around the central institution.

I'm almost done, sir.

The Chair: Go ahead and finish up.

Mr. David Eaves: But there, I worry that a single actor would have control over this type of infrastructure and they could use that control to leverage control over other parts of government to prevent them from launching services or force them to design services in certain ways that please them and not in a way in which perhaps Parliament or perhaps that ministry would like to offer those services.

My recommendation here is that a lot of investigation around the governance models needs to take place.

I'll pause there, and I can answer your questions.

The Chair: That's perfect. Thank you very much.

We'll start the first seven-minute round with Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon, everybody.

Mr. Eaves, I'll start with you first because you are living in the town where I also went to school. I went to Northeastern, in Boston, so let's start with you.

You brought up the concept of platform government. If we leave privacy aside for a moment and we look at the core infrastructure, which I think is an important way to recognize what is really involved, as you know, as a developed country we don't have any greenfields as Estonia does. It received its independence and it basically started from scratch. To some extent, part of India, depending on where you look, was also greenfielded. But we are an advanced country. We have advanced systems—systems that have been in place for 20 or 30 years. We have a way of doing business, and certain protocols.

However, when we look at Estonia, it's a unitary government, and there are only 1.3 million people. In Canada we have two issues. We have cross-department sharing of information, and also, because of the system of our federalism, each level of government controls different pieces of information. You have the *x* road in Estonia that goes across one level of government with separate databases, but here, in some cases.... Where I'm from, the Waterloo region, we have four levels of government: municipal, regional, provincial and federal.

When you talk about this infrastructure, and if we use the Estonia model, in which all information is not housed in one database but spread across multiple databases, which would also incur a certain level of security, how do we do it in Canada, where you have four different levels of government with four different core responsibilities?

● (1605)

Mr. David Eaves: All the constraints you have just mentioned.... The Estonians did have a greenfield, which meant that they did not have existing infrastructure, and it's much easier to build something from scratch than it is to try to basically rebuild a plane while it's flying in the air.

I think there are two answers that I would say need to happen simultaneously in order for us to do this. I actually think the technical challenges of building this are going to be significantly smaller than the governance challenges. Finding ways to get governments to agree on how to share information and how to share data is enormously difficult, so we'd better start getting the lawyers in the room together now because it's going to take many, many years probably for them to get to a place where they feel comfortable.

In fact, I was just chronicling this today. In the HealthCare.gov debacle, for that website, the amount of data you needed to have in order to sign up for health care in the United States had to come from 12 different agencies just within the federal government. It took them, I think, a year and a half to negotiate agreements for one service among stakeholders just within the federal government in order to share data so they could pump it into a single system to do one type of service delivery. So we'd better start thinking about that now.

My other piece of advice on that is that if you start just doing that, it will never get done. You need a forcing function, so it might behoove us to find the critical service that we think would have the highest impact on Canadians, the one it would be most helpful to make easy, and start working today on that service and figuring out what data we need from various provincial stakeholders, local stakeholders, ministerial stakeholders and the federal government, and pull that in now to work on something very practical and very real. We shouldn't get overly ambitious. We should focus on one, and then we would probably learn a lot about what we need to be doing.

Mr. Raj Saini: My second question is for Professor Roy. We have heard from other people that data collected by the government should be used only for the reasons for which it is collected. The term I think you used before is “data minimization”. When we look at the Estonia model, it's one-touch. In that regard, if you're going to have this system in Canada and advance digital government, there cannot be a continual repeat of information.

Now, the way Estonia works is that once you sign in, there is certain basic information—address, date of birth, social insurance number, or whatever they call it there—that is housed in one place, and from that place it goes to different areas. Again, that concept in law in Estonia, which I believe is one-touch, how do we do that here? How are we going to make sure that we can have the same effect? The purpose of digital government is to make things more efficient and easier. How do we put that in place here?

We look at the complexity of the country. We look at the population, which is 20 or 25 times greater. It's an advanced country in other areas. How are we going to be able to have that concept? If you don't have that concept of one-touch, then the efficiency won't be there and you won't get public buy-in, which is the other thing that I think all of you have spoken about.

Dr. Jeffrey Roy: I think this is one of the most interesting contradictions or paradoxes of government right now, this notion of privacy protection and the idea of using information only for the reason it's collected.... Let's be clear, that contradicts a lot of what governments are promising to achieve with respect to more citizen-centric, more integrated service models. So there is that contradiction there.

Certainly David Eaves could speak about Estonia much better than I can, but prior to this committee I was looking at some of the data governance work that's been done by the Government of Australia over the past year. They're currently preparing a new legislative framework to address your question. They put out a thought-piece late last year talking about data sharing and reusability within the public sector, how that could work and how to make that work essentially with a privacy framework that recognizes the need for limitations and transparency.

To be very concrete, probably in the short to medium term at least, there will need to be an opt-out clause in order for people to feel they're not participating. I'll give you two examples, one in B.C. several years ago, when they introduced the new integrated services card that brought together the driver's licence and the health care card. Working with the privacy commissioner in that province, the decision was made to allow citizens who weren't comfortable with that integration to opt out. I believe a small minority chose to do so, and that continues to this day.

The second example is with respect to digital health and the new health agency that's created now in Australia to create a health record for every citizen. There, too, very clearly, there is an opt-out clause that allows individuals to have their digital record removed from the system. I don't know whether they do it themselves or whether they sign in and make a request. I suspect it will have to be a tiered approach where we create these new models, but there will be some opt-out.

