HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 132 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, January 29, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, January 29, 2019

● (1535)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Good day, everybody. Welcome back—it's 2019—to the Standing Committee on Access to Information, Privacy and Ethics, meeting 132.

Before we get to our guests, we have some committee business. We have a couple of things. It's not necessary to go in camera.

Most of us in this room know about the international grand committee and the work we did in London. Charlie, Nathaniel and I went over in late November to join eight other countries to talk about this. Canada is picking up the torch where they left off. We're going to host it in Ottawa on May 28; that's what we're proposing. We looked at a date that would work for everybody, or as much as we could make that work, and May 28 seems to be the date.

I wanted to put that before the committee to make sure that we have your approval to move forward with it. It will be an all-day meeting, similar to what happened in London. It will start in the morning. We'll have meetings all throughout the day. We'll likely end the day at 4:30. Then we'll proceed into other things.

Mr. Raj Saini (Kitchener Centre, Lib.): What day of the week is that?

The Chair: It's a Tuesday.

Mr. Raj Saini: Okay. Good.

The Chair: I wanted to get some feedback on that. Perhaps you could raise your hand or give me a, “Yes, we're good to go”.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Yes, we're good to go.

The Chair: Nate, you wanted to speak to it. Go ahead.

Mr. Nathaniel Erskine-Smith: To the extent that you need direction from the committee, I would say that your direction as chair is to act on our behalf to make arrangements as necessary to make this happen in Canada, to invite the parliamentarians and the countries that participated in the U.K., at a bare minimum, and if we want to expand it further, to work to do so.

The Chair: Perfect.

Is that enough direction?

Mr. Kent.

Hon. Peter Kent (Thornhill, CPC): Mr. Chair, what are the requirements with regard to the financial support for a meeting like this? Would this have to go to the liaison committee ?

The Chair: It's a good question. There's a limit of about $40,000, so it's keeping it below that. I don't think that will be a problem.

Mike.

The Clerk of the Committee (Mr. Michael MacPherson): Basically, this is what we would be looking for. We would be reimbursing witnesses who appeared at committee just as we would for a regular committee meeting. However, members coming from other jurisdictions, let's say from the House of Commons in England or from Australia or wherever, would be paying their own way to come here, just as we paid our own way to go to the first one.

Hon. Peter Kent: What about for our facility usage?

The Chair: Go ahead, Mike.

The Clerk: We'll be fine. We'll have a budget to cover all that.

Hon. Peter Kent: Good.

The Chair: We'll be working a lot with Mike and the analysts to make sure it all comes to fruition. We want to make it an event that is really the next step in what we've already done. We look forward to it.

Hon. Peter Kent: Yes.

The Chair: Do you have any comments, Mr. Angus?

Mr. Charlie Angus (Timmins—James Bay, NDP): No. We certainly want to move ahead with this, so I say you have the mandate to take the steps necessary. We can come back and discuss the theme and what it is the international community is going to want to talk about. We can do that at a later date.

Mr. Nathaniel Erskine-Smith: Perhaps the analysts can mock up a proposal for us. I only would note that Sheryl Sandberg is on an apology tour; so there you have it.

The Chair: We will keep a list of witnesses and keep you informed about who we're asking to the function. I think that name came up as one that will be on the list.

Do members have anything more to say about the international grand committee? Do we have sufficient direction?

Thank you, everybody. We'll pursue that.

Now we have the notice of motion. We talked a little bit about this.

Mr. Angus, go ahead.

Mr. Charlie Angus: The subcommittee of the committee did meet to talk about direction in terms of taking us over the final few months. We have our study on digital governance. We have a whole bunch of other pieces that we have talked about that actually would fit under the rights of citizens in the age of big data. It could be ethical issues around AI or it could deal with people's financial information and what's happening. I will bring that forward.

Nathaniel said he wanted to look at some of the language. I don't want to take it up today, but I want to put it on the record that we're looking to do this. Some of the questions that we may be asking Dr. Geist or Ms. Cavoukian today, on the larger question of the rights of citizens in the age of big data, may be germane to that as well as what they may want to speak to on the issues of digital governance. We'll have the two studies going in parallel, so some of the evidence may be more germane to one study than another.

I'll bring that back on Thursday.

● (1540)

The Chair: You'll just withhold it for now?

Mr. Charlie Angus: Yes.

The Chair: Thank you, Mr. Angus.

Getting back to the regular agenda, today we welcome two witnesses: as an individual, Dr. Geist, Canada Research Chair in Internet and E-Commerce Law, Faculty of Law, University of Ottawa; and via teleconference, Ann Cavoukian, Privacy by Design Centre of Excellence, Ryerson University.

We'll start off with you, Ms. Cavoukian.

Dr. Ann Cavoukian (Privacy by Design Centre of Excellence, Ryerson University, As an Individual): Thank you very much.

Good afternoon, ladies and gentlemen. It's a pleasure to be here to speak to you today. I've worked with Michael for many years, so it's wonderful to be here with him to speak on these important issues.

What struck me in what you will be doing—I'm just going to read it out—is that your committee is to "undertake a study of digital government services, to understand how the government can improve services for Canadians while also protecting their privacy and security".

That is so vitally important. That's how I want to address something which I created years ago and is called privacy by design, which is all about abandoning the zero-sum models of thinking that prevail in our society. Zero-sum just means that you can only have a positive gain in one area, security, always to the detriment of the other area, privacy, so that the two total to a sum of zero.

That either-or, win-lose model is so dated. What I would like you to embrace today is something called positive sum. Positive sum just means that you can have two positive gains in two areas at the same time. It's a win-win proposition.

It was started years ago. I did my Ph.D. at the U of T when the father of game theory, Anatol Rapoport, was there. We used to discuss this. I always remember saying, "Why do people embrace zero-sum?" I am the eternal optimist. I would much rather deliver multiple wins than an either-or compromise. He said, "It's simple, Ann. Zero-sum is the lazy way out, because it's much easier just to deliver one thing and disregard everything else."

I want you to do more, and I think you want to. You want to deliver privacy and security as well as government improvements that can improve services to Canadians.

My privacy by design framework is predicated on proactively embedding much-needed privacy protective measures into the design of your operations and the design of your policies for whatever new services you want to develop and whatever you want to do in terms of data utility, but we do that along with privacy/security. It's a multiple-win model. It's privacy and data utility services to individuals. You can fill in the blanks, but it's "and" not "versus". It's not one to the exclusion of the other. But how do you do both?

I know that I only have 10 minutes and I've probably used up five, so I'm going to keep the rest short.

In the privacy world, there's a key concept called data minimization. It's all about de-identifying data so that you can benefit from the value of the data to deliver much-needed services in other areas of interest to Canadians and individuals without forfeiting their privacy. When you de-identify personally identifiable data, both the direct and indirect identifiers, then you free the data, if you will, from the privacy restrictions, because privacy issues arise and end with the identifiability of the data. If the data are no longer personally identifiable, then there may be other issues related to the data, but they're not going to be privacy-related issues.

Data minimization and de-identification will drive this goal of having what I call multiple positive gains at the same time, making it a win-win proposition. I think it will make governments more efficient. You will be able to use the data that you have available and you will always be protecting citizens' personal information at the same time. That's absolutely critical.

I am happy to speak more. I can speak on this issue forever, but I want to be respectful of my time restrictions. I will gladly turn it over to you and answer any questions that you may have.

● (1545)

The Chair: Thank you, Ms. Geist. I'm sorry, Ms. Cavoukian. I'm a little ahead of myself.

Voices: Oh, oh!

The Chair: We will move to Dr. Geist for 10 minutes, please.

Dr. Michael Geist (Canada Research Chair in Internet and E-Commerce Law, Faculty of Law, University of Ottawa, As an Individual): All right. Great. I don't think my wife is listening in.

Voices: Oh, oh!

