HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 023 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, September 20, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, September 20, 2016

● (1105)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Colleagues, I'd like to call this meeting to order. We're running a bit behind because of the issues of the previous committee.

I would like to welcome you all back. It's great to see smiling happy faces at the table and that everybody has safely returned from the summer. I hope and trust that all of you had as good a summer as possible.

We're going to resume our study of the Privacy Act. We're pleased to have four witnesses here today whom I'll be happy to introduce in a moment.

I want to let colleagues know that I've allocated about 15 minutes at the end of the meeting so that we can discuss and revisit the issues of our agenda going forward and do a little bit of planning. We do not have any witnesses on the books for Thursday, so I would like to use this time at the end of the meeting today to have a discussion about how we see the rest of this study going and what we're going to be doing next.

We have a new clerk. Hugues La Rue, I believe, is the name.

The Clerk of the Committee (Mr. Hugues La Rue): Hi.

The Chair: I did that *en français*. You couldn't tell?

We welcome you to our committee. Thank you very much for having this all prepared for us.

Ladies and gentlemen, our witnesses include by video conference, and we're pleased to have, Brenda McPhail, who is the director of privacy, technology, and surveillance from the Canadian Civil Liberties Association.

Can you hear me okay?

Ms. Brenda McPhail (Director, Privacy, Technology and Surveillance, Canadian Civil Liberties Association): I can, thank you.

The Chair: That's great.

As individuals we have Tom Keenan, who is here from the University of Calgary; Ken Rubin, who is no stranger to the committee, who is back to talk to us now about the Privacy Act; and Tamir Israel, who is a staff lawyer at the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.

Witnesses, we have about 10 minutes allocated for your opening remarks. Please keep within the 10 minutes. You don't have to use all of it. Then we'll proceed to rounds of questions from members of Parliament that will take us until about a quarter to one. Hopefully we can have it tied off by then.

Just going in the order that they appear on the agenda, Brenda, are you ready to go?

Ms. Brenda McPhail: I am, thank you.

Thank you very much for allowing the Canadian Civil Liberties Association to appear before the committee today.

We were founded in 1964 to protect the rights and freedoms cherished by Canadians and entrenched in our Constitution.

Too often these days, privacy is characterized as a barrier that someone can decide to erect or to take down. An institution or a group might want to build it higher, chip away at it, or smash it completely, depending on its assessment of privacy as a value. The barrier metaphor, which we see increasingly in the media and other conversations about encryption, health information, and national security, to name a few, is a confrontational, unproductive, and arguably ineffective way to think and talk about privacy.

CCLA suggests that, particularly in the context of this much-needed conversation about Canada's federal privacy legislation, we need to talk about privacy as a human right. A rights-based approach, of course, doesn't remove all conflict, because all of our charter-protected rights and every right that is enshrined in international law exist in tension with other rights. However, it does provide us the motivation to engage on the level of first principles, so when we begin to specify what privacy protection actually looks like in Canada, we are all operating from a common understanding that it matters, not just to individuals but to us as a society, nationally and globally. A commitment to privacy as a human right can help us navigate the dramatic changes we have seen since the act came into effect 30 years ago.

Technology hasn't just changed the ways we can collect and use data; it has also changed our societal attitudes toward information. The potential of large collections of information—big data—to reveal useful patterns and probably hidden secrets is regularly heralded by both private and public sector bodies. Government both collects information itself and potentially has access to the ever-increasing stores of information in the hands of the private sector. At the same time, what we hear from people when they call and speak with us at CCLA is that citizens are afraid of technologies and processes they don't understand being used in ways that can have serious consequences for their life chances without their knowledge. This legitimate fear is undermining public trust in bodies, including governments, that collect, manage, and store information.

In this data-rich environment filled with data-hungry actors and fearful citizens, it is increasingly important that Canada's privacy law be revised to be strong, flexible, and well-grounded. It needs to encompass contemporary and future uses of personal information and, most important, it needs to engender trust in Canadians.

All of our recommendations are made with these overarching concerns in mind. I am going to rocket through 10 points, most of which are going to be familiar to you because they are in agreement with the submission to this committee, in March, by the Privacy Commissioner of Canada and subsequent witnesses. I am going to be extremely brief, but I am happy to clarify during questions.

First, we must ensure that there is a necessity and correctness standard put into the legislation, to be applied when deciding whether to collect information, whether to keep it, and whether to share it. Is it needed? Is it correct to collect and use it? By that I mean, would it withstand a charter challenge? This standard will encourage data minimization and guard against what we all know is a well-known tendency to over-collect data and store it for too long, just in case it might be useful sometime in the future.

Requirements for information sharing agreements need to be clarified in this legislation as well. This is particularly vital since the passage of the Anti-terrorism Act, 2015, which greatly expanded the scope of information sharing between government departments. At the time then Bill C-51 passed, the reassurances that Canadians were given in relation to these new sharing powers were that the Office of the Privacy Commissioner of Canada would have review and oversight. Regardless of the changes that are or aren't made as a result of the ongoing national security consultation, we believe revisions to the Privacy Act can provide much-needed safeguards and transparency for all information, for any purposes, in Canada. There need to be openness and transparency regarding the way information sharing happens, the extent of that sharing, and the explicit safeguards that we assume will be put in place to ensure that sharing is proportionate and that privacy risks have been properly assessed and mitigated. Of course, this holds true for sharing domestically and with foreign governments.

Transparency reporting requirements, in that same vein, need to be clarified and established. In particular, that is the case for lawful access requests made in a law enforcement context to private sector bodies that hold information about individuals. These reports provide valuable public information that can foster and inform public debates and decisions about privacy and, going back to my earlier comments, enhance trust in government institutions. Citizens deserve, and many want, an understanding of the nature and frequency of requests by law enforcement bodies for their personal information when it happens without their consent or knowledge. CCLA has always argued that the ability of law enforcement to make these requests should be limited, as per Spencer, but to the extent that these requests are allowed, with or without a warrant, a strong transparency regime is necessary to ensure the public is properly informed.

In keeping with the theme of enhancing public trust in the way government collects and uses personal information, CCLA would also recommend that privacy impact assessments be mandatory when government departments create new or expanded programs that might affect Canadians' privacy. The assessments need to be submitted to the OPC, Office of the Privacy Commissioner, for review during the design and planning phase while there is still time to mitigate any privacy risks. At the conclusion of the process, appropriate summaries should be made public so that citizens can see that this process has happened.

● (1110)

In a similar vein, we suggest that there should be consultation with the OPC when drafting legislation and regulations that affect the privacy of Canadians. Again, that should happen before the bills are tabled. This recommendation is directly relevant to my preamble, where I asked for privacy to be talked about as a human right. Having a process in place where privacy interests can demonstrably be shown to have been taken into consideration in the development of new legislation gives privacy rights the appropriate weight and is consistent with international trends.

We would also encourage government institutions to lead the way in cybersecurity by adding a specific obligation in the act for them to provide the appropriate level of both technological and processual protection to data collected, whether it is in transit, at rest, during use, in storage, or at the time of destruction. We recommend the federal government take a proactive approach to making sure the data its institutions hold is protected to an exemplary standard. We believe this can be achieved, in part, by revisions to the Privacy Act. Of course, more information will come out about that in the cybersecurity review.

We would like to see breach reporting made mandatory in law rather than just policy. Government institutions should have to report breaches beyond a relevant threshold, an agreed-upon threshold, to the OPC and notify individuals in a timely manner. The threshold needs to be clearly defined in the legislation, much the way it was done in similar amendments to PIPEDA.

Even if breaches fall short of the standard that is agreed upon for mandatory breach reporting, government institutions should be required to keep records of all breaches for possible review by the OPC. Knowing that they are accountable for doing so will be a strong motivator for needed data security and improved data stewardship.

The record-keeping requirements need to be sufficiently robust so that the commissioner can look at them and make sure that the assessments about whether or not a breach meets the threshold are happening properly.

We would like to see order-making power given to the Privacy Commissioner. It was with interest that we noted he now agrees. More information sharing and collection means that more potential harm can come from excesses. There need to be consequences in proportion to the risks, which means that the commissioner needs expanded powers to make sure the fullest protection of the revised law can be brought to bear in a timely and effective manner.

Last, we recommend regular review of the act every five years. I don't think that requires elaboration in this changing environment.

Once again, thank you very much for allowing us to appear.

● (1115)

The Chair: Thank you very much, Ms. McPhail.

We will now move to Mr. Keenan, for up to 10 minutes, please.