Finally, I would go back to what I said earlier about your committee's work and the need to have a wider public conversation about what level of comfort citizens have in data sharing, and also bringing citizens more into the conversation, having perhaps citizens' advisory panels, citizens' oversight committees, to provide tangible input in understanding the trade-offs and the solutions going forward.

● (1610)

Mr. Raj Saini: Thank you.

The Chair: Next up, for seven minutes, we have Mr. Kent.

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

Thank you all for attending and informing us today.

Professor Clarke, you touched on the necessary balance between the public and private sector in developing effective digital government, whether only at the federal level or subsequent levels of government in Canada. We have two examples. One is the failed —or failing—Phoenix pay system, where the procuring agency cut some of the complexities that the digital developer recommended to have an effective system in catching up with contracts, distributing pay and so forth. Then the button was pushed too early on that incomplete system, and we have the disaster we see today.

On the other hand, we have Toronto's Sidewalk Labs, where the city has pretty much given over all control to the Google sibling Sidewalk Labs and allowed it to develop...in great secrecy—more secrecy than many Torontonians and digital authorities would like, to the point that Jim Balsillie, formerly of BlackBerry, said, “[it] is not a smart city. It is a colonizing experiment in surveillance capitalism”.

How do we find that balance? Does government have to better educate itself to be an informed buyer and an informed overseer of the way a digital government service would be developed and operated?

Dr. Amanda Clarke: That's a great question.

I didn't have time to bring it up in my remarks. I think that, if you're focusing on the question of digital service, design and delivery, procurement is a huge part of that conversation.

I think there are two interesting things happening in the procurement space right now. One, as I mentioned in my remarks, is that, early on, a lot of digital government enthusiasts, particularly with the dawn of open data, thought that governments wouldn't have to produce a lot of their digital services. That model didn't pan out, for a number of reasons. One of the big ones was that there are a lot of core services that governments are going to have to continue to develop, both citizen-facing but also internal corporate systems such as pay systems or email systems. In response to that, one of the things we've seen is an interesting return to the state on the procurement front, where we're seeing leading digital governments investing quite a lot in their internal capacity to be smart shoppers in this space.

I would say that both Sidewalk Toronto and the example of the Phoenix pay system originated in part from the same problem. In the case of Toronto, the waterfront board—and in the case of the Government of Canada, I guess it would have been Public Works—didn't have sufficient expertise to make smart choices about what systems they needed. This is part of what something like the Canadian digital service is attempting to remedy by bringing people in-house in government who can design contracts sensibly to procure what they need.

The other interesting thing that I think is happening in this space is how we originally ask what we need from the system. This is moving away from designing, in particular, citizen-facing services around government structures and internal government needs. Instead, it is borrowing from a field of work called design thinking to begin early on with deep research into users and how they're going to use the service. You would then structure any procurement you might need to do and any service design around that.

Something like Phoenix could have been prevented in many ways by doing that kind of work early on and realizing the complexities of the system and what you would have needed. That user testing allows you, in particular, to experiment on a small scale before you sign onto a long-term contract—what we call legacy contract—which often anticipates what you're going to need from a digital service before you've even tried it. If you look historically and globally at the big IT failures, you see that it's these legacy contracts that didn't begin with small-scale user testing that lead to the big failures we see. HealthCare.gov was mentioned, for example.

● (1615)

Hon. Peter Kent: Professor, thank you very much. That was very helpful.

Professor Roy.

Dr. Jeffrey Roy: The Sidewalk Labs example is interesting. I'm a little more hopeful on that front that, perhaps, with more transparency and open negotiation, a framework will emerge that balances the public and private interests. I think these sorts of examples are going to be very important to learn from going forward.

The one additional point I would make, beyond Amanda Clarke's comments, is that there needs to be a mechanism in place to facilitate the public dialogue that we're talking about. I know that right now the Government of Australia is appointing and creating the position of a new chief data commissioner. I can't speak to it in too much detail, so I won't pretend to be an expert there. The U.K. government, of course, has a chief data officer.

As important as the Privacy Commissioner is—and I'm not suggesting a diminishment of his role in any way—there does need to be a way of thinking about data as an open asset as well, and engaging with the public and stakeholders about what the appropriate trade-offs are in moving forward. The idea of having a position, whether in the executive branch or a new potentially independent position, that could reach out to the citizens more could be one way of facilitating the public dialogue that we're all in agreement is required going forward.

Hon. Peter Kent: Professor Eaves.

Mr. David Eaves: I will just make two comments.

First, I would say that one thing that makes this topic particularly challenging and that I want to make sure we understand in this room is that we're talking about moving from systems that we call vertically integrated, in which you're dealing with a system such as passports, to a system in which we're thinking about something that combines levels of horizontal systems that enable you to then quickly deliver new services on the top, so that the passport delivery reaches in and grabs information from various horizontally layered services.

The reason I appreciate your question, Mr. Kent, is that I am much more concerned about the governance when you have these horizontal layers, because if you get the governance wrong on something that's vertically integrated, it's very costly—to speak to Professor Clarke's point—but it can be remedied over some medium- or long-term piece, and it doesn't impact all the other things that are going on in government. If we get the governance wrong for one of these horizontal layers, however, it's actually quite serious, because then everybody who builds on top of it is impacted by it.

It's absolutely imperative, then, that this committee think very deeply about the privacy implications, the security implications, the design implications of this approach, because it has knock-on effects for what happens to everybody else.