Dr. Michael Geist: Good afternoon, everybody. My name is Michael Geist. I'm a law professor at the University of Ottawa, where I hold the Canada research chair in internet and e-commerce law and am a member of the Centre for Law, Technology and Society.

My areas of speciality include digital policy, intellectual property and privacy. I served for many years on the Privacy Commissioner of Canada's external advisory board. I have been privileged to appear many times before committees on privacy issues, including on PIPEDA, Bill S-4, Bill C-13, the Privacy Act and this committee's review of social and media privacy. I'm also chair of Waterfront Toronto's digital strategy advisory panel, which is actively engaged in the smart city process in Toronto involving Sidewalk Labs. As always, I appear in a personal capacity as an independent academic representing only my own views.

This committee's study on government services and privacy provides an exceptional opportunity to tackle many of the challenges surrounding government services, privacy and technology today. Indeed, I believe what makes this issue so compelling is that it represents a confluence of public sector privacy law, private sector privacy law, data governance and emerging technologies. The Sidewalk Labs issue is a case in point. While it's not about federal government services—it's obviously a municipal project—the debates are fundamentally about the role of the private sector in the delivery of government services, the collection of public data and the oversight or engagement of governments at all levels. For example, the applicable law of that project remains still somewhat uncertain. Is it PIPEDA? Is it the provincial privacy law? Is it both? How do we grapple with some of these new challenges when even determining the applicable law is not a straightforward issue?

My core message today is that looking at government services and privacy requires more than just a narrow examination of what the federal government is doing to deliver the services, assessing the privacy implications and then identifying what rules or regulations could be amended or introduced to better facilitate services that both meet the needs of Canadians and provide them with the privacy and security safeguards they rightly expect.

I believe the government services really of tomorrow will engage a far more complex ecosystem that involves not just the conventional questions of the suitability of the Privacy Act in the digital age. Rather, given the overlap between public and private, between federal, provincial and municipal, and between domestic and foreign, we need a more holistic assessment that recognizes that service delivery in the digital age necessarily implicates more than just one law. These services will involve questions about sharing information across government or governments, the location of data storage, transfer of information across borders, and the use of information by governments and the private sector for data analytics, artificial intelligence and other uses.

In other words, we're talking about the Privacy Act, PIPEDA, trade agreements that feature data localization and data transfer rules, the GDPR, international treaties such as the forthcoming work at the WTO on e-commerce, community data trusts, open government policies, Crown copyright, private sector standards and emerging technologies. It's a complex, challenging and exciting space.

I would be happy to touch on many of those issues during questions, but in the interest of time I will do a slightly deeper dive into the Privacy Act. As this committee knows, that is the foundational statute for government collection and use of personal information. Multiple studies and successive federal privacy commissioners have tried to sound the alarm on the legislation that is viewed as outdated and inadequate. Canadians understandably expect that the privacy rules that govern the collection, use and disclosure of their personal information by the federal government will meet the highest standards. For decades we have failed to meet that standard. As pressure mounts for new uses of data collected by the federal government, the necessity of a “fit for purpose” law increases.

I would like to point to three issues in particular with the federal rules governing privacy and their implications. First is the reporting power. The failure to engage in meaningful Privacy Act reform may be attributable in part to the lack of public awareness of the law and its importance. Privacy commissioners played an important role in educating the public about PIPEDA and broader privacy concerns. The Privacy Act desperately needs a similar mandate for public education and research.

Moreover, the notion of limiting reporting to an annual report reflects really a bygone era. In our current 24-hour social media-driven news cycle, restrictions on the ability to disseminate information—real information, particularly that which touches on the privacy of millions of Canadians—can't be permitted to remain outside the public eye until an annual report can be tabled. Where the commissioner deems it in the public interest, the office must surely have the power to disclose in a timely manner.

● (1550)

Second is limiting collection. The committee has heard repeatedly that the Privacy Act falls woefully short in meeting the standards of a modern privacy act. Indeed, at a time when government is expected to be the model, it instead requires less of itself than it does of the private sector.

A key reform, in my view, is the limiting collection principle, a hallmark of private sector privacy law. The government should similarly be subject to collecting only that information that is strictly necessary for its programs and activities. This is particularly relevant with respect to emerging technologies and artificial intelligence.

The Office of the Privacy Commissioner of Canada, which I know is coming in later this week, recently reported on the use of data analytics and AI in delivering certain programs. The report cited several examples, including Immigration, Refugees and Citizenship Canada's temporary resident visa predictive analytics pilot project, which uses predictive analytics and automated decision-making as part of the visa approval process; the CBSA's use of advanced analytics in its national targeting program with passenger data involving air travellers arriving in Canada; and the Canada Revenue Agency's increasing use of analytics to sort, categorize and match taxpayer information against perceived indicators of risks of fraud.

These technologies obviously offer great potential, but they also may encourage greater collection, sharing and linkage of data. That requires robust privacy impact assessments and considerations of the privacy cost benefits.

Finally, we have data breaches and transparency. Breach disclosure legislation, as I'm sure you know, has become commonplace in the private sector privacy world and it has long been clear that similar disclosure requirements are needed within the Privacy Act. Despite its importance, it took more than a decade in Canada to pass and implement data breach disclosure rules for the private sector, and as long as that took, we're still waiting for the equivalent at the federal government level.

Again, as this committee knows, data indicate that hundreds of thousands of Canadians have been affected by breaches of their private information. The rate of reporting of those breaches remains low. If the public is to trust the safety and security of their personal information, there is a clear need for mandated breach disclosure rules within government.

Closely related to the issue of data breaches are broader rules and policies around transparency. In a sense, the policy objective is to foster public confidence in the collection, use and disclosure of their information by adopting transparent open approaches with respect to policy safeguards and identifying instances where we fall short.

Where there has been a recent emphasis on private sector transparency reporting, large Internet companies, such as Google and Twitter, have released transparency reports. They've been joined by some of Canada's leading communications companies such as Rogers and Telus. Remarkably, though, there are still some holdouts. For example, Bell, the largest player of all, still does not release a transparency report in 2019.

Those reports, though, still represent just one side of the story. Public awareness of the world of requests and disclosures would be even better informed if governments would also release transparency reports. These need not implicate active investigations, but there's little reason that government not be subject to the same kind of expectations on transparency as the private sector.

Ultimately, we need rules that foster public confidence in government services by ensuring there are adequate safeguards and transparency and reporting mechanisms to give the public the information it needs about the status of their data and appropriate levels of access so the benefits of government services can be maximized.

None of that is new. What may be new is that this needs to happen in an environment of changing technologies, global information flows and an increasingly blurry line between public and private in service delivery.

I look forward to your questions.

The Chair: Thank you, Dr. Cavoukian and Dr. Geist.

We'll start off with Mr. Saini for seven minutes.

Mr. Raj Saini: Good afternoon, Ms. Cavoukian and Dr. Geist. It's always a pleasure to have esteemed eminent experts here. I will do my best to keep my questions succinct.

Dr. Geist, in one of the things you brought up, you talked about the different levels of government. I come from a region of the country that has four levels of government: federal, provincial, regional and municipal. In the model we looked at earlier, the Estonian model, they have what they call a once-only principle, where there is one touch and all the information is disseminated, albeit Estonia is a small country and probably has only two levels of government. In some cases, we have three or four.

How do we protect Canadians' privacy? Each level of government has a different function and a different responsibility. Rather than giving all the information once to the federal government, then the provincial government, then the regional government and then the municipal government—and that information, as you know, can be shared, whether it be tax records, health records or criminal records—how can we have a way of protecting Canadians' privacy but also making our government services more efficient?

● (1555)

Dr. Michael Geist: You raise an interesting point. In some ways it highlights—and Ann will recall this and I'm sure may have comments—that when we were setting out to create private sector privacy law in Canada at the federal level, we were in a sense grappling with much the same question: How do we ensure that all Canadians have the same level of privacy laws regardless of where they happen to live and which level of government they're thinking about?