Professor Thomas Keenan (Professor, University of Calgary, As an Individual): Thank you very much, Mr. Chair, for the invitation to participate in your meeting. I'm going to share some thoughts about technologies that are just around the corner and that I believe will have a profound impact on how we think about privacy. My goal is to help us understand them so that, as much as possible, our laws can be ready for what's coming next.

I am a professor in the Faculty of Environmental Design at the University of Calgary, as well as an adjunct professor of computer science. I'm a research fellow of our Centre for Military, Security and Strategic Studies and of the Canadian Global Affairs Institute here in Ottawa. I've spoken to all the major hacker conferences like DEF CON, Black Hat, and one with the intriguing name of Hackers on Planet Earth, so I try to keep track of what both the good and the bad hackers are up to.

I'm also pretty sure that I taught Canada's first course in information security in 1974. Back then it was simple: lock your computer room doors, choose good passwords, and don't put confidential stuff in the trash. Today, it's much more complicated.

Consider a 2015 project called “The Face of Litter”, sponsored by Hong Kong Cleanup. Workers collected discarded chewing gum and cigarette butts on that city's streets and sent them to Parabon NanoLabs, a privately held Delaware corporation. Parabon used DNA phenotyping to create an approximate digital portrait from each sample. A week later, on passing the scene of the crime, the spitter saw an eerily familiar face on a video screen, a DNA-driven self-portrait.

Now, how could they do this? There was plenty of saliva left on those discarded items to do DNA analysis. In fact, it requires only one nanogram. Certain traits like eye colour, hair colour, and facial shape are easy to work out. Ancestry can be analyzed. Stir in machine intelligence and real-world knowledge—gum chewers are more likely to be 18 to 34, and cigarette smokers older—and you get a very creepy scenario whereby biodata is used not to identify someone specifically, but to infer things about the person. This challenges our long-held definitions of personally identifiable information and personal health information.

In my 2014 book, *Technocreep: The Surrender of Privacy and the Capitalization of Intimacy*, I suggest that a store might grab a few skin cells when you type in your PIN and send them off for analysis. The next time you visit that store, you might see a pop-up asking if you knew you were pre-diabetic and saying, “Here's a special coupon just for you.” While to my knowledge no store is doing this yet, we have seen retail outlets in the U.S. and the U.K. use facial recognition to identify shoplifters, VIP customers, and known litigious individuals. Banks such as HSBC are already using facial recognition for client identification, and several Canadian banks are doing biometric trials.

Your biometric data, be it your voice, face, or DNA, might well be covered by the Privacy Act and under PIPEDA's definition of personal health information, though those definitions will need to be updated as technologies emerge, but does this legal protection do the average person any good? In practice, many customers would not notice an obscure clause authorizing the use of their biometric data in the retail or banking environment. It could be buried in the terms and conditions document, which hardly anyone reads. Some people might even give consent to the use of their biometrics, hoping to save money, get better service, or obtain useful health information.

I believe that citizens may not fully understand all the implications of collecting, storing, and exchanging their biometric data, as well as secondary uses and cross-correlation of biometric and other databases. We need laws that mandate full disclosure and a process to ensure real compliance, which would mean more than just guidelines on the OPC website. Even today, public overt surveillance cameras are supposed to carry proper signage. In my experience, most carry no signage, and nobody does anything about it.

Then there's the time problem. Fifty years ago, a criminal may have left blood at a crime scene with impunity since, aside from determining blood type, it didn't hold much information. Today, law enforcement is solving long-dormant cold cases through DNA analysis of old samples.

● (1120)

We cannot predict what future data analysts will extract from our biological and biometric data, except to say it will be more than they do today. Experts also suggest that quantum computers will be able to retroactively decrypt decades of data that we currently believe is secure. There's a wonderful phrase that describes all this: beware of time-travelling robots from the future.

I do detect a growing unease in the Canadian public. When I talk to people about biometric identifiers, from ear shape to heart rhythms to your unique body odour, which can identify you, their ears perk up. Recently I was approached by Costco's magazine for an article on the downsides of biometric identification. I explained how fingerprints can be stolen and put on a fake finger with a 3-D printer. A hacker named Starbug even captured the fingerprints of the German defence minister from a high-resolution photo of her hand.

Even more troubling is the belief that biometrics are infallible, which they are not. They have error rates that vary depending on parameters set by the designers. The first-generation NEXUS terminals used at Canadian borders would sometimes fail to uniquely match a person from the eye biometrics they obtained.

Illinois and Texas have passed specific commercial biometric privacy laws, and article 9(1) of the European Union's forthcoming general data protection regulation puts specific restrictions on use of genetic data and biometric data where processed to uniquely identify a person. Canadians need a similar level of protection, and these laws provide a starting point for us.

Another area that needs serious thought is behavioural biometrics. In *Technocreep* I review Progressive Insurance's Snapshot device, which people install voluntarily to try for a discount on their car insurance. It records how much they drive, when they drive, and how hard they hit the brake. I suggested that it might be a sensible choice for some people, especially since it didn't track where they drove. Then Desjardins insurance brought out the Ajusto app, which uses your smartphone to create a driving-quality score. Unlike Snapshot, this system knows exactly where you are, and even how well you respect the speed limit.

Right now, systems of this nature are opt-in, and the companies take pains to tell consumers that even bad driving will not raise their rates. However, there is certainly the possibility of driving monitors and even wearable fitness monitors becoming de facto mandatory in order to obtain insurance at a reasonable rate. Insurance is, after all, about spreading risk and charging risk-based premiums.

In opposing the long-overdue genetic privacy law for Canada, Bill S-201, Jacques Y. Boudreau, chair of the committee on genetic testing for the Canadian Institute of Actuaries argued that an essential element for insurance to work properly is an equal access to information by both parties. There is clearly tension brewing between our right to keep information private and commercial interests.

We spend a lot of time worrying about how an authorized data collector uses our data. However, a flood of data breach examples, from the Sony hack, to the DNC emails, to the Ashley Madison fiasco proves that our personal data can fall into the wrong hands with devastating consequences. People whose email addresses appeared on the Ashley Madison client list have received blackmail threats, suffered workplace repercussions, and in three reported cases have committed suicide. A further complication here is that people could appear on that list without having actually signed up due to the lax design of the system.

While there are hacking-related Criminal Code provisions such as mischief in relation to data and unauthorized use of computer, these do not directly address the privacy implications of hacking. Of course, many perpetrators are never caught, but some are. There should also be consequences for the entity that manages the data if they did not take reasonable precautions to secure it.

Therefore, I support effective data breach notification in both the public and private sectors, as well as enhanced mechanisms, including order-making powers, to enable the Privacy Commissioner to preserve public confidence. I also support regular review of our privacy laws at least every five years.

I will close by revealing that you've been listening to a cyborg, a human being with a new technological body modification. I had an RFID chip implanted in my hand at this year's DEF CON conference. Right now it gives me only one superpower: I can open my door at the university without fumbling for my ID card. In the near future, devices will be available to give people telephoto vision, super-acute hearing, and enhanced mental powers.

● (1125)

Canada's first privacy laws date from the era when information was kept on paper, and we dragged them into a world where our data lives in cloud networks somewhere on the planet. Our next challenge, one that will keep us busy for a long time, is dealing with the implications of the data being us, an intimate part of our humanity.

Thanks so much for your attention. I look forward to your questions.

The Chair: Thank you very much for your interesting presentation. At the risk of finding out the answer, I won't ask you where you keep your car keys.

We'll now move to Mr. Rubin.

Go ahead for up to 10 minutes, please.

Mr. Ken Rubin (Investigative Researcher, Advocate, As an Individual): Surveillance is always scary.

I'm back here to testify given my involvement for over four decades in privacy matters and advocacy. My privacy advocacy work began with a local civil liberties group dealing with the growing use of social insurance numbers as an identifier. As an investigative researcher, I dug up information on the problems with increasing use of computer matching of personal information, and yes, back then, I was a witness testifying on the limits of Canada's proposed privacy act and on secretive data sharing.

Now the privacy issues are even more complex in this digital age and are threatening given the widespread legal and illegal sharing of and access to personal data, metadata mining, data profiling, and massive surveillance.

Throughout I've never wavered in the belief that Canadians need more access to and control over their personal information and better information about intrusions. Canada cannot continue three and a half decades later to have weak privacy legislation. The focus on limited privacy access to one's records to the detriment of regulating the state and private sector's relentless intrusions into the lives of Canadians has left us with inadequate safeguards.

There is not much in the current Privacy Act and PIPEDA that puts a stop to online snooping, data mining, and biometric identity matching or that addresses and restricts the growing use of secretive newer surveillance technologies like Stingray cellphone listening devices or prevents the increasing sharing of Canadians' personal data with foreign authorities.