I think it's very likely that some of these horizontal layers will be held and owned by the private sector. It is unlikely, for example, in the long term, that the Canadian government will build and maintain its own cloud. It will probably have a private sector actor doing that.

One thing that then becomes potentially challenging is that the private player is determining what investments to make, how to expand that infrastructure and what future capabilities it's gong to have. Those choices will constrain what the Government of Canada can do and may even be made in a way that constrains us from choosing competitors when building things further downfield.

We'd better be really sophisticated and nuanced, therefore, in understanding how these players are acting, because they may choose to constrain us in ways that are not immediately apparent to us.

● (1620)

Hon. Peter Kent: Thank you.

The Chair: Thank you, Mr. Kent.

Next up for seven minutes is Mr. Angus.

Mr. Charlie Angus: Thank you, Mr. Chair.

Well, I have my government phone here and I get messages all the time telling me that I have to do such-and-such function right away, and I try to do the function and then it says that I'm not allowed to do it, because it won't recognize my phone.

That's all interesting, but it's not what our committee is here to discuss. We are the privacy, ethics and accountability committee; we're not the government operations committee. There are many cool things and many neat things we could do. We could try saying that we're doing better government services, and if we believe that we can turn it all around, I think that's great. But our committee's job is to protect citizen rights, end of story.

I am a little concerned, Mr. Eaves. Maybe I heard wrong. Were you quoting Nora Young when you talked about citizens having to be data activists and governments having to challenge privacy rights? What was that quotation?

Mr. David Eaves: I don't think that was me, sir.

Mr. Charlie Angus: I'm sorry.

Mr. Roy.

Dr. Jeffrey Roy: That was me.

The quote itself was limited to the “data activists” part. It wasn't suggesting that citizens need to challenge governments, just to be clear on that.

Mr. Charlie Angus: You said something about governments needing to challenge.

Dr. Jeffrey Roy: I was pointing out that sometimes governments need to restrict privacy rights for a variety of reasons or think about limits to privacy rights, whether for service improvements or service integration in terms of information sharing, or for a whole host of security reasons when information is shared for a variety of reasons in terms of focusing on public safety and things of that sort.

I wasn't suggesting that governments don't respect privacy rights. I'm just suggesting that privacy is one consideration that governments need to balance with other considerations. Nora Young's point was more that citizens need to have a certain sense of responsibility for their own data ownership and to be thinking about what transpires with their data and doing their best to try to understand it.

Mr. Charlie Angus: Okay, thank you.

Mr. Eaves, I was very interested in your saying that you were more concerned about what your own government will do with your information. We are told all the time that people get information only for good reasons. Police go to get information from telcoms only because it's important, but they do it time and time again without a warrant, which undermines basic principles of the judiciary.

In Canada, time and time again, we have issues of private information that has been gathered. How do we secure the rights of citizens, maybe from the security state, or maybe from people who think that someone may be a terrorist or that someone is just problematic? They have the capacity to access all that data without any protections.

Are you concerned about limits and how we protect citizen rights?

Mr. David Eaves: My second grand point was about our breaking the social contract. I think some people don't trust the state, so they don't want to share information at all. Others think the state is simply not capable, so they're happy to hand over data because they don't think the state is actually capable of weaving that data together to do anything interesting with it. Other people are quite comfortable and don't mind; they trust the government.

I think the model that we're talking about with the Estonians is just so radically different from what we have today that we need to have a very intentional dialogue about what the new social contract might look like. In Estonia, one thing they do that I think is an important piece of that social contract is logging who's accessing information about, say, Mr. Angus. You can log in at any point and see who took a look at your data, and then you can complain. You can ask why this police officer or this doctor is looking there. I was talking to the chief information officer of Estonia, and he said that in the early days they prosecuted some people very aggressively who were looking at data they shouldn't have, in order to reset the culture inside government about what was appropriate behaviour.

My sense is that this type of activity is probably going to have to happen with us, but it will need to be balanced with the police forces, who are going to want access with a legitimate warrant.

Mr. Charlie Angus: For sure, if anything, it would be with a warrant. With government, we've had CRA people who have spied on people's financial information. If there is a protection mechanism so we can actually see that something has been looked at.... Maybe sometimes it legally is—and if it's legal to look at it, then it's useful—but we need to know that.

I'm concerned, though, about what you said about the building of the infrastructure. Is it going to be public? Is it going to be private? We have the issue with Sidewalk Labs and Google. Google was kicked off Apple's apps because they couldn't be trusted and they were spying on people, and yet we're going to let them do the infrastructure of a major urban city. How do we say that, if we're going to have public spaces, they're going to be...? How do we trust Google? I don't trust them.

Amanda Clarke asked if she could answer that.

● (1625)

Dr. Amanda Clarke: I think you're right to bring up the Sidewalk Toronto example as something we wouldn't want to emulate, but perhaps that's just where that begins and ends. I think the one thing we can learn from that disaster is exactly how this committee and other policy-makers shouldn't structure the involvement of private actors in digital service delivery or in digital projects.

I agree with Mr. Eaves that there will invariably be private actors involved in the infrastructure, which our governments are going to be relying upon to protect privacy, but also to design and deliver services and manage data.

I think the real question becomes, how can we structure those contracts in a way that allows us to prevent some of the problems that I think Mr. Eaves has rightfully put on the table? But also—

Mr. Charlie Angus: I just have a minute left, so I'm going to have to interrupt you there.

Dr. Amanda Clarke: Yes, of course. Go ahead.