The sad reality is that decades later, the answer is they don't, and they still don't. We can certainly think about whether there are mechanisms we can find through which governments can more actively work together with respect to these issues. I think if we're candid about it, though, the reality is that provinces have taken different approaches with respect to some of these privacy rules, and that's just one other layer of government. Quebec's private sector privacy law predated the federal law. A couple of provinces have tried to establish similar kinds of laws. Other provinces have done it on a more subject-specific basis. The mechanism within PIPEDA that we use for that is to see whether the law is substantially similar, but the practical reality is that there are still many Canadians in many situations who don't, practically speaking, have privacy protections today because they don't have provincial laws that have filled those gaps. That's not even getting into the other layers you've talked about. It's a thorny constitutional issue and it is also one that raises really different questions around some of the substance as well.

Mr. Raj Saini: Ms. Cavoukian, the next question is for you.

Some of the benchmarks of the Estonian model were that there had to be the once-only principle; they had to have a strong digital identity, but also more importantly, there had to be interoperability between different government departments. The way they structured it was to have not one singular database but different databases that held very specific and particular information that could be accessed. Their infrastructure is called X-Road. Is that a model we should be pursuing?

Also, what is the benefit or disadvantage of having data spread out? There are certain advantages, but there are also certain disadvantages. What would be the advantage or disadvantage of having that data spread out and, more importantly, of making it easier for Canadians to access the information they need?

Dr. Ann Cavoukian: I think it's an excellent model and it's one you're going to be seeing more of. It's called a model of decentralization, in which all the data isn't housed in one central database that different arms of government can access. The problem with centralization is that it is subject to far greater risk in terms of data breaches, privacy infractions, unauthorized access to the data by curious employees, inside jobs and all of that. All of the data is placed at far greater risk if it's in one central location.

You may recall about six months ago that Tim Berners-Lee, who created the World Wide Web, was aghast and said he was horrified at what he'd created because it is a centralized model that everyone can basically break into more easily and access everyone's data in an unauthorized manner. Centralization also lends itself to surveillance and tracking of citizens' activities and movements. It is fraught with problems from a privacy and security perspective.

In Estonia, the decentralized model is superior, with different pots of information. Each database contains information that can be accessed for a particular purpose. Often that's referred to as the primary purpose of the data collection, and individuals within the government are limited as to the uses of the data. They have to use the data for the intended purposes. The more you have decentralized pots of information the greater the likelihood the data will remain and will be retained for the purposes intended and not used across the board for a variety of purposes that were never contemplated.

You have far greater control and people, citizens, can be assured of a greater level of privacy and security associated with that data. It's a model that is proliferating and you're going to see much more of it in the future. It doesn't mean that other arms of government can't access it. They just can't automatically access it and do whatever they want with it.

● (1600)

Mr. Raj Saini: That's great. Thank you.

I have one final question, Dr. Geist. You mentioned that there will be an interface or nexus between the private sector and the public sector. Obviously the two different sectors are governed by two different privacy regimes. More importantly, when we look at the Estonian model, we look at blockchain technology. It's a technology that's safe and accountable.

If you're going to have two different systems, the public sector and the private sector, the technology has to be equal. As we know, sometimes the private sector technology is greater than the public sector technology. How do we get both to change to make sure there's accountability and that the interface will work efficiently for the citizen?

Dr. Michael Geist: I see accountability as being a legal principle and not a technological one, and that speaks to the accountability of the information that gets collected.

In terms of ensuring that both public and private are using best of breed security, for example, I think we've seen some of the mechanisms, at least in the public sector where we can try to do that, with the government's efforts to try to embrace different cloud computing services. It's a good illustration of how the government has recognized that cloud may offer certain concerns around where the data is stored and those kinds of localization issues, but it also may offer, depending on the provider, some of the best security mechanisms with regard to where that data's being stored. So how do you get the benefits of that, while at the same time creating some of the safeguards that may be necessary? We've seen some efforts in that regard.

Some of that comes down to identifying different kinds of data or perhaps, especially at the federal government level, different kinds of rules for different kinds of data. I think it does require an openness to blurring those lines sometimes, within the context of recognizing that we still need to ensure that Canadian rules are applicable.

The Chair: Thank you, Mr. Saini.

Next is Mr. Kent for seven minutes.

Hon. Peter Kent: Thank you, Mr. Chair.

Thank you both for attending before this committee.

The study of digital government is a huge topic. We began it last year and then back-burnered it, because of the Cambridge Analytica, Facebook and AggregateIQ study.

I was fascinated when I spent some time last year with Prime Minister Juri Ratas of Estonia. He showed me the card, the chip it contains and the fact that it's basically cradle-to-grave data. They've had a couple of breaches and glitches with their chip manufacturer, but it's a fascinating concept.

I'd like to ask both of you this. Whereas the Estonian digital government model is built on a fledgling democracy after the collapse of the Soviet Union, with a still compliant society that accepted the decision of its new government leaders to democratically impose this new digital government on the population, in our context, our wonderful Canadian Confederation has had, through 150 plus years, democratic challenges to government, with skepticism and cynicism in many ways, with regard to significant changes in government and referenda on any number of issues. I'm just wondering, for any government, whether federal, provincial, regional or municipal, in any of the contexts, how practical the pursuit of a single card with a chip à la Estonia is for Canada and Canadians.

Dr. Cavoukian, would you like to go first?

Dr. Ann Cavoukian: Forgive me; I was shaking my head. Estonia is highly respected, no question. I personally would not want to go with one card with one chip that contained all your data. That's a centralized model that is just going to be so problematic, in my view, not only now but especially in the future.

There are so many developments. You may have heard of what's happening in Australia. They've just passed a law that allows the government there to have a back door into encrypted communications. Why do you encrypt communications? You want them to be secure and untouched by the government or by third parties, unauthorized parties. Australia has passed a law that allows it to gain back-door access into your encrypted communications and you won't know about it. No one can tell you about it. It is appalling to me.

Personally, I am not in favour of one identity card, one chip, one anything.

Having said that, I think we have to go beyond the existing laws to protect our data and find new models, and I say this with great respect. I was privacy commissioner of Ontario for three terms, 17 years. Of course we had many laws here and I was very respectful of them, but they were never enough. It's too little too late. Laws always seem to lag behind emerging technologies and developments. That's why I developed privacy by design. I wanted a proactive means of preventing the harms from arising, much like a medical model of prevention. Privacy by design was unanimously passed as an international standard in 2010. It has been translated into 40 languages and it has just been included in the latest law that came into effect last year in the European Union called the General Data Protection Regulation. It has privacy by design in it.

The reason I'm pointing to this is that there are things we can do to protect data, to ensure access to the data, digital access by governments when needed, but not across the board, and not create a model of surveillance in which it's all in one place, an identity card, that can be accessed by the government or by law enforcement.

You might say that the police won't access it unless they have a warrant. Regrettably, to that I have to say nonsense. That's not true. We have examples of how the RCMP, for example, has created what are called Stingrays. These impersonate cellphone towers so they can access the cellphone communications of everyone in a given area when they're looking for the bad guy. Of course, if they have a warrant, I'd say to them, “Be my guest, by all means. Go search for him.” Did they have a warrant? No. They did this without anyone knowing, but CBC outed them, and they finally had to come clean that they were doing this.

With the greatest of respect and not to say anything negative about Estonia, that's not the direction I would want us to take here, one of greater centralization. I would avoid that.

● (1605)

Hon. Peter Kent: Thank you.

Dr. Geist.

Dr. Michael Geist: Ann has raised a number of really important issues, especially around that issue of centralization.

I couldn't help, as you were talking about that, thinking about the experience so far on the digital strategy advisory panel for Waterfront Toronto, which I must admit has been more than I bargained for. As chair of that panel for the past year—

Hon. Peter Kent: I'm sure we'll get to that.