No Canadian minister or prime minister has stepped in demanding better privacy protection or proposing remedies against what Edward Snowden revealed as the means of secret massive surveillance trolling.

No Canadian prime minister has put in place regulatory restrictions that, for instance, deal with the handling of increased amounts of Canadian personal data housed or transmitted through the United States and potentially captured under its Patriot Act or subjected to other foreign entity intrusions.

Public Safety Minister Ralph Goodale's recent discussion paper on police security powers does not alleviate civil liberties privacy protection concerns. Treasury Board President Scott Brison's statements, including before this committee, that more not fewer records must be exempt under national security, do not calm those concerns. Brison went on to say that the Information Commissioner, or for that matter the Privacy Commissioner, would have limited review and access to such security records, so the Trudeau government's opening moves are then far from reassuring.

What we do need is a greatly strengthened data protection act. Let me briefly turn to 10 areas in which improvements can be made.

My first recommendation to improve legislation is in agreement with testimony of a previous witness, Lisa Austin. We must begin by framing further advances restricting privacy invasion in terms of and in line with Canada's Charter of Rights and Freedoms, so first and foremost a new act's purpose clause must recognize privacy protection as a constitutional protected right.

My second recommendation is that a basic rewriting of privacy legislation needs to create a whole new predominant part one section that emphasizes transparent and enforceable obligations and restrictions on data sharing, matching, profiling, and tracking.

If a privacy act is to become, as it should be, a data protection act rather than simply a limited and outdated access to personal information act, there must be provisions added for tougher and clearer regulation and restrictions on personal information sharing.

While the Privacy Commissioner calls for prompt mandatory reporting of public sector personal data breaches, he only advocates some selective notification of those affected and minimal transparency, and he sets out no enforceable binding order or penalty powers for his office despite the fact that such breaches occur fairly regularly. I'll explain that more.

My third recommendation is threefold. First, individuals should be given mandatory rights of consent on a timely basis for government collection and use of their information. Second, there should be fewer exemptions, exempt banks and delays so individuals can promptly obtain more fully their information. Third, all agencies, including the prime minister and his office, should be covered.

● (1130)

My fourth recommendation, which former privacy commissioner Jennifer Stoddard suggested, is that unrecorded information such as personal biological samples, including DNA and iris scans, be covered. Data gathered from radio frequency identification chips or now by Stingray collection needs to be explicitly covered by public and private sector privacy legislation.

My fifth recommendation is that officials' salaries and perks and private sector violations no longer be considered as personal information, but be public. For example, exact bonus payment information received must be made public The company's name, as in the case of the bank fined $1.1 million by FINTRAC, or in the case of companies and individuals found to be tax haven offenders must also be made public.

My sixth recommendation is for a privacy commission to have order-making power. Now Commissioner Therrien agrees at this point, but enforcement powers and stiffer penalties for privacy invasion would still be needed to help effectively restrict privacy invasions and regulate transborder data flow. His office would need wider investigative powers to review such matters as questionable transborder data flow and metadata collections. It's not simply a matter of order powers.

My seventh recommendation, in agreement with Commissioner Therrien, is that both he and all Canadians need a legislative expanded right to go to court, including in cases of improper collection and use of personal data. Courts now are only able to hear cases about access to blocked individual personal files. It would help too if individuals and groups bringing such privacy violation cases to court were given resources to sue the government. It is important to note that individuals and groups may still challenge commissioner orders as limited and want the courts to provide greater privacy protection than commissioner orders offer.

My eighth recommendation is that oversight be separate when it comes to access to information and privacy. Joining such acts so closely together destroys their opportunities to more fully develop their separate and, at times, conflicting public interests. One is for proactive disclosure and multi-transparency tools and accountability practices; the other is for restricting privacy invasions and enhancing data sovereignty. It's time to untie privacy legislation from access to information legislation.

My ninth recommendation is that in order to have an effective data protection act, the House privacy committee must consider bold changes to the Privacy Act in conjunction with improving the Personal Information Protection and Electronic Documents Act, PIPEDA. The threats under both acts are similar, the remedies the same and the object the same, which is that Canadians want more control on what personal data third parties, from police to marketers, can access.

My 10th and final recommendation is for greater transparency—no surprise—when it comes to the public knowing about the use of privacy invasion powers. Canadians remain largely unaware of the systems and means authorities are using to conduct surveys that can affect them. Little is known about the cost of surveillance and about the budget and expenditures law and security forces have in this regard. We remain in the dark about how frequently and where, for instance, Stingray equipment is used and the cost involved. We remain unclear about what laws or authorities allow surveillance. I can think of dozens of such laws.

The committee, in addition to conducting periodic reviews of privacy legislation, should have a subcommittee tasked with reviewing and questioning laws that broadly allow privacy invasion and intrusions.

Let me end with an example of where the public is kept in the dark on how Canada's system of surveillance operates. Recently I uncovered data whereby the public safety minister and his officials had issued, in a 2014 to early 2016 period, licences to the RCMP, CSIS, and CSE of National Defence which in turn allow unnamed private companies to have and sell surveillance equipment to unnamed buyers, be it possibly malware, Stingray, or other surveillance equipment or components. This is done under the cover of a section of Canada's Criminal Code.

● (1135)

Documents obtained indicate, for instance, that CSIS has trusted, long relations with certain surveillance companies, and, in one instance, a ministerial licence granted was backdated. We do not know, then, what kind of surveillance occurs, and there is no known reporting requirement, like under wiretap legislation.

The point, Mr. Chairman and members of the committee, is a minister of the crown oversees this surveillance arrangement far away from public scrutiny. His or her first concern is not to champion privacy protection for the public. I and others are offering up suggestions for Canada to move beyond weak privacy protection legislation and lax regulation to protect citizens.

I thank you very much.

The Chair: Thank you very much, Mr. Rubin.

We now go to our last witness, Mr. Tamir Israel, from Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic.

You have 10 minutes, sir.

Mr. Tamir Israel (Staff Lawyer, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic): Mr. Chair and members of the committee, good morning. My name is Tamir Israel, and I am staff lawyer with CIPPIC, the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic at the University of Ottawa's Centre for Law, Technology and Society and the Faculty of Law. CIPPIC is a public interest legal clinic that works to advance the public interest in policy debates arising at the intersection of law and technology.

I wanted at the outset to thank you for inviting us to testify before you today, as well as for undertaking this important review of the federal Privacy Act, a central component of Canada's privacy, transparency, and accountability framework.

Since the introduction of the Privacy Act in the late 1970s, the policy landscape surrounding data protection has evolved dramatically, driven by tectonic shifts in the technical capability and general practices surrounding the collection and use of personal information. The federal Privacy Act has simply not kept pace with these dramatic changes, a reality that hinders its ability to continue to achieve its objectives, in light of heightened incentives and technical capacities to collect and keep personal information at unprecedented scales. The nature of the objectives incentivizing state data practices has rapidly evolved over the years since the adoption of the act, which initially focused primarily on regulating data practices animated by administrative purposes.

Today's privacy challenges are driven by a far more diverse set of incentives. The era of data-driven decision-making, colloquially referred to as “big data”, increasingly pushes state agencies to cast wide nets in their data collection efforts. Additionally, more often than not, the act is applied in review of activities motivated by law enforcement and security considerations that are far removed from the administrative activities that animated its initial introduction.

Finally, data sharing between domestic and foreign state agencies now occurs on a more informal, and often technologically integrated, basis than could have been envisioned in the late 1970s.

The Privacy Act is in drastic need of modernization, and to that effect, CIPPIC has reviewed and largely endorses the recommendations made by the Office of the Privacy Commissioner of Canada to this committee with respect to changes necessary to ensure today's data protection challenges are met. We will elaborate on a few of these, as well as on some additional recommendations that we have developed in our comments today. In addition, in our written comments, which will eventually make their way to the committee, we provide some legislative language suggestions, which we hope will help guide your review of this act.

The remainder of our opening comments focus primarily on discussing and highlighting specific recommendations designed to enhance proportionality, transparency, and accountability, as well as address shortcomings that have arisen from specific technological developments.

Before turning to these broader themes, however, our first recommendation addresses the Privacy Act's purpose clause, which we believe should be updated to explicitly recognize the objectives of the act: to protect the right to privacy of individuals, and to enhance transparency and accountability in the state's use of personal information. Express recognition of these purposes, as is done in provincial counterparts to the Privacy Act, will assist in properly orienting the legislation around its important quasi-constitutional objectives, and will help to secure its proper and effective application if ambiguities arise in the future, as they surely will.