Mr. Charlie Angus: On indigenous data, I worked for a first nation government. They always said, "Just give us your data. We love you people. We want to work with you. Give us your traplines. Give us your sacred sites and we'll help map them." The only power the community had was their data, because Indian Affairs controls everything else. The communities are not going to turn over their data.

How do you think we can have a conversation about the rights of indigenous sovereignty, given the 250 years of bad faith in Canada? How can we have a conversation about what data means to an indigenous community and how to protect it? I think it's very important that you raised that.

Dr. Amanda Clarke: Yes, I think those are all key questions. As I said, this isn't my area of expertise. There is some really interesting work that OpenNorth has led, working with first nation communities in B.C. There's also some really progressive work in this space from New Zealand. I really think that bringing some indigenous voices to the table here would be important, because, as you note exactly, data is power. Data is power that these communities have, and traditionally, Canada has not used data in ways that lifted up indigenous communities, to put it softly. Quite frankly, I think we can find very good examples of data being used to marginalize and oppress. It's part of a violent colonial history. So, it's a really important piece of this discussion that needs to take place here.

Mr. Charlie Angus: Thank you.

The Chair: Thank you, Mr. Angus.

Next up for seven minutes we have Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Thanks very much.

I want to start with something really simple. I have a social insurance number. I'm not entirely sure what it's for most of the time. Now I'm going to attach a password to that social insurance number and then the government is going to issue me an RSA key with a rotating number to ensure that there's a two-factor system to it. Now I can access CRA immediately. When my wife is on maternity leave and needs to access EI, she could use that same system. When I'm reapplying for my password, I could use that same system. Why is that so hard?

Mr. Eaves.

Mr. David Eaves: It's a question of what the implications are of making that choice.

We could say, okay, your social security number is now your unique identifier, so let's start putting your unique identifier against every piece of information that the government collects about you, maybe at the federal level, but maybe also at the provincial level and the local level. Someone could come along and say, well, let me see if I could query a whole range of databases and start pulling together information that I know is specific to you and then use that to create a profile of you that may be helpful, but I may chose to do things with that information that are not helpful.

Mr. Nathaniel Erskine-Smith: Great. That's really useful.

Let's add another layer. Now there's a population register with my basic information: name, address, phone number, and perhaps email address. Hopefully the government is able to communicate with me by email in the way that I used to be able to communicate with my clients. It's bizarre that I can't get my blood results by email when I could certainly deliver legal advice, which is as sensitive oftentimes, by email.

Now there's a population register with my basic information. Now the only information that every department, except for that population register, has about me is my SIN. Now there's an additional layer where they don't know anything about me except for a connection of my information. If it's a health care system, they know my blood results in relation to a SIN but not in relation to my name. If they have to access that, then they're accessing the population register first, so now we add that layer.

Then we add another layer, which is the Privacy Act or whatever data governance piece we want to layer on this to govern the queries that these databases can make of one another. Those are the moving parts of this system, and if we get those layers right, the system presumably can function effectively.

● (1630)

Mr. David Eaves: I agree.

I get very torn. I love this subject because this is the future I teach about. This is the endgame that we want to drive towards. Everything I'm trying to talk to you about today is the questions that I ask myself.

What happens if we win? What happens if we succeed? What happens if we get to that world? What are the things we want to be thinking about to mitigate the possible negative outcomes?

I would put forward that probably people such as you and me have not experienced the worst violence the state can bring upon an individual. If you were someone for whom the state has not always been a friendly and helpful person, you might be deeply concerned about what I would call a very hyper-powered state and its ability to use this information against you.

Mr. Nathaniel Erskine-Smith: Yes, I appreciate that.

You've laid out in your article four concerns. Your first concern is the social contract. Say, as a starting point, when we're rolling this out—if we were to roll such a thing out—it begins voluntarily. Someone such as me or you, who has trust to at least try out the system, can do so, and those who are concerned don't have to.

Would that not meet the social contract concern, at least in the first instance?

Mr. David Eaves: It may, in the first instance, but there are two concerns that I would have following on that.

The first is that people who are most likely in need of state assistance tend to be those who are most likely to be marginalized. I can actually imagine a two-track system, where those who are wealthy, who really don't need to engage with the state very much, end up contributing very little information into the state and the state knows less about them, whereas those who are most in need or those who are most marginalized actually end up putting a lot of information into the state. Therefore, we almost have a state that's capable of large amounts of surveillance on the people who are maybe the least prepared to protect themselves.

Mr. Nathaniel Erskine-Smith: If it is opt-in, and then there's the system as it is for those who don't have trust in the system, these data challenges already exist for governments. The challenge that you just laid out already exists for governments. Governments do share information among agencies. There are pathways for doing so within the Privacy Act, within the Security of Canada Information Sharing Act.

What changes when it's digital?

Mr. David Eaves: A lot changes, such as the scale at which you can do things.

Right now, things may be digital, but my ability to share information between ministries and identify who exactly is David Eaves, and figure out which file is about that David Eaves versus possibly another David Eaves, requires someone who is a motivated actor piecing that story together, whereas in a world in which everything is connected to a unique identifier, where I'm going to identify exactly who I am and all the information connected to me, I can do that at scale. I can do that for all 33 million Canadians simultaneously.

Maybe I can throw a machine learning algorithm against that and figure out what services I offer people, figure out who's Muslim and who's Christian. I could be doing all of that in a way that I could never do in the world in which we exist right now.

I'm deeply in favour of going to this world, but I really want to make sure we figure out the governance models before we do it.