Dr. Michael Geist: I have to say when you take a look at that, that isn't a single identity card. That is taking a relatively small piece of land and wanting to embed some of the kinds of technologies, emerging technologies, that allow for smart government. Both the controversy that has arisen in association with it, and even more, just the kind of public discussion around what we're comfortable with, which vendors we're comfortable with and what role we want government to play in all of this highlight some of the real challenges. That's in a sense a small pilot project for some of the smart city technologies. Talking about a single card for all data to me is a force multiplier behind that which raises a whole series of issues in our environment.

Hon. Peter Kent: I'm sure in the two hours the committee will get back to the larger digital government question, but to come back to Sidewalk Labs, there's a bit of a David and Goliath situation in Sidewalk Labs, given the way Alphabet, the parent company to Google, has been dictating its dealings with the city and the other potential partners. Dr. Cavoukian's departure would speak to that, I would think.

Dr. Michael Geist: Sure, she departed from her position as an adviser to Sidewalk Labs. My role has been on the advisory panel to Waterfront Toronto, and I still feel that it's early days in terms of trying to identify precisely what the final development project looks like and whether it gets approved. That's really what this advisory panel is all about: trying to better understand what kinds of technology are being proposed, what sort of data governance we have around the intellectual property and privacy, and ensuring that the terms are not dictated but rather better reflect what the community is thinking about.

● (1610)

The Chair: Thank you, Mr. Kent.

Next up is Mr. Angus for seven minutes.

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

I would certainly like to begin with a discussion of Sidewalk Labs, because it's a very interesting proposal and it's certainly been fraught with a number of questions.

Dr. Cavoukian, your decision to step down from Sidewalk Labs raised a lot of eyebrows and a lot of questions. Can you explain why you felt that you no longer wanted to be part of this project?

Dr. Ann Cavoukian: I didn't resign lightly. I want to assure you of that.

Sidewalk Labs retained me as a consultant to embed privacy by design—my baby, which I've been talking to you about—into the smart city they envisioned. I said, "I'd be very pleased to do that, but know that I could be a thorn in your side, because that will be the highest level of privacy, and in order to have privacy in a smart city...". In a smart city, you're going to have technologies on 24-7, with sensors and everything always on. There's no opportunity for citizens to consent to the collection of their data or not. It's always on.

I said that in that model we must de-identify data at source, always, meaning that when the sensor collects your data—your car, yourself, whatever—you remove all personal identifiers, both direct and indirect, from the data. That way, you free the data from privacy considerations. You still have to decide who's going to do what with the data. There are a lot of issues, but they're not going to be privacy-related issues.

I didn't have any push-back from them, believe it or not. I didn't. They agreed to those terms. I said that to them right at the initial hiring.

What happened was that they were criticized by a number of parties in terms of the data governance and who was going to control the uses of the data, the massive amounts of data. Who will exercise control? It shouldn't just be Sidewalk Labs.

They responded to that by saying they were going to create something called a civic data trust, which would consist of themselves and members of various governments—municipal, provincial, etc.—and various IP companies were going to be involved in the creation of it. But they said, "We can't guarantee that they're all going to de-identify data at source. We'll encourage them to do that, but we can't give any assurance of that."

When I heard that, I knew I had to step down. This was done at a board meeting in the fall. I can't remember when. Michael will remember. The next morning, right after the meeting, I issued my resignation, and the reason was this: The minute you leave this as a matter of choice on the part of companies, it's not going to happen. Someone will say, "No, we're not going to de-identify the data at source."

Personally identifiable data has enormous value. That's the treasure trove. Everybody wants it in an identifiable form. You basically have to say what I said to Waterfront Toronto afterwards. They called me, of course, right after my resignation, and I said to them, "You have to lay down the law. If there is a civic data trust, or whoever is involved in this, I don't care, but you have to tell them that they must de-identify data at source, full stop. Those are the terms of the agreement." I didn't get any push-back from Waterfront Toronto.

That's why I left Sidewalk Labs. I'm now working for Waterfront Toronto to move this forward, because they agree with me that we need to de-identify data at source and protect privacy. You see, I wanted us to have a smart city of privacy, not a smart city of surveillance. I'm on the international council of smart cities—smart cities all around the world—and virtually all of them are smart cities of surveillance. Think of Dubai, Shanghai and other jurisdictions. There is no privacy in them. I wanted us to step up and show that you can create a smart city of privacy. I still believe we can do that.

Mr. Charlie Angus: Thank you. I want to step in here.

One of the concerns I've been hearing from citizens in Toronto is about the need not just for privacy by design but democratic engagement by design; if this is a city, they're citizens' public spaces. We have a problem. We have a provincial government that is at war with the City of Toronto and has trashed a number of councillors, so there's a democratic deficit. We see Waterfront Toronto in an in-between place with a province that may be against it. We see the federal government continually dealing with this through Google lobbyists, so there are a lot of backroom dealings.

Where is the role for citizens to have engagement? If we're going to move forward, we need to have democratic voices to identify what is public, what is private, what should be protected and what is open. In terms of the other big players, we're dealing with the largest data machine company in the universe, which makes its money collecting people's data, and they're the ones who are designing all of this.

I'd like to ask you that, Dr. Cavoukian—I don't have much time, maybe one minute—and then Dr. Geist. Then maybe we'll get another round on this.

● (1615)

Dr. Ann Cavoukian: I want to make sure I leave time for Michael.

We need enormous transparency on exactly who's doing what and how this information is being disseminated in terms of the data and the decisions being made on the part of the various levels of government you talked about that always seem to be at each other. I'm not here to defend government, because there has to be a way that there can be an interplay in which citizens are allowed to participate and have an understanding of what the heck is going on. That is absolutely essential. I'm not suggesting that's not important; I just think we should be focusing on the privacy issues to at least make sure that privacy is addressed.

Mr. Charlie Angus: Dr. Geist, what are your thoughts?

Dr. Michael Geist: I could really just comment on the role that my panel has been playing. All our meetings are open. The materials are made publicly available. In fact, we've learned about some of Sidewalk's plans from a technological perspective. They have come via the panel as they present to us. Anyone can attend those meetings. Those meetings are actively recorded. In fact, someone shows up to each meeting and records it themselves and then posts it to YouTube. There have been additional meetings. We have a meeting at MaRS next month that deals specifically with civic trusts.

This notion that there aren't avenues or there isn't public discussion taking place, I must admit with respect, is at odds with my experience in the year or so to date that I've been there, where literally anyone in Toronto can come out to any meeting they want.

Mr. Charlie Angus: Dr. Geist, with respect—and I've had this from Google—they tell me that people are frustrated because Google wants to talk about how much wood is being used in the building. Come on. Eric Schmidt cares about wood products in Toronto? They're talking about data. That's what people tell me. They come out of this and they're not getting answers.

Dr. Michael Geist: That's precisely what we talk about at our committee. We spend our time talking about data governance issues, privacy issues, IP issues. In fact, we try to identify what the technologies are that they say they're going to put into place and what the implications are for IP, for privacy, for data governance. For example, the proposal for a civic trust came first to our panel.

As I say, could more be done? I'm sure it could, but I can say from my own perspective, from where I sit, that I see the media coming. I see citizens showing up. I see blog posts and otherwise coming out of that. All of this is taking place completely in the open.

The Chair: Thank you, Mr. Angus.

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

Mr. Nathaniel Erskine-Smith: Thank you very much.

Thank you both for attending.

To begin I want to clarify a bit of a misconception in some of the questions from Mr. Kent with respect to the e-ID in Estonia. It is not a mini computer that centralizes all personal information. In fact, the very foundation of the Estonian digital government is decentralization. The digital ID is an identity card that allows them to access the system, but it's not storing mountains of personal information.

What I really want to get at, and I think the usefulness of this study, is to ask how we can apply the idea of privacy by design to digital government so that we can actually improve services for Canadians.