Necessity and proportionality are animating principles that have become central to data protection regimes around the world, but are absent from the aging Privacy Act. It's important to explicitly recognize these principles in the act, and to adopt additional specific measures that are absent from its current purview, but are nonetheless essential to ensuring private data is collected in a proportionate manner.

As a starting point, first, the Privacy Commissioner's recommendation for explicit recognition of necessity as the standard governing data collection practices should be implemented. Necessity is a formative data protection concept and provides important context for assessing when data should or should not be collected, used, or disclosed. The existing standard, which requires only that data practices relate directly to an operating program or activity, is simply too imprecise in the age of big data, where organizations are increasingly encouraged to collect data that has minimal clear, immediate connection to current objectives.

● (1140)

Second, the Privacy Act imposes no explicit limitations on how long data can be retained once it is legitimately collected. The lack of any explicit obligation to adopt reasonable retention limitations can mean that that data is kept well beyond the point where its utility has expired, exponentially increasing the risk of data breach and of inappropriate uses. The lack of an explicit retention limitation requirement can even lead to the indefinite retention of data that has only a very short window of utility, greatly undermining the proportionality of a particular activity.

As an example, our clinic, along with Citizen Lab at the Munk School of Global Affairs, recently issued a report examining the use of a surveillance tool called a cell site simulator. These devices operate by impersonating cellphone towers in order to induce all mobile devices within range to transmit certain information that is then used to identify or track individuals or devices. The devices operate in a coarse manner. For each individual target the devices are deployed against, the data of hundreds or thousands of individuals within range will be collected. Non-target data collected is only immediately useful for identifying which datasets belong to the individual, the legitimate target of the search, and which do not, an objective that could be accomplished within 24 to 48 hours of collection. However, as the underlying collection of these thousands of non-targeted datasets is legitimate, these datasets might be kept indefinitely. These large datasets can then be reused at any point in the future and, subject to ancillary statutory regimes such as the Security of Canada Information Sharing Act, which was recently adopted via former Bill C-51, can be shared across a wide range of other agencies.

Including an explicit retention limitation provision would not only mandate state agencies to adopt clear retention policies, but would also allow the commissioner to address unreasonable retention in a principled manner. This, in turn, will reduce the risk of data breach and generally increase the proportionality of data collection practices.

Third, we would recommend the adoption of an overarching proportionality obligation that would apply to all collection, retention, use and disclosure of personal information by government agencies into the Privacy Act. This would be comparable to its counterpart that is currently found in subsection 5(3) of PIPEDA. As you have heard from other witnesses, the Privacy Act increasingly provides an important avenue for ensuring charter principles for the protection of fundamental privacy rights are fully realized. An overarching proportionality or reasonableness obligation modelled on subsection 5(3) of PIPEDA would provide an avenue for assessing charter considerations across all data practices. It will also provide the Privacy Act with a measure of flexibility, allowing it to keep pace with technological change by providing a general principle by which unanticipated future developments can be measured.

In addition to these proportionality measures, there are clear gaps in the Privacy Act's current transparency framework and further opportunities to enhance the openness of state practices, which in turn will encourage accountability and public confidence.

At the outset, we encourage the adoption of the Privacy Commissioner's recommendation for a public policy override to the act's confidentiality obligations. This would allow important information regarding anticipated privacy activities to enter the public record in a timely manner.

Second, the Privacy Act should be amended to include statistical reporting obligations attached to various electronic surveillance powers in the Criminal Code. As Mr. Rubin mentioned, statistical reporting obligations were once a hallmark of electronic surveillance regimes and are attached to certain electronic surveillance activities, such as wiretapping, but these activities have largely been superseded by other electronic surveillance activities that have no comparable statistical reporting obligations attached to them.

One investigation conducted by the Privacy Commissioner's office recently found that law enforcement agencies themselves did not have a clear picture of the scope of their own practices in relation to the collection of subscriber information from telecommunication companies. Understanding the nature and scope of state surveillance practices is all the more important in light of the tendency for rapid change in practices in this sphere. Imposing a statistical reporting obligation in the Privacy Act that applies across the spectrum of electronic surveillance powers would therefore provide an important transparency mechanism.

Finally, the adoption of a general obligation on state agencies to explain their data practices would greatly enhance transparency. While the act currently obligates government agencies to explain to individuals the purposes for which their personal information is collected and used, it lacks a general obligation to explain agency practices.

One modelled on PIPEDA's openness principle would be beneficial. If this concept is adopted, it should address the challenges raised by algorithmic non-transparency, which would entail an obligation to explain the logic of any automated decision-making mechanisms adopted by the state.

We have some suggestions on accountability and compliance measures that I will submit in writing and you folks can review at a later time.

I did want to very quickly touch on a couple of recommendations we have that address very specific technological developments that have led to gaps in the Privacy Act.

● (1145)

We would recommend updating the definition of “personal information” so that it is aligned with the comparable definition under PIPEDA. The current definition only applies to personal information that is recorded, whereas many modern data collection and use practices never actively record any personal information, but can still have a very salient privacy impact.

In addition, we would endorse the Privacy Commissioner of Canada's recommendation to adopt an explicit obligation to adopt reasonable technological safeguards, as well as individual breach notification obligations.

Finally, and very briefly, we would also endorse the Privacy Commissioner's recommendation to formalize the privacy impact assessment requirement, as well as recommend an avenue for facilitating public input into the process so that discussions of privacy-invasive programs can occur with public input at the formative stages.

Thank you. Those are my comments for today.

● (1150)

The Chair: Thank you very much, Mr. Israel, and to all of our witnesses.

We're going to proceed to rounds of questioning. I would ask the questioners and the witnesses to keep it as concise as possible.

We're going to start the seven-minute round with Mr. Long from the Liberal Party, please.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Welcome, everybody. It's great to see everybody back. I'm happy to see Mr. Rubin in front of us again.

How's the farm?

Mr. Ken Rubin: The crops are coming in, and the Liberals are not coming in.

Mr. Wayne Long: Mr. Rubin, let me be frank. You were here before, obviously, advocating for open information by default. You're here today talking about privacy and people's privacy. How do you square the two?

Mr. Ken Rubin: Fairly simply, there are certain things that the state has no business knowing about, or if they are to know about it they need certain restrictions or rules. That's a lot different from public policy issues, where the public has the need for that information. There has to be accountability for it.

One of the things I was trying to draw a parallel to, since I'm back again, is with proactive disclosure agreements and so on. On the Privacy Act side, section 48 is about collection of information. As a result, even back in the 1980s, there were many thousands of personal information data-sharing agreements among different departments, the provinces, internationally, but on the access side, almost zippo. There's no suggestion of getting on and agreeing to transparency, so we have a dichotomy there.

I won't go further, other than to say that I think the two are compatible in certain ways, but the only way they're going to function better is to separate.

Mr. Wayne Long: Okay, thanks.

You were quoted in an article—there's an article in *Kamloops This Week* about the Gold Trail School District, where a trustee was censured.

Mr. Ken Rubin: Yes.

Mr. Wayne Long: A report came out, people wanted some information, and obviously the school board blocked out a lot of that information. Your quote was:

> There are documents that are withheld like that on disciplinary matters, but it's the credibility of the actions, where you would hope public accountability would demand at least some summary of what it was.

In that case, would you protect that individual's rights, or are you saying the public's going to demand that? Again, how do you square that?

Mr. Ken Rubin: It's difficult. I was not advocating for every detail of the case. Personal matters can be sensitive, but when you're a trustee on a public board, the public or the public trustees or everybody else should know something about it. This reporter going out to B.C. was kept totally in the dark. For everybody's credibility a certain minimal transparency should happen, but the person's privacy has to be protected to a point.

Mr. Wayne Long: You see the—

Mr. Ken Rubin: Oh, there is.

Mr. Wayne Long: Where do you find that balance?

Mr. Ken Rubin: Well, you just gave an example and I'm trying to say how I would handle that example. Different people have different perceptions of what is private and what shouldn't be private. But a lot of people have misconceptions about what should be public, and they think surveillance of people should always remain a state secret. That's the problem. We hide too much stuff. It isn't that we have a better understanding of privacy.

● (1155)

Mr. Wayne Long: Thank you.

Mr. Keenan, thanks for your presentation today.

This is a quote from one of your articles. You say, "We're already in a surveillance society, and there ain't no going back on that."

Prof. Thomas Keenan: It's true.

Mr. Wayne Long: In this article, they say you're always counting surveillance cameras wherever you go.