Mr. Nathaniel Erskine-Smith: That's right.

I guess the question then is that we already have a governance model in place. We have been told multiple times that it is insufficient as it relates to the Privacy Act. However, that would be the governance model that we're looking at.

Is it so insufficient as of today? It governs data sharing between institutions already. Just by virtue of the fact that I'm now allowing these agencies to interact, and let's say the population register is a starting point, it doesn't seem that worrisome to me, given that these agencies all have this information and it will allow me to access these services in an easier way.

As a starting point, say we didn't even update the Privacy Act—although I think we should make recommendations on that front again. I don't really understand how the governance challenge is different, because we already have a data governance framework in place—the Privacy Act.

Mr. David Eaves: My fear is that the Privacy Act is actually impeding certain types of activities and innovation that we would want to have, and not necessarily preventing certain types of activities that we don't want to have. That's why I worry about the current state of the Privacy Act. I don't think it's far from perfect, but I think it probably needs a little bit of reworking.

Then, more importantly, are we setting expectations among the public about what they want? Even an opt-in world.... You know, in India, they did an opt-in; in theory, their unique identifier was opt-in as well. However, the alternative has become so poorly done that, really, if you don't opt in, the service level is so terrible that everybody ends up opting in. So, are you really opting in because you're happy to give this information over to the government and you actually believe that it's going to use it in good faith, or is the hassle level simply so high that you don't really feel like you have a choice anymore? I would really want to make sure that I answer that question carefully.

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

One thing I would just challenge Ms. Clarke with is this: If you see a point to inject your opinion, feel free to do so. It's up to the members to decide whom to include in their question and who answers that question, but if you see a gap, feel free to jump right in.

● (1635)

Dr. Amanda Clarke: That's right.

I just wanted to—

The Chair: Except time is up for you now....

Voices: Oh, oh!

The Chair: We'll go to Mr. Gourde next, for five minutes, and then maybe you'll have a shot.

Go ahead.

[*Translation*]

Mr. Jacques Gourde (Lévis—Lotbinière, CPC): That works for me, Mr. Chair.

My question goes to Ms. Clarke.

In Canada, digital services are currently provided by each department, and they evolve constantly.

Redefining digital services for Canadians implies either keeping what currently exists or throwing the baby out with the bathwater.

Who will get the benefit? Will the project help Canadians, or the government that will be able to provide more services? Will it make for better connections between certain departments? Do Canadians want departments to be talking to each other about their files, if they have not asked for it?

None of my constituents has come to tell me that they want an official from the Canada Revenue Agency to be communicating with someone from Citizenship and Immigration, for example. No one is asking for that, and I do not get the impression that Canadians have asked the government to redefine what digital means in Canada. Let us not kid ourselves, if we start focusing on going digital again, we will not be talking about spending millions, but billions. The project will take a very long time, for ever, in fact.

Ms. Clarke, in your opinion, who will get the most benefit from redefining the digital world in Canada?

[*English*]

Dr. Amanda Clarke: That's a great question. The question of what citizens even want in this space has come up a number of times. I don't think we have very strong data on that question right now.

To speak directly to your point—"Do people want this?"—there are two things. On the one hand, sometimes people don't know what they want until they are.... They're not even aware how good things could be. Your constituents may not be asking for this, but if they were shown how easy it could be to apply for a service and see their information already populated, or how the organization of services around what we call life events could make their interactions with the state much more seamless, they might be much more supportive of the kinds of transformations we're talking about in data governance.

What do I mean by "organized around life events"? This is something the Government of Canada has led on for quite a while. It might have come up in your discussions that we used to be kind of the darling of e-government. That was because of early work we did, following the same principles that Estonia follows right now, which is to say that when citizens interact with the state, they don't care which department does what. They're not very interested in navigating a whole bunch of siloed websites. They're going because they just had a baby and they need to figure out all the things they have to do when that happens.

They also don't care about levels of government, and often don't understand who's responsible for what, which can create a lot of inefficiencies in our interactions with the state. I think the model of horizontal, platform government begins with an appreciation of user needs. That's the driving force behind this, when you look at the jurisdictions that have really led on it.

I think that's the endgame we could be going for, to make it a purely time-and-resource question, so that when you go to transact with the state, it's fast. I think that, on a bigger level, this has democratic implications, because when I interact with the state and it doesn't work well, I question where my taxes are going. I wonder what is going on in all those bureaucracies. It fuels narratives of the gravy train, and it allows governments to say they're going to show up and clean up all the inefficiencies.

Those narratives rest, in many cases, on people's very personal stories of bad transactions with the state. I've heard Canadians say to me a number of times, "Phoenix is such a disaster. If they can't even run a pay system, how can we trust them to solve climate change, administer a carbon tax, handle child welfare benefits or run the school system?" The list goes on, and I think we have to be really thoughtful about the larger stakes at play here.

I take Mr. Angus's point that there is some blurring here of jurisdiction and mandate between what you're focused on, which is privacy and ethics, and what other committees would look at around government operations. I think this reflects exactly what we're talking about, which is that policy issues are porous. There are problematic silos between parliamentary committees, in many ways. The decisions you make and the recommendations you put forth on privacy will have deep implications for how well we can structure government services and how well governments can operate. The endgame that unites the work of, say, the government operations committee and your committee is delivering government services that citizens have faith in and that underpin a strong trust in the state.

Yes, I definitely think that even if people aren't asking for this, it could do a lot to make your constituents happy.