At the outset I would note that according to Estonia's public information, nearly 5,000 separate e-services enable people to run their daily errands without having to get off their computer at home. As a Canadian who wants better service out of his government, I want that. How do we alleviate privacy concerns from the get-go so we get better service?

If we look at the Estonian model, we have a digital ID. We have a separation of information between departments using X-Road and blockchain technology. Then we have transparency in the sense that when a government employee accesses my information, I can see who did it and it's time-stamped as to when they did it. If you add those layers of detail into a digital government system, is that sufficient to address privacy concerns? Are there other things we should be doing if we're looking to digital government?

I'll start with Dr. Cavoukian and then Dr. Geist.

Dr. Ann Cavoukian: You have a number of elements that are very positive in what you've described in terms of the transparency associated with each service that's provided and the ease of access to this online by citizens.

I want to make one comment about blockchain. Let us not assume that blockchain is this great anonymous technology. It's not. It has benefits, but it also may have negatives. It's also been hacked. I'm going to read one very short sentence that came out from a text on the GDPR. GDPR is this new law that came into effect in the European Union. They said, “Especially with blockchain, there is no alternative to implementing privacy by design from the start, as the usual add-on privacy and enhancements simply will not satisfy the requirements of the GDPR.” GDPR has raised the bar on privacy dramatically. They're saying, “Sure, use blockchain, but don't do it without privacy by design because you have to make sure privacy is embedded into the blockchain.” There are some companies, like Enigma, that do it beautifully. They have an additional privacy layer.

I just want us to be careful not to embrace blockchain and other technologies without really looking under the hood and seeing what's happening in terms of privacy.

● (1620)

Mr. Nathaniel Erskine-Smith: My understanding is that in Estonia they were using this technology before it was called blockchain, but it was in 2002 that they implemented a system. The idea is that when they use blockchain as a technology, it's actually when information is being transferred as between departments on a back end. As a citizen, I log on and it's one portal for me, but on the back end, my information is housed in a number of different departments. If they want to share information, those pathways are only open by way of blockchain to ensure that it's private. If I'm at the CBSA, I can't see information that is at employment services... but duly noted on the blockchain concern.

With respect to, I guess, my fundamental question.... I have more specific questions, but this is the broad question. If we build in a digital ID, if we build in anonymization as between departments when they're sharing information and I can log on it and have user control of my information, if those are the three fundamental building blocks of this, am I missing something? Am I missing something else?

Dr. Ann Cavoukian: It sounds very positive. You're going to have security embedded in [*Technical difficulty—Editor*]

Mr. Nathaniel Erskine-Smith: The digital ID is itself an encryption device, exactly.

Dr. Ann Cavoukian: Yes.

Mr. Nathaniel Erskine-Smith: As I understand it, in Estonia it's itself a microprocessor and it's an encryption device, so it verifies my identity.

By the way, on Estonia, the biggest sales pitch—and I know Mr. Kent might have been worried about it—when they came to our committee was that they said there's been no identity theft since they implemented this system—no identity theft. Why? Because if they lose the digital ID, the certificate can easily be revoked, so nobody can use that digital ID to access services in faking to be someone else.

If those are the three building blocks, and if you don't have a clear answer to any...and you say those all sound positive, the overarching question is, are there other layers we should be building in to make sure we have privacy by design built into digital government services, as Estonia does it? Is Estonia missing something or should we do what Estonia does?

Dr. Ann Cavoukian: Estonia is very, very positive—

Mr. Nathaniel Erskine-Smith: The—

Dr. Michael Geist: If I could respond, I'm not going to speak specifically to Estonia, but I will say that there are two elements to it. When you're a hammer, everything looks like a nail, and when you're a law professor, everything looks like a legal issue. In terms of describing largely technological standards and saying that's how we're going to effectively preserve.... I understand why that has a great deal of appeal, but my view would be that you need a commensurate law in place as well.

The other thing is that one of my other issues that I focus on is access, of course, so what else do you need? You need to ensure that all Canadians have access to the network if we're going to be able to embrace these kinds of services. We still find ourselves with too many Canadians who do not have affordable Internet access. We need to recognize that part of any conversation about asking how we can provide these kinds of services to Canadians must include how we ensure that all Canadians have affordable access.

Mr. Nathaniel Erskine-Smith: I appreciate those comments.

Because I'm running out of time, the last question I have is about data minimization. On the one hand, Estonia I think generally adopts this rule, but when we look at government services, we might say in the same way companies do that more data is better to deliver better services for consumers. As a government, we say that more data in certain instances is better. I want to use one example.

Very few Canadians take up the Canada learning bond. Everyone is eligible for the Canada child benefit because it's automatic, provided they file their taxes. Now, if we know who all the individuals are who have received the Canada child benefit, we also know that they're eligible for the Canada learning bond. By using that kind of information to proactively reach out to citizens to say, “Hey, by the way, there's free money here for your kid's education that you are eligible for, so please apply if you haven't applied”, we are having to use their information, ideally to improve services. Are there risks here that I should be worried about?

● (1625)

Dr. Ann Cavoukian: I don't think more data is better at all.

The example you give is a very worthwhile one. You want to reach out to people, but there are so many risks in using data for purposes never intended. Theoretically, we give data to the government for a particular purpose. We pay our taxes or we do whatever. That's the intent. It's the primary purpose of the data collection. The intention is that you're supposed to use that data for that purpose and limit your use of data to that unless you have the additional consent of the data subject, the citizen.

The minute you start deviating for what you might think is the greater good, and that it's better for them if you have access to all their data and can send them additional services or information.... They may not want you to do that. They may not want.... Privacy is all about control: personal control relating to the uses of your information. The minute you start stretching that out because you think—I don't mean you personally—the government knows better, that's going to take you down the path of surveillance and tracking, which is the completely wrong way to go. I say that with great respect, because I know you mean well here, but I would not go.... Plus, when you have data at rest, massive amounts of data at rest, it's a treasure trove.

The Chair: Thank you, Dr. Cavoukian—

Dr. Ann Cavoukian: It's a treasure trove for hackers. People are going to hack into that data. It's just going to be a magnet for the bad guys.

The Chair: Thank you.

We have votes coming up at 5:30 p.m., and we have a bit of committee business that I have to take in camera for about five minutes, so I would look to be done at about 4:50 p.m., if that's possible.

We'll go to Mr. Gourde for five minutes.

[*Translation*]

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

Thank you to the witnesses for being here today.

My question is very simple: can the Estonian model be applied in Canada, given our challenges, the various levels of governance and of access to the Internet on such a vast territory?

There are regions of Canada that are not connected. If we choose this, we will have to provide Canadians with two levels of service, to take those who have no access into account. Is it really worth it?

Ms. Cavoukian, you may answer first.

[*English*]

Dr. Ann Cavoukian: Improving service levels to citizens is, of course, extremely important and not everyone, as [*Technical difficulty—Editor*], has equal access to the Internet and different levels of technology. I think improving services to individuals, to citizens, is a very valid pursuit. It's the means by which you do it. This is always the question mark that arises. How do you reach out to individuals and direct more services in their direction without invading their privacy, without looking into what additional needs they may have? If they provide you with that information, then by all means, that's wonderful. That's positive consent. You can then direct additional services to them. But I don't want the government fishing into the data they already have about citizens to find out if some additional services might be of value to them.

I think you need to ask citizens if they would like to pursue these additional services, and then by all means direct them to work with you, etc. I don't think we should do it by means of digging into drifting databases of information on our citizens.

Dr. Michael Geist: I'm glad you raised again the issue of access. As I've been writing for some time, I've long believed that one of the real reasons that governments.... This is not a partisan issue at all. We've had successive governments struggle with this issue. One of the reasons that there's a need to make real investments in ensuring universal, affordable access is that the cost savings in being able to shift to more and more e-services from a government perspective, I believe, depends upon ensuring that you have universal, affordable access.