How many did you count today?

Prof. Thomas Keenan: I actually counted 14 just in a very short trip over here.

I met my wife counting surveillance cameras in San Francisco and it took us an hour to find 100. Then we went out on our first date. It was a wonderful date.

Voices: Oh, oh!

Mr. Wayne Long: So you did count them today.

Prof. Thomas Keenan: Today I didn't really need to count them, because every one of you is carrying one in your pocket in your cellphone. There are cameras that are so small that you wouldn't know.... I was just looking around this room wondering how hard it would be for someone to hide a camera in here.

We see that at DEF CON all the time. People put in surreptitious devices, not just cameras but even things that pick up your Wi-Fi. They'll leave them at the Starbucks and they can sit there for months transmitting all the data.

So yes, we are in a surveillance society.

Mr. Wayne Long: I have some quotes. "These cameras are put up for two primary reasons", and we are talking about cameras. You're from Calgary, and in Calgary there are upwards of 3,500. Then we talk about Edmonton, which has more than 3,000 cameras. There's one in every bus.

These people are saying that these are put up for protection of assets, public safety, and so on.

Do you agree with that?

Prof. Thomas Keenan: Sure.

Mr. Wayne Long: You do.

Prof. Thomas Keenan: Sure.

For example, take the Boston Marathon bombing. The best footage of that was from a department store camera pointing out on Massachusetts Avenue, and the police were darn glad that was there. Take the Vancouver Stanley Cup riots. There were citizens' videos. It came to an interesting privacy question actually, which the provincial commissioner had to rule on. Could the police take the licence database and run it up against photos of people looting stores to identify them?

She made a very wise decision. She said that they could submit the looting tape and a third party, the B.C. licensing people, could look at it, but then they needed a judge to unseal the data.

I think we need more oversight, because otherwise you can have a fishing expedition. I use an example in my book of a guy who parked in stall number 11, and he was put in a police computer as a known associate of a Mafioso. That was because the guy who parked in stall 12, unbeknownst to him, was a Mafia don. They would say good morning every day, so under surveillance he got put in there as a "known associate".

Mr. Wayne Long: On another point, you talk about signs warning about cameras.

Do you advocate that signs should be up?

Prof. Thomas Keenan: There are actually recommendations on the OPC website that say there should be a sign, that the sign should say what the purpose of the camera is, that it's there under the authority of a certain act, and tell you who to call.

Guess what? Toronto has a phone number for the Toronto police. Calgary says to call 311. You could wait on hold for two hours calling 311, so that's not an effective way, plus only the downtown LRT stations have signs. You go out to the sticks and you're not going to have any warning signs at all.

Mr. Wayne Long: Again, in this article in the *Calgary Herald*, it says that cameras don't really deter most crimes.

Prof. Thomas Keenan: Well, the evidence certainly in the U.K. was something like one crime per 10,000 cameras in one particular study....

I mean, they may. Obviously, if people know they're under surveillance, their behaviour may change, but good old police work actually solves most crimes.

Mr. Wayne Long: Would you agree, though, that if signs were up, it would deter more crime?

Prof. Thomas Keenan: No, I just think that people have—

The Chair: Mr. Long, we're well past the seven-minute mark. It was a good set of questions. If we get some time, we'll come back to them.

Mr. Jeneroux, for up to seven minutes, please.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): He looks so disappointed, Mr. Long.

The Chair: I was kind of, too. I didn't really want to, but it was—

Mr. Matt Jeneroux: Thank you, everybody, for being here. I think a few of you are back today. Mr. Keenan, I think it's your first time before us. Again, thank you for being here.

I want to talk a bit about how technology changes so quickly. We have an act that's been around since 1983. However, there are a number of policies which have been implemented at the government level that address a lot of the new technology.

If we say here's what we want to do in 2016 as outlined by the Privacy Commissioner, how does that not become out of date almost immediately in terms of technology?

Could you comment on how you see this progressing and address the policy versus the act argument? I'm hoping to get all of you in on this, if you don't mind.

● (1200)

The Chair: Go ahead, Mr. Israel.

Mr. Tamir Israel: Thanks.

I would point to the Privacy Act's counterpart, PIPEDA, which wasn't introduced quite so long ago but adopted a very principled framework as opposed to a more prescriptive one. Some of our recommendations try to accomplish this, as well as some of the recommendations of some of the other witnesses, but I think if we get to a more principled framework, it allows it to keep up with the changes a little better. Then you still need to always tweak any law really in these days of technological change occasionally, so adding things like a five-year review helps. I think making it a little bit more principled with stuff like an overarching proportionality obligation helps it keep pace with these types of technological changes that we can't really foresee, other than Mr. Keenan here, who has a little bit of a window to the future.

Mr. Matt Jeneroux: Ms. McPhail, do you have anything to add to that?

Ms. Brenda McPhail: I would agree with Tamir. I think that the solution is to make sure that the law is grounded in principles rather than details and minutiae. Looking at the necessity requirement as well will help, because regardless of what technology was used to collect a piece of information, it's still helpful to ask, do we need it? Was it collected appropriately? Was it collected properly? The idea of appropriately and properly may change versus the technology, but the concepts of needing to know for sure that we've done things based on these core principles doesn't change and allows us to be flexible and keep the law relevant as things change.

Mr. Matt Jeneroux: Does anybody else wish to comment?

Mr. Rubin.

Mr. Ken Rubin: I have just one informational thing. Canada has really had the Privacy Act since the late 1970s because I operated under part IV of the Canadian Human Rights Act, so it's an interesting act.

The Privacy Commissioner tries to do this to some extent, but my only comment is that I think it would be helpful if there was an office of technology—the Science Council of Canada used to talk about this—that would look at the impact of technology from several aspects, including privacy, so you have some place that consistently continues to look and project new ideas of what technology is and its implications. We don't seem to have any continuity. It's always this comes up, that comes up.

That would be the only thing I would add, other than, yes, things have changed dramatically since the first part. But with SIN identifiers and metadata and all the rest, there are still similarities to what you can do about it.

The Chair: Mr. Keenan.

Prof. Thomas Keenan: I'm a professor, so you know that I'll say fund more research. The Privacy Commissioner does some already, but could a lot more. I want to give you another concept.

I did a sabbatical once with a company called Northern Telecom. My project was to find new features for their phones. I came up with one that was a solution to the telemarketer problem. They were always interrupting my dinner. I said I should be able to put on my phone a dollar amount. Maybe I'm lonely, so it's zero or 10¢, but maybe I'm having a wonderful romantic dinner so it's $1,500 to interrupt me. If you wanted to pay that, you would be charged that amount. Nortel didn't build a function, but I do it. When somebody calls up, I tell them, “This is costing you $100 an hour; I take Visa or MasterCard.”

What's the relation to this? People need to value their privacy. You're worth something like $800 a year to Google if you use Google, Gmail, YouTube, and so on. There's no way to pay Google for that. Their services are free, but they're selling you. There's this whole concept of surveillance capitalism. Shoshana Zuboff, a Harvard professor, talks about that. There's an economic aspect. Maybe what we need to do is tell people that if they think their privacy is worth something, there should be a way for them to get paid for it, just like taking the telemarketer call. Maybe you do want to give your information to the insurance company because you want that discount. Just know that you're doing it. The law has to make it really clear in some way how companies will disclose what you're paying.

Mr. Matt Jeneroux: Thank you.

I'm not sure if that answered a lot of it there, but we'll come back to that with subsequent witnesses, I imagine.

I quickly want to get your thoughts, Ms. McPhail, on the expansion of this. One of the recommendations is to expand the act to the Prime Minister's Office and ministers' offices. This wasn't a recommendation previously when the Privacy Commissioner made recommendations a number of years ago. It's now part of them. Would you mind commenting on how you see that progressing?

● (1205)

Ms. Brenda McPhail: Briefly, we would be in favour of that move. I think that at all levels of government and at all levels of power Canadians have the right to know that information is being collected and held safely and well and of the concurrent right to make requests under other acts for the information. I think moving that to the upper levels of government is a wise and sensible thing to do.

Mr. Matt Jeneroux: Good.

The Chair: Mr. Blaikie, you have up to seven minutes.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Thanks to everyone for their presentations.

I appreciate how the shift to a more principled framework could be useful in allowing the legislation on the books to keep pace somewhat with technological change.

On the enforcement side or on the side of having people better understand their rights and how they're protected, can any of you put some meat on the bone in terms of what that looks like so that the notice to people who are accessing government services, for example, and agreeing to the use of their private information is not just a clause buried in the fine print? What are some concrete examples of what that would look like for people? What would change from what's there now?