● (1640)

The Chair: Thank you. That is your time.

The next five minutes will be split between Ms. Vandenbeld and Monsieur Picard.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you. I'll be quick.

My question is for Dr. Clarke. First of all, it's nice to see this kind of expertise right here in Ottawa, at Carleton University.

I'm a bit alarmed, as an MP who represents a lot of public servants, about what you said in regard to public servants being unable to download tools or access websites or even Wi-Fi. I just wanted to get a little commentary on that. How widespread is that?

The other question I have is this. You did your studies on the U. K., and you mentioned something in the beginning about Westminster democracies. Does the form of government—in our case, Westminster-style—have implications for how we can actually do digital democracy?

Dr. Amanda Clarke: On the question about Westminster, I'd say that one of the clearest potential tensions is around our vertical accountability structures and this horizontal model that we're increasingly pushing towards, when we think about platform government or the Estonian model.

Right now, the way we allocate praise and blame in our system is through the notion of ministerial responsibility. When a service fails or when funds are spent irresponsibly, the minister is the one who's called to account. In a really practical sense, they field those questions in the House. Who will be responsible—very practically speaking, in a concrete way, before Parliament—when there is a failure in one of these horizontal systems?

I want to be clear that there are ways to overcome this, and the beauty of the Westminster system is that it's inherently evolutionary. It is built to adapt to the times. I think we really could explore what are often called models of horizontal accountability or shared accountability. Essentially, it's the point we've been discussing. This is not so much a technical question as it really is a governance question—laying out, ahead of time, which parts of the bureaucracy and then, ultimately, which ministers will be responsible for how these systems are rolled out. I fear that right now a lot of the enthusiasm around platform governance has actually ignored that question, in part because we're often just dealing with pilots to show how this might work. If we're going to scale this, we need to be thinking about those questions.

I think the second piece of work that might be done around here is not just on the question of ministerial responsibility, but also getting into some of the data governance questions. Earlier on, the point was raised about whether the Privacy Act is fit for this purpose. The Privacy Act is one of the tools we need to look at to address these data governance issues, but it's actually not the only one, and it doesn't address a lot of the questions we're talking about.

Mr. Erskine-Smith mentioned the point about how this data could be used and combined to, say, tailor services to me in particular to say, "By the way, we know you had a baby. Now you're eligible for this tax credit." Those kinds of questions have privacy implications, but they also have other questions around how data can be combined, when we feel comfortable with the state contacting us directly, and how we want different ministries to be able to access data. Privacy is one lens, but there's a whole other lens around ensuring we don't disadvantage certain groups over others, and those sorts of questions.

Again, it's the bleeding edge nature of the issues you're looking at. It's about privacy, but we also need to maybe develop entirely new regimes, not necessarily in legislation, but in principles of data use. Again, that's why I pointed you to the work that's being done on artificial intelligence. There, I think, we have a great example of the federal government being really progressive and open in talking about some of the very real ethical questions that are going to arise when we apply artificial intelligence to policy-making. The same thing can be done for a lot of the questions you're talking about.

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

I've been hearing about this Estonian model for weeks and weeks. Who worked on this model, who tested it, and on what basis do you support your probably overrated appreciation of the model? This is for anyone.

● (1645)

Dr. Amanda Clarke: David, you wrote the article, so I'd say it's you who's going to field this one.

Voices: Oh, oh!

Mr. David Eaves: One of the things about the Estonian model is that it emerged after the Soviets left Estonia. They really had very few services, very few business processes in place, almost no infrastructure in place, and they really needed to build a state from scratch.

I think the Estonians were lucky in that they started to do this at the very same time the Web was emerging. Rather than trying to simply replicate the way state services had been built in other types of governments, they looked at how people were building software on the Web—distributed systems with canonical datasets—and so they started to simply say, we're going to do something really different. They were actually forced by the fact that they had very little money, so they said, we can't afford to replicate all of these systems in every single ministry.

You had a very specific point in time with a very specific history, with a relatively young leader who was willing to give political cover to people who were trying something very different. Those are the historical roots of how Estonians ended up doing what they did. One of the reasons why I think they're a wonderful model to look at—but probably not a wonderful model to try to emulate—is that their situation was so unique.

The Chair: Thank you, Mr. Picard.

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

Hon. Peter Kent: Mr. Eaves, thank you for that.

I'd like to pick up on your question about threat models. Earlier this week, you may have noticed if you looked at the blues that Chris Vickery was talking about the Estonian model and Estonia's claims on their website. I quoted their reassurance...that they had been hacked once. They'd been subjected to a massive attempt by Russia in 2007 to penetrate their system. Mr. Vickery was so confident that their system was hackable that there was a discussion here off camera sort of saying, why don't we ask him to try to do it in real time as we watch from Ottawa?

What are your thoughts about threat models constantly evolving? Perhaps, as you said, the domestic threat is a greater real one in terms of individual privacy, but we know that the governments of Russia and China, primarily, are constantly working to get into government systems. Whatever new system is developed, it's almost obvious—Mr. Vickery was quite convincing—that someone will come up with a way of penetrating it.

Mr. David Eaves: For me, there is not really a big choice here. The foreign actors are already very interested in our systems, and there is a long history of them penetrating our systems already. I believe that five, six or seven years ago, Treasury Board was very compromised, to a degree where I think they had to throw out almost all the computers in the entire department.

I want to be really clear. It's not like the current system is somehow secure and we want to move to a new system that has kind of dipped into the unsecure. What we have to be thinking about is the types of threats and what they mean for us.