Until you reach that point, I think you're quite right that you basically have to run parallel service sets to ensure that everybody does have access. You can't have certain kinds of government services that some people are effectively excluded from being able to access because they don't have access to the network. It makes sense to invest where the private sector has been unwilling to do so, and for a myriad of reasons. One of them is that there is a payoff from a government perspective, because I think it better facilitates the shift to some of those more efficient electronic services.

We are clearly not there yet. Studies repeatedly have found that we do not have universal, affordable access on the broadband side, and on the wireless side we continue to pay some of the highest wireless fees in the world. That tells us that we continue to have a significant policy problem when it comes to affordable communications in Canada.

● (1630)

[*Translation*]

Mr. Jacques Gourde: My last question is also quite simple.

Do we have the required level of programming expertise in Canada? I believe the industry is experiencing a crisis, a shortage of programmers. We have to look outside Canada. It seems that finding very competent people is quite complicated. The new generation does not seem to like this kind of work.

Would it be difficult to implement such services for and by Canadians?

[*English*]

Dr. Michael Geist: Well, speaking as a proud father of two kids who are doing engineering at the University of Waterloo, I'm not so sure that's true. I think we do see a lot of people increasingly move in that direction. When I take a look at my own campus at the University of Ottawa, and frankly at campuses across the country, there is an enormous interest in the STEM fields and the like. If there is a shortage of that expertise, I think it only serves to highlight just how in demand these skills are. It's not that we don't have people developing and moving into that area. I think we unquestionably do.

Dr. Ann Cavoukian: I agree with Michael. I think we have very strong resources here in Canada. Perhaps they will be insufficient in the future, but certainly in terms of the younger generation, I mentor a lot of students and I always tell them, "Make sure you learn how to code." You don't have to become a coder, but learn how the technology works. Learn how you can use various coding techniques to advance your interests in completely different areas, etc. The fundamentals are associated with understanding some of the emerging technology. I think that's pretty widely accepted now.

The Chair: Thank you, Monsieur Gourde.

Next up is Mr. Baylis for five minutes.

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

I'd like first of all to follow up on a bit of clarification that Nate did with respect to what Peter was asking in regard to Estonia. I think that's the foundation. If we're going to go to a digital government, we need a digital identity.

Are you in agreement with that, Ms. Cavoukian, or do you have a concern with starting off with a digital identity?

Dr. Ann Cavoukian: Forgive me, but I'm going to say it depends, because it depends on how it's constructed.

A digital identity, if it's strongly protected and is unique and encrypted and has very restrained access, may facilitate greater access to services, etc., but identity theft is huge. It's the fastest-growing form of consumer fraud ever. If you have a digital identity, that can also be subject—

Mr. Frank Baylis: Yes, but the new digital identities have biometrics. In the end, you can never stop a thief, but for someone finding my number, my SIN, say, versus finding that I have a properly encrypted digital identity that has biometrics and my eye scan and all of this, the likelihood of them stealing that is an order of magnitude less than what they can do today. I would say that —

Dr. Ann Cavoukian: As long as the biometric is a strong biometric or uses biometric encryption, which encrypts the data automatically in a way that only the individual with their own biometric can decrypt it.... Unfortunately, there's a lot of association of biometrics with risk, so it's not a slam dunk that your biometrics are linked to your digital identity. You have to use biometric encryption and you have to ensure that it's properly kept. It's not that I'm disagreeing with you, sir. I'm just saying that the devil is all in the detail, and that's what we have to answer here.

Mr. Frank Baylis: I understand.

Would you like to weigh in on that, Dr. Geist?

Dr. Michael Geist: Yes. I guess I would use the opportunity to again reiterate that for me the policy frameworks around the technology are in some instances just as important as the technology itself. Even in the way you phrased your question, you made a compelling case for why those technologies—

Mr. Frank Baylis: Let's assume that we're going to use the latest technology. The latest technology has all these things built into it—

Dr. Michael Geist: Precisely.

Mr. Frank Baylis: —versus, say, my social insurance number. If I give it to you today, it's done.

Dr. Michael Geist: I get that, so that notion of using best of breed technology makes a whole lot of sense, but there is still a full policy layer that comes around that. I think there certainly will be many who will voice some amount of concern given that our previous experience is that sometimes there are assurances that we are going to use certain kinds of encryption or other sorts of technologies, so "don't you worry, there will be no access". Until you come across a particular use case where you say it would be really great if law enforcement had access just under this circumstance or under that circumstance—

● (1635)

Mr. Frank Baylis: I think I understand. We're skating a little further ahead.

Let's say we start today. Estonia's benefit is that they were a new country and they were starting fresh, so they wouldn't have to convert. They're a small country with a small number of people, relatively speaking. Let's say we start today. It seems to me that the first step we have to do.... I agree with Ms. Cavoukian that we can keep the silos, and I agree that it's the safer approach. What Estonia does is they have a backbone so you can come in and go here or you can come in and go there, but it's not all one big database.

I also believe it will be a lot easier to build out from our existing silos, as opposed to trying to do it.... I'm in agreement with that, but it seems to me that if we're going to do it, we have to start off with a digital link, okay? Let's say I'm Frank Baylis and I just showed up on the system. “Okay,” it says, “prove to me you're Frank Baylis.” Right now, it says to type in my SIN, that number, and that's pretty easy to rip off, right? Whereas if it says, “Let's get a scan of your eyes” or “Let's get some biometrics” and some questions asked and all of that, it seems to me that, to your point, you could have privacy and security.

I think that was the first statement you made, Ms. Cavoukian. Can we not start there and have an agreement on that before we get into all the other stuff?

I'll pass it back. I cut you off. I'm sorry.

Dr. Michael Geist: At the risk of saying that this is a chicken or egg kind of issue, I'm not comfortable giving you my biometric information unless we have a legal and privacy framework established in Canada that meets current privacy standards.

Mr. Frank Baylis: Okay, so you're saying that before we get there, before we start down that path, we better be darn sure that the privacy is just locked hard.

Dr. Michael Geist: It's not just a matter of locked hard. We have a decades-old set of rules that effectively apply to that system.

Mr. Frank Baylis: It doesn't work.

Dr. Michael Geist: I don't think you can make an argument to say we're as modern and as digital as can be while using 1980s laws that provide the safeguards around the system that you've just created.

Mr. Frank Baylis: Do you want to weigh in, or am I out of time?

The Chair: If she can answer in 20 seconds that would be great.

Dr. Ann Cavoukian: I just want to say, Mr. Baylis, that I agree with you. We have to explore these new technologies. There's no question. We just have to ensure that in addition to what Michael said, we have to update our laws. They're so dated. We have to ensure the technology is such that we can truly safeguard the information and it won't be accessed by others.

I gave the example of biometric encryption. There's now a lot of concern about facial recognition technologies that are happening everywhere, obtaining your facial recognition, and using it for purposes never intended. I'm working with an amazing company out of Israel, an Israeli company called D-ID, which can actually obscure the personal identifier so it's not picked up by facial recognition.

There are a number of complexities. I'm sure we could address them as long as we address them up front, proactively, to prevent the harms from arising.

The Chair: Thank you, Mr. Baylis.

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

Hon. Peter Kent: Thank you very much, Chair.

This is a very interesting conversation. I apologize that votes are going to cut it short. You may anticipate being recalled, both of you, in the days and months ahead.

This committee has recommended to government in a couple of reports now that the General Data Protection Regulation be examined and that Canadian privacy regulations across the board and the Privacy Commissioner's powers be greatly strengthened and contemporized.

I wonder, just in the final few minutes we have, if you could offer cautions. I'm hearing signals from the government side that digital government is coming down the track: Stand back; it's about to be presented in some form or another. I wonder if you could both offer cautions to the government before they get too far down this track.

Dr. Cavoukian.