Prof. Thomas Keenan: If you look at the European Union's new general data protection regulations, you will find fines that are astronomical, something like 4% of the annual turnover of a business. People are quaking in their boots, and even people in Calgary are thinking about it because they do business in Europe. I've sat down with people who say we have to be aware of this because we can be fined an awful lot if we invade somebody's privacy. Maybe that at least gets the attention.

Mr. Daniel Blaikie: I apologize because I don't know the specifics, and you may not be able to answer because I don't know enough about it, but I have heard tell of a case going on in B.C., a suit being brought against Facebook for the use of some personal information. Part of what is at issue is that there's a clause in the Facebook user agreement that says you can only litigate in California. Without prejudging the outcome of that trial, even if we have some of the best privacy protection laws in Canada, how vulnerable are we? Is there anything we can do about those agreements that people agree to without really reading and that force them to litigate outside the boundaries that would be protected by an updated privacy law?

Mr. Tamir Israel: Without my prejudging the outcome of that decision, what's at issue there is whether, through very contractual clauses, an entity like Facebook that has millions of customers in Canada could essentially opt out of Canadian law. If the decision is that this is the case, I think we will be back here at some point asking for some sort of legislative reform that would expressly preclude the enforceability of that type of clause. It doesn't need to be an absolute prohibition. In the manner that it interacts with private entities like that, the Privacy Act is probably a little bit shielded from that type of activity.

Making sure that, at least in some cases, there is the ongoing ability to apply Canadian standards and laws to international entities operating from abroad is very important moving forward, to ensure a level of transparency and privacy protection that is in accordance with Canadian standards.

Mr. Daniel Blaikie: One of the recommendations to this committee is the idea that the government should be consulting with the OPC prior to tabling new legislation to see what the privacy outcomes would be. We know that international trade deals and other kinds of agreements with other governments also have privacy implications. Would you say that should go beyond simple bills that the government is tabling to any kind of substantive legal agreement the government is entering into?

Mr. Tamir Israel: I think so. We saw in one instance where a B. C. committee reviewing a counterpart to this law in B.C. had not been aware of a trade commitment that was made, even though some level of the B.C. government was involved in the negotiations of trade agreements. They're so multilateral these days and they have applied it in so many areas of daily life that a more integrated consultation process needs to be set up, because they weren't even aware that a mechanism might have been adopted that would impact their law in a significant way. The same could be said for other aspects of the Privacy Act as well as of PIPEDA. Finding a way to incorporate that type of consultation at early stages will be very important moving forward as more and more of these decisions are made in that context.

I don't know if Ms. McPhail wants to address this, but the CCLA put out a report earlier today on how to better address constitutional protections in legislative processes. You may want to ask her that.

● (1210)

Mr. Daniel Blaikie: Okay. I know Mr. Rubin was trying to angle in.

Mr. Ken Rubin: You can penalize people as a method of enforcement.

I think the problem I have is that in the current act, if you look at the sections on use, retention, and collection, it is so vague. That's why I'm saying you have to build that act up. You can't be explicit in everything, but transborder data flows? Come on. We've had a history of these. If we can identify them, we can anticipate some. If we don't build in some explicit language in that regard, what are you going to be enforcing? You have to have much more of what these things are: metadata, biometric data. You have to have some degree of the content there, so that you can then enforce it.

Mr. Daniel Blaikie: Ms. McPhail, did you want to weigh in?

The Chair: We can't hear you, Ms. McPhail.

Ms. Brenda McPhail: Technological difficulty is an appropriate theme for today.

Mr. Israel was referring to our just released “Charter First” report, which is a position paper that CCLA has introduced, in which we are actually arguing that all legislation that's created in Canada should undergo charter review prior to being tabled. It's very much in line with the recommendation here that legislation that involves privacy implications should be reviewed by the appropriate body that can consider all of the implications, and in the case of the Privacy Act, we would say that would be the Privacy Commissioner. In general, we would be in favour of multi-level protection to make sure that charter-protected rights—and privacy is a quasi-constitutional right—are always subject to review and consideration in any kind of activity. Whether it's a multilateral treaty, a trade agreement, a new piece of legislation, or a new data processing system, there should always be at some appropriate level consideration of what the risks are going to be to people's privacy, and of course, a number of other factors.

The Chair: We now move to Mr. Lightbound to end the seven-minute round.

Mr. Joël Lightbound (Louis-Hébert, Lib.): First, if I have more time at the end, I'll share it with Mr. Erskine-Smith.

Thank you all for being here. My question is for Madam McPhail and Mr. Israel.

In the Privacy Act there is a general prohibition on information sharing, but then in subsection 8(2), there is a whole list of exceptions, such as, for instance, information shared in accordance with federal legislation or regulation. Then along comes a bill such as Bill C-51, which allows for information sharing among, I think, 17 government institutions or agencies, maybe more or less.

How should we approach the exceptions to information sharing, and do you have any recommendations?

Mr. Tamir Israel: One of our specific recommendations is to adopt an overarching proportionality mechanism. As we've envisioned that and as it operates in PIPEDA, the private sector counterpart, it would actually sit on top of those exceptions. It doesn't mean that any exception could be overridden in every instance, but it would allow for some ability to incorporate proportionality in the application of those exceptions, if that makes sense. That would be our immediate suggestion for how to address those.

The list of existing exceptions is very long. I think courts have also defined and narrowed some of them through charter interpretations and so on. We don't have any specific recommendations on addressing any of the specific exemptions in there, but we think the overarching proportionality consideration would allow for more problematic applications of those exemptions to be tempered.

● (1215)

Ms. Brenda McPhail: I think we'd support that same proportionality suggestion. In general, should the committee be willing to undertake a detailed examination of all of the exemptions, our position would be that exemptions should be limited, and they should be as narrow as possible in all cases.

Mr. Joël Lightbound: If you would be so inclined as to send us written recommendations in terms of the exceptions and how you would curtail them, the committee would appreciate that very much.

My second question regards metadata. We've touched upon it a little bit. I know it's not defined anywhere in Canadian legislation. There was a private member's bill a few years ago by Joyce Murray to define metadata, but she was proposing to have it defined in the National Defence Act. Do you think it would be pertinent to have metadata defined in the Privacy Act, and to have it addressed?

My question again is more for Mr. Israel and Madam McPhail.

Mr. Tamir Israel: In terms of adopting, I think it would be useful to clarify this. Metadata already falls outside the definition of personal information in the act where there are ambiguities. An IP address is a good example. Often the argument will be that because an IP address takes three or four steps before you connect it to a name, it's not personal information. That's because the definition of personal information is tied to information that's about an identifiable individual. I think some of that can be addressed through interpretation by the Privacy Commissioner, etc. In Europe, I think they've actually issued directives around specific problematic items of metadata like IP addresses, saying that this is to be considered personal information.

I think part of the problem with addressing metadata in a statutory definition is that it's a constantly evolving category of data. Maybe something that would refer to regulation, that would allow for a rolling definition that gets adopted through regulation, might be the best way to address that particular problem and make sure that this type of data is kept within the scope of the protections in the Privacy Act.

Ms. Brenda McPhail: I think we'd be a bit more direct than Mr. Israel and just say yes, we think metadata should be a category of protected data. I think there's been sufficient jurisprudence now to suggest that metadata can be very revealing of intimate personal details about the biographical core.

On the actual mechanism for doing that, perhaps regulation is great for the detail, but in terms of a general purpose statement as part of the kinds of information covered, we'd love to see that placed directly.

Mr. Joël Lightbound: Mr. Erskine-Smith, you can have my last two minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks.

My first question is with respect to the PIPEDA model of damages. Would you propose incorporating that same model, whether it's administrative damages or damages at the Federal Court, in the Privacy Act? That's for any or all of you.

Mr. Tamir Israel: It's a bit of a tough one, but yes, as a starting point, we would, and probably further than what's in PIPEDA right now. The current damages mechanism in PIPEDA is closer to a fine, basically. It's hard to actually implement, because you need to meet very high standards of proof before you can show that someone intentionally violated privacy, whereas an administrative monetary penalty regime would be more appropriate to these types of regulatory regimes.

We specifically suggested in our comments, but very briefly, consideration of a private right of action. There is an issue, of course, where you're opening the government up to fines, and obviously that has to—

Mr. Nathaniel Erskine-Smith: The private right of action does exist in PIPEDA, though, under sections 14 to 17.

Mr. Tamir Israel: Yes.

Mr. Nathaniel Erskine-Smith: We're looking at that kind of model then.