Under our current model, maybe one of the advantages is that, because it's disorganized for us, it's also disorganized for an attacker. So if they penetrate a system, they may penetrate only a single system and learn so much. But in a system where, say, it's very easy to identify my unique identity and the systems are more connected, they may, too, now be able to penetrate the system and get a more global view. So that poses a new type of threat.

The flip side of that is that it may also be easier to defend. Right now, your information is only as well protected as the weakest database it happens to be in, if it's in five different databases. In America, that turns out to be Equifax or some other poor databases that get widely used. It may be that some consolidation would actually allow us to bring in our defensive resources and concentrate them.

But there are real risks here either way.

Hon. Peter Kent: Professor Roy, what are your thoughts?

Dr. Jeffrey Roy: For me, the key issue here is one of resilience and openness. When you go back to the Estonian model—which I appreciate everybody is getting a little fatigued hearing about—when they started using e-voting in that country, they put out their source code as open source and challenged people to find shortcomings in it, and a group of researchers found shortcomings and published them online. But that did not shake the confidence of Estonians to continue to use e-voting. It simply led to corrections. If you think about Apple in the past week, notwithstanding their justified criticisms of Facebook and Google, as Mr. Angus rightly referred to, they, too, had a privacy breach with respect to FaceTime that they had to apologize for.

Governments traditionally, especially with respect to IT architectures, have tended to be very inward in terms of thinking about proprietary systems, proprietary controls, of course wanting to minimize the notion of breaches and the information that gets out around breaches. On the other hand, I think we need to kind of turn that around and think more and more about being outward and open about admitting the vulnerabilities and looking more at how we can address them collectively and adapt in ways that improve the resilience of our systems in both technical and social ways, going forward.

● (1650)

Hon. Peter Kent: Professor Clarke, we have time for—

Dr. Amanda Clarke: I think that's an excellent point that I'll echo. One of the conditions that need to be in place for all of this to work is citizen trust in the system, and that's also going to be about generating a certain tolerance for failure amongst the public. I'm not talking about the public kind of smiling and shrugging off large-scale data breaches or anything like that. One of the things I constantly hear when I speak to governments that are doing very innovative things on digital is that part of it is that they have a licence to innovate. They have a population that trusts that their state has their best interests at heart, that their state will be open and honest about mistakes when they happen, and that their state has appropriate systems in place to manage those errors so they're not large-scale.

I don't think we have that culture right now in the Government of Canada. One of the previous witnesses—I believe it was Mr. Fishenden—suggested that one way we could improve the culture of privacy and the accountability around privacy would be to institute a new extra-governmental oversight body. I would strongly disagree with that. We have a history, in the federal government in particular, of looking at all accountability issues as ones where we need to create more oversight, more rules, more top-down punishments.

What this creates in the civil service is this absolute fear that in trying anything new and different, if it doesn't go right, you're going to be smacked down so hard that, first, you should lie about it when it happens, and second, you just shouldn't even try it in the first place. It's incredibly frustrating for employees who are trying to do things that are different, but it also just puts a full stop on a lot of the innovations that we're talking about here, which will in many cases rest on work from within the civil service. There will be parliamentary leadership, and we will need to have ministers behind it, but civil servants are going to do the grunt work, if we're planning on moving towards any of these sorts of models.

I think a model that focuses on accountability for learning could be a really important part of generating a culture in the Government of Canada that respects privacy but also allows us to be more innovative in our services.

Yes, I think that's something we need.

Hon. Peter Kent: Thank you, Ms. Clarke.

The Chair: Last up, we have Mr. Sikand for five minutes.

Mr. Gagan Sikand (Mississauga—Streetsville, Lib.): Thank you.

I'll start by thanking Ms. Clarke for the work she did at the Library of Parliament. I am co-chair of BILI, and we're still talking about digitization, so thank you for that.

I'm just going to go through what my thoughts were after I heard everybody, and then open it up for any comments.

Initially, I thought, “Wow, holy 1984“, and then I thought about the social contract that we have. I started thinking about how, if we do something like what Estonia did and we can ask for data only once.... Okay, the data's there once, but governments change. I thought about the implications of that. If you take that further, if there's a natural disaster and perhaps the servers are taken out, does that mean the government has just gone down? Then there's the legal implication of that, if you have to ask again for that information; in Estonia, they can't do that.

Then I started thinking about foreign attacks. Again, if the Trojan Horse comes and takes out the information and we have to continuously give our data...the privacy implications of that.

Then I started thinking about Amazon and how they host their own servers and have algorithms. There's the topic of whether it's going to be public or whether the government should have its own cloud-based data. The Internet of things is progressing, so is this something that we start to put resources behind, under infrastructure?

Then, again, I was thinking, “Okay, if it goes private, we have elections and governments change, and then you can start to track people”—as was pointed out.

I guess, along with all these thoughts, my question comes: If we do a cost-benefit analysis, do we need to go digital?

Chime in if you have any thoughts.

● (1655)

Dr. Jeffrey Roy: If I could, I will begin. To go back to the issue of cloud providers and Amazon, I believe the Government of Ontario, under the prior government, has already outsourced a number of its database servers to Amazon web services. From a privacy and security point of view, I think it's setting the bar much too high for the public sector to be building the databases of the future. It's very clear that Shared Services Canada has struggled. That's no secret. A lot of problems have arisen from that. A member referred to Phoenix a short time ago.