Dr. Ann Cavoukian: I totally support Commissioner Daniel Therrien's call to the federal government to upgrade the PIPEDA, for example, which dates from the early 2000s. He also said we need to add privacy by design to the new law because, after all, they have embedded it in the GDPR. We need new tools. We need to be proactive. We need to identify the risks and address them up front. We can do this.

Upgrading the laws is absolutely essential. Giving the commissioner the much-needed authority that he needs but now lacks is essential. I can say, having been a privacy commissioner for three terms, that I had order-making power. I rarely used it, but that was the stick that enabled me to engage in informal resolution with organizations, government departments that were in breach of the privacy law. It was a much better way to work.

I had the stick. If I had to issue an order, I could do that. That's what Commissioner Therrien lacks. We have to give him that additional authority and embed privacy by design into the new law so we can have additional measures available to the government to proactively address a prevention model, much like a medical model of prevention. It would be much easier if we had that. Then far less would go to the already extended Privacy Commissioner to be addressed.

Thank you.

● (1640)

Hon. Peter Kent: Dr. Geist.

Dr. Michael Geist: I would like to start by commending this committee for the reports it has put out over the last year or so, which I think have been really, really strong and have helped fuel a lot of the public discussion in this area. I think it's been really valuable.

I would say that I don't know what the government is thinking on this. I do know that they have held a consultation on a national data strategy. I guess in some ways I'm waiting to see what comes out of that. To me a national data strategy, to harken back to my comments off the top, really, if they take a holistic approach that recognizes that part of what you're dealing with in that context, includes data governance-related issues, PIPEDA-related issues, private sector-, public sector-, and Privacy Act-related issues including some of the enforcement types of issues that have been raised repeatedly by the Privacy Commissioner. That tells me there's a recognition that it's critically important to get that piece right for any number of reasons, including the prospect of trying to embrace some of the e-services that the government might want to move toward.

Hon. Peter Kent: How critical is consent in that process?

Dr. Michael Geist: Consent has long been viewed as a bedrock principle. I think one of the reasons we really struggle with some of these issues comes back to Mr. Erskine-Smith's question about why we can't find a way to inform someone and I think try to do good with that prospect. Part of the problem is that in theory we might ask if we can find a mechanism for our citizens to provide consent to allow the service provider, in this case the government, to inform them about the services they're eligible for. I would say that our standards of consent have become so polluted by the low standards found in PIPEDA, which I think have been widely abused, that few people actually trust what consent means at this stage.

One of the things I think we have to seize back is to try to find mechanisms to ensure that meaningful consent is truly meaningful, informed consent. We have strayed badly in that regard. It's possible that the GDPR will be part of the impetus for trying to do that.

The Chair: You have 30 seconds, Mr. Kent.

Hon. Peter Kent: Dr. Cavoukian.

Dr. Ann Cavoukian: I couldn't agree more with Michael. He's absolutely right that the notion of consent is almost non-existent the way it's been whittled down.

You see, consent is essential to control. Privacy is all about personal control over the uses of your data. If you're not consenting to it in a positive way, with positive, affirmative consent, you don't know what's happening with your data. As for expecting people to search through all the legalese in the terms of service and the privacy policy to find the opt-out clause to say no to additional uses of these data and negative consent, life is too short. No one does that, but it's not because they don't care deeply about privacy.

In the last two years, all of the public opinion poll surveys from Pew Internet research have come in at the 90th percentile for concerns about privacy. I've been in this business for well over 20 years, and that's the first time I've seen such high levels of concern, with 91% very concerned about their privacy and 92% concerned about the loss of control over their data.

Positive consent, strong consent, is essential.

The Chair: Thank you, Dr. Cavoukian.

Next up is Mr. de Burgh Graham for five minutes.

Mr. David de Burgh Graham (Laurentides—Labelle, Lib.): Thank you.

Anita had a very quick question to start. I'll then take it from there.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): Thank you.

I'm sharing my time, so I would be grateful if the answers could be short.

I want to express my pleasure that we once again have expertise on the panel from the University of Ottawa, which is right here in Ottawa. It's good to see Dr. Geist here.

Dr. Geist, you spoke about the predictive analytics that are already being used by government. There's the example of the CRA fraud and being able to predict. If we were to go to data minimization and to only using data for the purposes for which it was collected, would that preclude the ability of government to use this kind of predictive analysis or AI?

● (1645)

Dr. Michael Geist: Not necessarily; I'll start by saying that. Think back to the controversy we saw last year with respect to StatsCan and the banking data. I thought one of the real weaknesses with respect to StatsCan was that they had never made enough of a compelling case that they couldn't achieve what their end goals were by collecting less than massive amounts of banking data from Canadians. Similarly, with respect to your question, I suppose it depends. If there is a compelling case that the existing data doesn't provide a sufficient level of information to be as effective as having more data would be, then it becomes part of that cost-benefit analysis. Maybe in some instances it does make sense to collect more, but I think it's incumbent on you to do part of that analysis before you simply collect and say, “Hey, the more data we have, the better this will be.”

Ms. Anita Vandenbeld: Thank you.

Mr. David de Burgh Graham: Dr. Geist, I first of all want to thank you for your point on Internet access. As I've said in many fora on many occasions, less than half my riding currently has 10 megabits or better. A good deal have satellite or even dial-up to this day in my riding. We're pretty tired of being left behind on this kind of file, so thank you for making that point.

How do we predict, define and declare what data is necessary and what is not necessary on the collection side? We say we only collect necessary data. How do we define that?

Dr. Ann Cavoukian: May I speak?

Mr. David de Burgh Graham: Whoever would like to.

Dr. Ann Cavoukian: The whole point is that when you're collecting data from members of the public, they don't give you their personal data to do whatever the heck you want with it. They give it to you for a particular purpose. They have to pay their taxes. They're required to do that. They realize that. They're law-abiding citizens. They give you the information necessary, but that doesn't mean that you, as the government, can do whatever the heck you want with it. They give it to you for a particular purpose. It's called purpose specification. It's use limitation. You are required to limit your use of the information to the purpose identified. That's fundamental to privacy and data protection. Personally identifiable data, which has sensitivity associated with it, must be used for the purposes intended.

Michael mentioned the Stats Canada debacle when they wanted to collect everyone's financial data from the banks. Are you kidding me? I'm sure you know how much outrage that created. They wanted to collect this from 500,000 households. Multiply that times four. It's completely unacceptable.

You have to be very clear what you want to do with the data and obtain consent for that legitimate purpose.

Mr. David de Burgh Graham: I think that's my point.

I want to hark back to something that happened in the U.S. recently.

The EFF, the Electronic Frontier Foundation, recently found that the ALPR systems, automatic licence plate readers, are networked across the United States and are exchanging data on where people have been across the country, which is obviously not the intention of those devices.

Where is the line between voluntary and involuntary collection of data? Should you be informed, for example, if an ALPR picks up your licence plate while you pass it? If that's the case, should you have the right to opt out by locking your licence plate, which we know is not the intent at all of these things and it's illegal in a number of ways? Where are the lines on these things?

I have only about a minute.

Dr. Ann Cavoukian: Licence plates are not supposed to be used for that purpose. They're not supposed to be used to track you coming and going. That's how surveillance and tracking grow enormously.

I have a quick, funny story. Steve Jobs, who, of course, was the creator of Apple, used to buy a new white Mercedes every six months less a day. Then he would take it in and buy the new model of exactly the same thing. Why? Because at that time in California you didn't have to have a licence plate on your car. You had six months after you bought a new car. He didn't want to be tracked. So six months minus a day, he took it in, bought another one, and that continued.

That's just to give you an example. People do not want to be tracked. That's not the purpose of licence plate numbers. We have to return the uses of personal information to the purposes for which they were intended. That's the goal.

Mr. David de Burgh Graham: Okay.

If we don't have some degree of centralization and we retain the siloing that we currently have in government, what's the purpose of moving to a smart government in the first place, if we don't add any convenience?