Mr. Tamir Israel: That mechanism is tied to damage recovery. I would make it little bit different, because the one in PIPEDA is ancillary to a complaint. You have to file a complaint, go through the process, and basically start all over again in Federal Court if you hope to get damages. Very few people are willing to go through that entire process.

● (1220)

Mr. Nathaniel Erskine-Smith: An administrative penalty followed by some form of judicial review at the Federal Court level.

Mr. Tamir Israel: And maybe an independent, individual right of action that's in parallel would be worth considering.

Mr. Nathaniel Erskine-Smith: Is there any disagreement?

Prof. Thomas Keenan: I would just add one thing. I was on a board once that disbursed $2 million of administrative penalties collected by the Alberta Securities Commission. We used it to educate the public about investors. I would suggest that education would be a wonderful use of any monies collected.

Mr. Nathaniel Erskine-Smith: Thanks very much.

The Chair: We'll now start the five-minute round with Mr. Kelly, please.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you to all for coming today and for appearing.

When we undertook our study of the Access to Information Act and the systems that were in place, many witnesses, including you, Mr. Rubin, began with fairly compelling and very strong cases on the current failings that existed under the status quo, with very forceful arguments on the need to change. In these presentations, many excellent concerns were raised about the anxieties Canadians have around privacy, changes to technology, and things that were hitherto seemingly science fiction that are now reality.

Can you comment on where the compelling case is for the need to rewrite the act as opposed to perhaps some of the policy-based things that are in place now? I'll let maybe each of you have half a minute or so on that.

Mr. Ken Rubin: In polls and all the rest, a lot of people rank privacy as their number one concern, and I don't think they're reassured. A lot of people will say privacy is dead, but on the other hand, people need reassurance, and included in that is legislative reassurance. I think the act has to be brought up to date so that the public can feel much more confident in these times where surveillance makes privacy much more difficult. They need to know that there is some toughness and so on. If you don't bring in the order-making powers, if you don't bring in the charter, if you don't bring in other legislation, people will not feel that their leverage and their privacy rights are protected. We do need the change.

Ms. Brenda McPhail: At CCLA we have members of the public calling us. The kinds of calls we get in relation to privacy are things like, they heard on the news that CSE is tapping phones in airports and how can that be legal, or they heard that police are collecting thousands of people's data to catch a jewel thief using a Stingray device and how can that be legal.

The overwhelming tone is the sense that there's something fundamentally wrong if they can't understand that practices that are happening and which they're being told are okay really are.

There's a sense that the law is not keeping up with their expectations, that there should be limits to the amount of data about them that can be used and collected.

I talked about trust a number of times in my presentation. I think that public trust in bodies that collect people's information is eroding. You could think about it perhaps more in relation to the private sector, but having trust in government is fundamental to ensure political participation in our democratic society. It's absolutely vital that citizens believe that their government has their best interests at heart when it comes to the protection of their personal information. If they don't have that feeling, then the social licence that public bodies like national security agencies and law enforcement agencies have from the public is going to be compromised. I think we're already seeing signs of that happening. That would be my suggestion as to a compelling case.

● (1225)

Mr. Tamir Israel: I'd like to largely adopt the comments of my two colleagues and add one more example that gets a lot of attention and undermines public confidence and trust, and that's in the security context where we're getting increasingly large numbers and frequency of data breaches often with government-held data. This often leads to harm to individuals because it often leads to identity theft and other ancillary types of harm. It does erode public trust. Against the backdrop of this, this is information that citizens need to entrust to their government to participate in daily life.

In that particular subset of considerations, in addition to the ones mentioned by my colleagues, should be imposing and formalizing obligations for technical security safeguards so that the Privacy Commissioner's office can leverage the expertise it has in this field to ensure we adopt high levels of technical safeguards, imposing notification obligations so that individuals are uniformly notified when these types of breaches happen and are able to take remedial action. These types of things really are important moving forward because they're going to be more problematic down the road, not less.

The Chair: Thank you.

We now move to Mr. Saini.

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

I want to highlight a point and get your comments.

When the act was first written, we had written records and now we're moving to digital records. There's always this fear of oversharing or over-collecting of data. Right now in the act there is something where government institutions can collect data that they consider relates directly to the program they're analyzing. One of the issues, and Ms. McPhail and Mr. Israel spoke about this, is the necessity of collecting information.

How would we define a necessity test? How could we put that into legislation?

Mr. Tamir Israel: Our written comments, which we'll submit in due time, will provide you with some legislative suggestions. Many of the provincial counterparts of the Privacy Act have a necessity obligation. What it does functionally is important. You could get to the same place with the existing standard, which is information relating to an operational program. But reorienting the thinking on necessity is an important step that lets government achieve its legitimate objectives but refocuses the data practices adopted by civil servants around whether they really need a piece of information and whether they need to keep it for the length of time they have in mind.

Having necessity in there explicitly would be a defined legal standard. It would also help to reorient the thinking around data practices so that they're not over-collecting or keeping things too long.

Mr. Raj Saini: Ms. McPhail, did you have a comment?

Ms. Brenda McPhail: I would agree with Mr. Israel. I think it's really important that something in the act causes people to ask not just what they can collect, but what should they collect. Is it necessary? Is it important? Those are the things that need to be considered and the technical ways as to how you would introduce that.

We could provide some written submissions if that would be useful, but just as a general principle, the overarching idea in the age of over-collection of data is that the government is saying, “Wait. Stop. Is it necessary?” I think that's a really important foundational point.

Mr. Thomas Keenan: I'd like to make the case for data obfuscation, which is you don't always have to keep all the data and keep it exactly.

I was approached by a member of a provincial union who said their salaries are going on the sunshine list right down to the pennies they make and was that a risk for identity theft. I said you're darn right it is. If somebody calls a bank and they know your exact salary, that's another point of identity.

I suggested that be rounded off to the nearest $500. It didn't happen, so the reality is maybe governments don't need the data as precisely as they might think. They might be able to put it in ranges. StatsCan does an admirable job of making sure you can't track it to an individual when they let data back out. Nobody seems to think about that. We always seem to think we need exactly down to the penny. Maybe we don't.

Mr. Ken Rubin: The way government legislation is written, there are always exemptions to getting this or that. Why aren't there any exemptions to what's necessary? I think maybe a list of things that government has no business collecting may be one way of helping facilitate a narrower definition of necessity.

● (1230)

Mr. Raj Saini: Mr. Israel, I want to ask you a question specifically, and other people can comment also.

You have written about the importance of individual notification when there is a privacy breach. You mentioned that earlier. I was curious for a bit more detail about what kind of system that would entail. How would it work?

Mr. Tamir Israel: There is a regime now adopted in PIPEDA that could probably work very effectively in the Privacy Act as well. It focuses on notifying individuals where there is a risk of harm, and harm is defined as a way that entails there are mitigation efforts the individual could take so they should be notified in a timely manner so they can take those measures.

It also entails record keeping at the institutional level of even less harmful breaches so that we have a better picture of what's happening in security breaches, which again is going to be important moving forward so entities like the Privacy Commissioner and whatever entities become responsible for cybersecurity can look and get a clearer picture of what's happening. If there's no record keeping, if every agency is just dealing with these on their own, you don't have that holistic picture, and we're not able to keep these standards going forward.

Again, we'll try to address that more comprehensively in our written brief. Our thinking right now is that mechanism in PIPEDA roughly works in the Privacy Act context as well, but we're still trying to see if there are any specific peculiarities in the public sector context that should be addressed, if that helps.

The Chair: Thank you very much, Mr. Saini.

We now move to Mr. Kelly for five minutes.

Mr. Pat Kelly: I understand from my previous question and got an idea that there is certainly anxiety from people who are in contact with, for example, the Civil Liberties Association raising concerns about anecdotal things people hear and are trying to get a handle on new technologies and fear their implications.

There seems to be a greater anxiety around changes in technology than specific instances of breach, or specific ways in which government may have mishandled information.

What do each of you make of the commissioner's recommendation that his office receive an explicit public education in research mandate? The education around privacy, we've had talk from some of you witnesses about the value Canadians place or ought to place on privacy.

What do you make of the recommendation for an education mandate for the commissioner? I'll let each of you have a quick stab at that.

Mr. Ken Rubin: I think it's important, but I think expanding his investigative powers—that's his main job—is even more important, because right now he doesn't have all the tools in place to go to court or to make recommendations on metadata, biometric data, and all the rest.

If you don't mind, to go back to your earlier item, here's the act and you ask, why do we need it done? It's the purpose clause. When you look at the purpose clause, it doesn't talk about the right to privacy. It talks about the right of access to personal information, and that's a totally different thing. When you get to the sections on collection and retention disposal, it's a page and a half, and it doesn't say anything. It's out of date.