There are, of course, imperfections and challenges in working with private actors, as has been discussed. It seems to me that the better route is to work with the most sophisticated technology companies in the world. They have the security capacities to enshrine privacy, as Apple tries to do—perhaps more than social media companies today. Certainly, Amazon and Microsoft are very focused on security in terms of their cloud offerings. We should also be engaging the private sector in a dialogue about the privacy implications of that and ensuring there is robust accountability for how they partake in public infrastructure and what the implications are. I don't really see an alternative.

Mr. Gagan Sikand: To follow up on that, if the best technology is actually from a different country, now our sovereignty becomes a bit of an issue. Do you have anything to say to that?

Dr. Jeffrey Roy: That's why, despite this notion of the cloud that is very porous with server farms all over the world, many countries have negotiated agreements where data centres for certain types of data need to be located within national boundaries.

That really shouldn't be a limitation for Canada, which has a number of data farms from large entities that have set up here. Quite often, they are very much under the radar screen because they don't want the locations overly publicized. I think that's not necessarily a limitation. For this meeting, however, I was just reading through my privacy policy for the PC Optimum online program, and they very clearly state in their program that they can't guarantee that data is not shared on servers in other countries as well.

It is a challenge; I grant you that. I'm not saying that it's not, but I do think there are ways in which governments have stipulated.... For example, even Apple has to store iCloud data in China, according to Chinese law. Most countries are going in that direction. There's some flexibility in having certain datasets located only within the country under certain regulations but having other datasets that are perhaps less sensitive, less critical, in different layers of the cloud, while still demanding that these private actors be transparent in different forums, in terms of explaining how that data is being used.

Mr. Gagan Sikand: Thank you.

The Chair: Go ahead, Mr. Picard, for two minutes, if you have a short question.

Mr. Michel Picard: It's a very short one, yes.

What is the threshold for the privacy aspect of my data? Who chooses what is private and the limit of what can be gathered?

I'll give you a scenario in a smart city hypothesis. If I'm walking in the street at two o'clock in the morning, I hate the idea that the government will have my facial recognition and know that I was there at that specific hour with someone I may or may not have to be with. I do need my own privacy, and leave me alone.

However, if I become the victim of a hit and run, I do want all the cameras to get the son of a gun who got me, the licence plate, the picture of the driver and everything. I wouldn't care that much about privacy.

What's my challenge? Who decides what is and what is not private?

Mr. David Eaves: I tried to surface this earlier, and I said that I think you guys need to be engaged in a dialogue with the public, because I had the exact same example with my health care records. I don't want someone to see them on any given day, but if I'm lying in the street dying, I definitely want people to have access to them.

The honest truth is that there are no simple answers to these questions.

One of the key things I am trying to convey to you—and I think Professor Clarke is as well— is that we need to be thinking about what culture and what norm we want to build in this country around how we are going to manage these things. The opportunity space for us to do something different is there, but if the public doesn't come along and we don't move, then there's going to be an efficiency tax, an opportunity tax that we all pay as Canadians but that other countries won't be paying as they do things differently.

How are we going to not just build this infrastructure, but bring the public along and build something that they have trust and confidence in, and that they see as infrastructure they can rely on, not just from a technical perspective but from a trust and privacy perspective?

I'm sorry, but I don't have a better answer for you.

● (1700)

Dr. Amanda Clarke: I think you're exactly right to note that people sort of want it all.

On this point, I think the committee should be really careful with how it interprets a lot of the data we currently have on citizens' preferences with regard to government data collection and use, because most of these surveys don't actually present the realistic trade-offs to citizens.

You'll find countless surveys that suggest that Canadians are very uncomfortable with certain types of data being collected, used in certain ways and combined with other datasets. There's a line around whether people would want government to collect data and then use it for purposes other than what it was originally collected for. Of course people reply “no” when the situation is presented like that.

We need to move to surveys and studies that, instead, say that data may be used for purposes other than that for which it was collected “if it means that wait times are shorter at hospitals” or “if it means that you could be made aware of all the tax benefits you're not claiming right now that could save you thousands of dollars per year”.

We have to put forward that value proposition, because right now most of our data only asks citizens if, essentially, they want to be surveilled and have their data abused. Everyone's going to say no to that. That's not what we're talking about here. These are really important trade-offs in the efficiency of government and the quality of the services it provides, with questions around data use, some of which are privacy-related but many more of which get into questions of broader governance issues.

I think it's important to be careful with how you're interpreting the data from those surveys because they're actually not very helpful. They would suggest to you that we should not move forward with many of the reforms that we're putting on the table because they essentially say that citizens care only about privacy, and I'm not sure that those surveys actually capture the real trade-off.

Mr. Michel Picard: Sure.

The Chair: Ms. Murray has asked for one question.

Go ahead.

Ms. Joyce Murray (Vancouver Quadra, Lib.): I just want to thank all the panellists.

David, yes, I've been here at this committee meeting. Thank you for your work. I'll see you in Vancouver Quadra before too long.

The Chair: Thank you.

I have one last thing, a bit of committee business. Supplementary estimates (B) were tabled this morning, so I want to ask if it is the will of the room to have the minister appear in the future. I've already talked to Mike here, and there's availability on March 19 or 21. Is there a preference? That's when there are openings.

Hon. Peter Kent: It's common practice.

Mr. Nathaniel Erskine-Smith: I don't care.

The Chair: We'll proceed on that.

With that, I want to thank all the witnesses for coming today. I appreciate your testimony at our committee. Thank you.

The meeting is adjourned.