HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 046 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, February 14, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, February 14, 2017

● (1545)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Welcome, colleagues, to our new meeting location.

We're going to start with our witnesses right now.

This is our first meeting hearing testimony for our new study of PIPEDA, the Personal Information Protection and Electronic Documents Act. I am not even reading that; I actually just know it, which tells you that I've been here far too long.

Welcome to our new committee space.

We have some very distinguished guests, many of whom have been before committees previously. We have Chantal Bernier, now from Dentons Canada, who has a wealth of knowledge and experience in this area. Thank you very much for being here.

From the Public Interest Advocacy Centre, we have Alysia Lau and John Lawford. We thank you both for being here.

We also have Éloïse Gratton and R. Gary Dickson who have been here before. It's great to see you both.

We'll start with your 10-minute presentations, in either official language, in the order I introduced you, which is just the order you happened to be listed in. You all know how this works. We'll wrap up at 5:30 sharp because other people have travel arrangements.

Madame Bernier, the floor is yours.

[*Translation*]

Ms. Chantal Bernier (Counsel, Global Privacy and Cybersecurity Group, Dentons Canada): Thank you, Mr. Chair.

Thank you for this opportunity to contribute to your work on the revision of the Personal Information Protection and Electronic Documents Act.

I will be giving my presentation in both languages and would be happy to answer questions in both as well.

In my presentation, I will refer to the Personal Information Protection and Electronic Documents Act as the act.

My starting point is the letter that the Privacy Commissioner of Canada sent to you on December 2, 2016, bringing to your attention four possible areas of intervention. I will add my observations from my experience as a privacy regulator and now as a lawyer in the private sector.

The first topic concerns valid consent.

Last summer, I submitted a brief further to the Privacy Commissioner's consultations on consent. I concluded that the current system of consent of the act is adequate for two key reasons. First, it has the rigour necessary to obtain valid consent. Second, it has the flexibility to ensure that consent applies to the various applications that exist on the Internet.

Consider section 6.1 of the act, which states the following:

> the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

That means the act truly allows for the complexity of the Internet, without specifying the modalities, thereby making it possible to adapt the principle to any application that emerges.

The act also recognizes the possibility of implied consent. Specifically, pursuant to section 4.3.6 of schedule 1, implied consent is acceptable in certain circumstances.

In my brief, I point out that enhancing consent involves privacy policies, which must meet three specific criteria, in my view. First, they must be written in accessible language. Second, they must be adapted to the organization. Third, they must be structured for easy consultation. This does not require any legislative change.

Furthermore, there is an improvement that does not require, but would benefit from, a legislative change. It would be to specify in the act, as European law does, that anonymization is a way to exclude personal information from application of the act.

I make that suggestion because, very often, in privacy policies, I see a paragraph advising the reader or consumer that de-identified personal information will be used for purpose X or Y. That is pointless. When identifiers are severed from the information to prevent identification of the individual, the act does not apply. I think it would be helpful to make that clear, as European law does.

● (1550)

[*English*]

The second concern brought to your attention by the commissioner is a widely shared one. That's the protection of reputation online. However, the issue is only partially in federal jurisdiction. Most of the harm that occurs to reputation online occurs not within the framework of commercial transactions but within the framework of personal relationships, which come under provincial legislation.

I will give you examples of five pieces of provincial legislation that may be helpful in that regard, and one piece of federal legislation.

Regarding provincial legislation, in British Columbia, Manitoba, Saskatchewan, and Newfoundland and Labrador, there are specific acts that say that the violation of privacy can be an actionable tort. In Quebec, a judge can prescribe measures to stop harm to reputation online.

At the federal level, there is the Protecting Canadians from Online Crime Act, which, as you know, criminalizes the online dissemination of intimate images without consent.

So there is a framework in which you can have some tools to stop harm to reputation online, but there is a legal void that remains. That legal void could perhaps be addressed through the federal act. That would be by creating—on the model of European law, and as mentioned by the commissioner in his letter—a right to be forgotten, meaning the right to erasure of certain information.

Such a provision would reduce the dissemination of personal information harmful to reputation and therefore would add some protection. In order to properly control its scope, however, I suggest that it be strictly framed with this beacon in mind: that this right to erasure would apply only to any display of personal data declared by a court as a violation of the right to privacy, with possible injunctions to stop the dissemination during trial. Still, I believe it is important to give it some solidity rather than leave it as discretionary and a burden to the platforms.

Given the seriousness of the damage to online reputation and in spite of the limited nature of federal jurisdiction in this matter, you may want to explore how the federal act could be amended to include the right to erasure as a method of reducing harm to reputation online.

The third issue brought to your attention by the commissioner concerns his enforcement powers. From my practice at Dentons, which is the biggest law firm in the world, I practise privacy law on a world level, which means that I see very concretely the disparity between the enforcement powers of our commissioner, which are actually absent, and those of his counterparts.

I cannot but observe the hold that other commissioners have on business because they can impose fines of millions of dollars. The Federal Trade Commission, for example, in the same investigation as our commissioner, can impose millions of dollars in fines, while our commissioner can only make recommendations.