Dr. Ann Cavoukian: Well, smart government doesn't mean you identify everybody and track what they're doing. With due respect, that's not what smart government means. If that's what it means, then it's no longer free. It's not a free and open society any longer. We have to oppose that. Smart means you can deliver smart services to lots of citizens without invading their privacy. We can do both, but that has to be the goal.

The Chair: Thank you. That's it.

Next up, for another three minutes, is Mr. Angus.

Before you get going, we do have a bit of time. The bells don't start until 5:15 p.m., and we're going to push that to about the 5:05 p. m. range, so don't feel rushed. I think we have time to get everybody finished.

Go ahead, Mr. Angus.

● (1650)

Mr. Charlie Angus: Thank you.

One of the questions we've raised in opposition over the years is about giving police more tools, because if you give police tools, they use them. My colleague Mr. Erskine-Smith suggests that if we get everybody's data and information, government can help them by sending information to them.

I've been in opposition for 15 years and I've seen government often use those resources to say, “Hey, have we told you about our great climate change plan? Have we told you about the great child tax benefit?” To me, if you had everyone's data, the power you would have to send that out in the months leading up to an election is very disturbing.

I represent a rural region in which a lot of people have real difficulty obtaining the Internet, and yet seniors are told, “We're not taking your paper anymore. You're not filling this out. You're going to have to go online.”

We're forcing citizens to become digital. What protections do we need to have in place to say that citizens are being forced to use digital means to discuss with government, but they don't want to hear back from government, so that we limit the ability of government to use that massive amount of data to promote itself in ways that would certainly be disadvantageous to other political parties?

Dr. Michael Geist: Maybe I'll start.

You've raised two separate issues. You've raised the issue of people being forced into digital, which we've talked a little bit about already. I think it's striking how this issue gets raised by members on this side and by members on that side, and that has been true for many years. I've been coming to committees and we have talked about this access issue. I must admit that to me it remains a bit of a puzzle how we haven't been able to move forward more effectively in ensuring we close the digital divide—

Mr. Charlie Angus: It's still there.

Dr. Michael Geist: —that continues to exist. Part of the solution is to say that everybody does need affordable access. That is the full stop of what we have to do, and we have to make the commitment to make sure that happens.

You've also essentially raised the question of what happens when data gets used for purposes that go well beyond what people would have otherwise expected or anticipated. On the private sector side, we would say that's a privacy violation. You collect the data. You tell me what you're going to use it for, and if you turn around and start using it for other purposes you haven't obtained appropriate consent for, then I, in theory, can try to take action against you or at least file a complaint.

Part of the shortcoming—and this comes back to even the exchange with Mr. Baylis—is that we still don't have good enough laws at the federal level to ensure that data isn't misused in certain ways. We have seen over many years, especially the years with debates around lawful access and the like, very often the notion that if we have the data, surely we need to use it. There is always going to be a reason for that. You need to establish both, I think, the rule sets and the frameworks to ensure there are the appropriate safeguards in place and there's the appropriate oversight on top of that. I think at the end of the day you need to ensure you have governments, just like companies, that recognize that where they become overly aggressive with using data, because they feel they can, they cause enormous harm to that information ecosystem, and ultimately undermine public confidence not only in them but also, I think, in governments more broadly.

Mr. Charlie Angus: It's also a question of democracy, because even if they say they'll get consent, and 10% of the public decides to opt in, they are still obtaining information—good stuff, and good news stories, potentially—that can sway them democratically.

There is a whole different question that I think we haven't talked about in terms of the need to protect the democratic equality of citizens, both those who choose to opt in and those who choose not to. If they are dealing with government, it's because they have to deal with government and because they have to fix a problem with their SIN card or CRA. That's why they obtain it, not so they're receiving that information.

To me, it's like the consent boxes that we have for private business right now. If government used them, they'd be laughing all the way to the election.

Dr. Michael Geist: I think you're right. I think consent remains very weak, but let's recognize—and I know this has been discussed before this committee as well—that we still don't have political parties subject to those sorts of privacy rules.

Mr. Charlie Angus: Do you want to put that on the record?

Voices: Oh, oh!

Dr. Michael Geist: On the idea that we're going to say this is an issue of democracy, yes, it's an issue of democracy. It's a real problem when our political parties will collect data and aren't subject to the same kinds of privacy standards that they would subject any private company to.

The Chair: Thank you, Mr. Angus.

We have a couple of questioners left, which will take us to the end of our time.

We have Anita Vandenbeld and Monsieur Picard.

● (1655)

Mr. Michel Picard (Montarville, Lib.): I'll turn to Mona.

The Chair: Go ahead.

[*Translation*]

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

I have two questions.

We touched on this briefly, but it's important that it be understood. Collecting data and having access to it is viewed in a negative light by part of the Canadian population. It's unfortunate that some of these tools, including some of the work undertaken by Statistics Canada, are used by political parties to frighten Canadians. I'm talking about third parties here.

How can we win the trust of Canadians, so as to be able to put some of these measures into effect, measures that are intended, ultimately, to allow Canadians to access the government and the services it provides?

[*English*]

Dr. Ann Cavoukian: I just want to say one thing. There are a variety of things, of course, that we can do, but you asked how we can regain the trust of the public in terms of what government is doing. With due respect, there was one thing that took place last year that further eroded that trust. Prime Minister Trudeau was asked by the federal Privacy Commissioner to include political parties under the privacy laws. Mr. Trudeau said no. He basically did not go in that direction.

That was a most disappointing thing. Why wouldn't political parties be subject to privacy laws just like businesses and other government departments are? Unfortunately, there is not a lot that is increasing trust in government. With due respect, I think that was a very negative point. I think these are the things....

Also, Mr. Trudeau defended Stats Canada in their pursuit of very sensitive financial data from the public. There was a huge push-back to that. This has not been really disclosed: the banks offered the chief statistician at Stats Canada.... They said, “Okay, we will de-identify the data and remove all personal identifiers and then we will give you the data. You can have the data you need but it will be privacy protected because we're going to strip the identifiers.” What did Stats Canada say to that? They said, “No, we want the data in identifiable form.” From what I heard confidentially, there were a lot of data linkages that Stats Canada wanted to make with the very sensitive financial data of citizens. That is completely unacceptable.

I just give you that, ma'am, as an example of things that are eroding trust as opposed to increasing trust.

Thank you.

[*Translation*]

Mrs. Mona Fortier: Mr. Geist, what would you do?

[*English*]

Dr. Michael Geist: It's hard to follow Ann in this regard. She has pointed to a couple of examples. I'll give you another one, which is very small and is not one that generates headlines.

I've been actively involved in the creation of legislation that created things like the do-not-call list and the anti-spam law. Political parties have consistently exempted themselves in the name of democracy. If you want to talk about how you ensure respect, stop exempting yourselves as political parties from annoying phone calls at dinner and the ability to spam people.

I think that respect starts with respecting the privacy of Canadians. It's fair to say that when presented with the prospect of real restrictions and the ability to use information, the political parties—and I think this needs to be absolutely clear: This has occurred under Conservative governments and under Liberal governments. This is not about this particular government. It is about the history of governments that, I think, have consistently said that when it comes to privacy-related issues, they are much more comfortable setting high standards for everybody other than themselves. We see that in the exemptions. We've seen that in the inability to get the Privacy Act updated in any meaningful way for decades, and we see it with some of the examples that Dr. Cavoukian just raised.

[*Translation*]

Mrs. Mona Fortier: Thank you.

Mr. Picard, do you want to ask the next question?

[*English*]

The Chair: Thank you. I think we're done for time.

Thank you very much, Dr. Cavoukian and Dr. Geist, for coming. This subject is a big one. We've stumbled upon this iceberg, as we've mentioned, many times, and it just seems to be growing, but thank you for your time today.

We're going to go in camera to do some committee business for five minutes.

[*Proceedings continue in camera*]