I think we need more than giving the commissioner more powers and explicit powers. He already does education and so on. He needs to do more audits. He needs to do more technological assessments.

In terms of the act, I think it does need updating, and I'm sorry if I'm going beyond what your question was.

Mr. Pat Kelly: Not at all, that's perfectly fine.

Mr. Tamir Israel: I want to say, and just underpin, without mitigating it we do feel that in the investigative area there are shortcomings in the substantive elements of the act that need to be addressed from a public policy perspective, as well as to ensure public confidence moving forward.

I also think the education component is important on both fronts. A lot of what we do is explain to people what is happening. Sometimes there is a tendency to overreact or under-react because the technology is so sophisticated and it's hard to understand what it's doing on the ground. An education mandate would help a lot on both those fronts, as it does already on the private sector side with PIPEDA.

● (1235)

Mr. Pat Kelly: I'll ask Mr. Keenan a question.

I was intrigued by one of the first things you said in your preamble about hackers and differentiating between good and bad hacking. Perhaps the good and bad is maybe in the eye of the beholder. If people have a fundamental right to privacy, what is a good hacker then?

Prof. Thomas Keenan: In my book the good ones are the ones who expose vulnerabilities and talk about it. A guy called me over and said, “Hey, let me show you something.“ About half the buildings in Canada are locked with a key proximity card called HID. He has discovered a way to hack it remotely. He works for a big company. He's disclosed that to the manufacturer of this card, just like a year ago when people disclosed vulnerabilities in cars like the Jeep Grand Cherokee that could be remotely hacked.

I did learn something interesting. Although General Motors and the companies behind it have put out fixes, major car rental companies haven't bothered to implement those fixes yet. You may be renting a car in the U.S. that's still hackable because they don't want to lose the revenue and take it off the line.

My point is that things have to be done. The hackers provide the information, but then it's up to whoever's responsible for the data, or the car in this case, to do something about it.

The Chair: Thank you for that answer.

Mr. Bratina for five minutes, please.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): I'm interested in the consequences of breach, material, theft of intellectual property, damage, loss of reputation, and so on. We're getting into this notion of malfeasance versus whistle-blowing. Is Snowden a hero or a villain?

Mr. Tamir Israel: Can you guys recommend amnesty, or is that outside the scope of this?

Mr. Bob Bratina: We need a recommendation.

Mr. Tamir Israel: I would say that having worked in this space pre-Snowden, we anticipated a lot of the activities he exposed and many found to be a bit disproportionate. It at least kicked off a robust conversation around the appropriate parameters of these activities.

There was no way of getting any sort of evidence, even though it was known what was happening by us, as well as by bad actors. There was no way to get the policy debate going, and having this trove of direct and credible information on what's happening on the ground, to us, was useful as a civil society organization.

My understanding was that he tried to be cautious in ensuring that the information that made it into the public record was contained and redacted in ways that didn't undermine security capabilities too much. I put that to his credit, but everyone can judge for themselves.

Mr. Bob Bratina: Mr. Rubin, do you have a comment?

Mr. Ken Rubin: I think he's performed a very valuable service. When you're talking about how we should expand the education mandate of the Privacy Commissioner, I think everybody, whether they're in the workplace or citizens, has to be vigilant or call to account things that they know about, and talk about them. These are problems that we all have to face, and so I think it's very important that a guy like that has exposed a whole set of technology and confirmed it, which otherwise wouldn't be there.

I think you should offer incentives for people—call them whistle-blowers—and some protection, for sure, for good hackers or whatnot, who are doing this kind of thing. We need more than just another educational paper on metadata. We need people who are on the front lines and are telling us what is there. This was major.

If President Obama wants to pardon him, I would not object.

Prof. Thomas Keenan: I know Snowden's parents, and his mother sent a copy of my book. I said, “Do you want it in digital form?” She said, “No, I can get stuff to him in Russia.”

He definitely did a service, there's no question about that, and in some subtle ways. For example, last year the United States Department of Defense had a “hack the Pentagon” contest. You had to be an American. You had to be a certified white hat hacker. They actually got bug reports about their own system. It's an admission that nothing can be fully secured, and there was the U.S. Pentagon admitting that. I'm not sure if that would have happened if it hadn't been for Snowden.

● (1240)

Mr. Bob Bratina: Ms. McPhail.

Ms. Brenda McPhail: I'm in alignment with my fellow panellists when I say I would come closer on the hero side than the villain. I think that, even if you just look at the conversations we've started to have now about mass surveillance, about what limits there should be, about whether it's effective, whether it's useful, all of those kinds of conversations were started once we knew exactly some of the things that were happening in the world.

I'm part of an international civil liberties group. I can tell you that people engaged in civil society work from every country have been using the information that he put out in order to start conversations in their societies about the appropriate limits of surveillance, and about the appropriate ways that we weigh privacy rights and security rights in democratic societies. I think he made a very valuable contribution.

Mr. Bob Bratina: Thanks, Chair.

The Chair: We now move to Mr. Blaikie. You have three minutes, sir. Then Mr. Long, I think we might have one minute left for you to finish your questions.

Mr. Blaikie.

Mr. Daniel Blaikie: Thank you very much.

I know there was reference made to a standard in Europe. I was just wondering if any of the panellists want to provide some other examples of good privacy legislation in other jurisdictions, and in particular some features of that legislation that you think would make sense to adopt in Canada.

Prof. Thomas Keenan: I'll just say I brought up the EU GDPR, general data protection regulation. Some people say it's the reason for Brexit, that it's 88 pages of rules. It does look a bit bureaucratic. I think it should be mined by us to look for the very good ideas that are within it, but not adopt it holus-bolus.

Mr. Tamir Israel: There are a number of regional documents. The OECD has a set of privacy guidelines, which Canada actually took a very active role in updating a year or two back. The Council of Europe has a comparable overarching data protection framework that is inspired by the European framework but is actually a little more universal and less steeped in the 85 pages of details; it's a much shorter document. That's also being updated right now, so I would keep an eye on that.

One of their recommendations in particular has to do with how to deal with transparency around algorithm decision-making, which I touched on very briefly in my comments. It's something that is going to be a problem moving down the road as governments adopt automated processes as shorthand for making various decisions. The challenge there is how you get transparency around the decision-making process without giving away the actual math, because then it could be gamed. They're working to find a way to address that, so I would keep an eye on that. We could provide some others in our written comments as well.

Thank you.

Mr. Daniel Blaikie: I have a last question about something that's curious to me.

When we talk about technology taking off and data taking off, one place where that happens is with political parties, which are gathering a lot more data now. That's not covered under the Privacy Act, because that's government. It's not covered under PIPEDA. It's not really covered anywhere. Where would any of you think is the most appropriate place, if there were going to be some regulation around the use of personal information by political parties, to place those rules?

Mr. Ken Rubin: Within the acts, I do think it should be covered.

I know the Privacy Commissioner said he'd take a pass on that. However, in India, on the access to information side, political parties are covered. Political parties handle fundraising, pretty large databases of information. With the private sector and some non-business communities now being considered for coverage, political parties should be covered and regulated in that way too.

Ms. Brenda McPhail: I would agree, and I would note that Alberta, which has recently been reviewing their PIPA document, explicitly asked as part of their review process if this should be something that is included within PIPA. We responded that it should.

Political parties are collecting vast amounts of information and subjecting it to the same kinds of data analysis that every other private and public sector body can. They're using it for very specific purposes and getting data from places that individual citizens may not expect them to get it from. All of those things warrant appropriate protection. It could be that PIPEDA is the right place, particularly since the Privacy Commissioner has said he doesn't think it belongs in the Privacy Act.

I would certainly encourage the committee to give some consideration to where you think it should go and to adding it in.

● (1245)

The Chair: Thank you very much.

Mr. Israel, quickly, please.

Mr. Tamir Israel: Briefly, I just want to say there may be some room for overlap because some of the information sometimes flows from government activity to the political parties. That could be covered by the Privacy Act and the rest by PIPEDA. That's worth considering as well.

The Chair: Okay, I'm going to thank our witnesses now.

Colleagues, we're going to suspend for a few minutes and then use the last 15 minutes to go in camera. I am going to ask our witnesses to leave the room as quickly as possible. I do want to sincerely say thank you very much. It was an excellent discourse and conversation today, and we much appreciate it. We know that if we have any subsequent questions, we can follow up with you.

Thank you very much for your contribution.

[*Proceedings continue in camera*]