France can impose fines of 300,000 euros and, interestingly, just this past February 7, Russia has increased tenfold the fines under privacy law. It's still not a big number. It's from 10,000 rubles to 35,000 rubles, which equates to about $1,600 Canadian, but it shows a trend toward increased enforcement powers. The New Zealand privacy commissioner has now recommended to his government $1 million in fines for privacy violations.

As you may have heard, the European regulation, which will come into force on May 25, 2018, does provide for fines of up to 4% of a company's global revenues.

That said, the Canadian commissioner's officer is performing quite well, especially with the right to name companies, because reputation is such an important asset. On the one hand, we have to weigh the advantage of this ombudsman model, which, according to the private sector, favours collaboration between regulators in business and the worldwide peculiarity, I would say, of our commissioner.

However, I have to tell you that in my experience as both a regulator and a privacy counsel to business, I do not see enforcement powers as the determining factor in collaboration, but rather good faith on both sides. That's what really matters.

● (1555)

Also, the imposition of sanctions is not necessarily bad for the private sector, because it evens the playing field. You have good organizations that invest the money up front and, therefore, get good results on privacy protection, and you have negligent organizations that fail to make the upfront investments and, therefore, pay the fine at the end. A lot of good organizations will tell you, “Thank you. You've just evened the playing field.”

That said, comparing the enforcement powers of the Canadian office with the rest of the world favours an upgrade, but I would like to put some parameters around that.

I encourage you to explore the possibility of creating a power to impose fines, but framed rigorously as follows. First of all, I think the fine should be imposed only if there is evidence of negligence. Incessant attacks and uncertainty in the breadth and scope of the law mean that organizations cannot be required to ward off every blow. It's unfair.

Secondly, the fine should be payable, obviously, to the receiver general. There are some data protection authorities where the fine is payable to the data protection authority. It creates a conflict of interest. It should be subject to the Federal Court. Obviously, and this is of huge impact, it has to be appealable.

Finally, as in the case of the European regulation, I would favour the fine being a percentage of annual revenues, because the use of personal information is part of profits. Therefore, the misuse of personal information should be part of financial loss. There is a logic there that I believe recognizes the monetary value of personal information. Secondly, it matches the investment that is required to be made upstream and leaves the issue of damages to the courts, where that would be more appropriately dealt with.

[*Translation*]

The fourth subject that the commissioner brings to your attention is, in my view, the most urgent. Why? Because it concerns the new General European Data Protection Regulation, which will come into force on May 25, 2018. The regulation considerably changes European legislation on personal data protection and puts our adequacy status at risk. Allow me to explain.

The issue is economic. Canada has the status of suitability to Europe, which allows Canadian companies to receive European data without any other form of authorization. This is a crucial competitive advantage. We could lose our adequacy status for two reasons. First, the new regulation provides for the review of adequacy status every four years, which means that our status will be questioned. Second, we will be evaluated against the standards in the new regulation, which are very different from those in the current federal legislation. The problem is that our rules are not in line with the new regulation.

In short, we could lose a major competitive advantage. Canada is the only North American state to have the status of suitability to Europe, so I encourage you to consider the issue.

On that note, I would be happy to answer any questions you have.

● (1600)

[*English*]

The Chair: Thank you very much, Madame Bernier.

You went a little bit beyond the 10 minutes there, but given your capacity as a former commissioner, I thought that we would do that.

Mr. Lawford, are you the one bringing remarks from your organization?

Mr. John Lawford (Executive Director and General Counsel, Public Interest Advocacy Centre): I'm beginning.

The Chair: All right.

Mr. Lawford, the floor is yours.

Mr. John Lawford: Thank you, Mr. Chairman.

The Public Interest Advocacy Centre is a national, non-profit organization and registered charity that provides legal and research services on behalf of consumer interests, in particular vulnerable consumer interests concerning the provision of important public services. We have been deeply involved with PIPEDA from before its passing.

Five years ago, we came to this committee to talk about privacy and social networks. Today, we come to discuss your review of PIPEDA. It is still about social media, but this time it has brought along its friend, big data.

Social networks and most smartphone apps routinely gather personal information as defined by PIPEDA, and retain that information on central servers. That information is then used, as permitted by PIPEDA, to target advertisements to that person, their friends, families, and colleagues on social media.

The term for this is “behavioural advertising” or marketing, as the vast amounts of very personal data, including one's preferences as to a myriad of products, previous purchases, location, age, gender, ethnicity, and much more, allow advertisers using this information to target these ads to your presumed behaviour and profile.

They call it “big data” when advertisers or other companies are able to combine data sets from various apps and website visits, and even from only one site over a long period. Then data mining occurs, using algorithms to look for patterns that suggest how successful targeting ads may be, or even attempting to find presumed ways to know or influence your future behaviour.

The companies doing this will tell you today that they are doing it lawfully under PIPEDA, that they have privacy policies, that they have your consent, and that they follow all the rules of sharing and processing data. The fact, though, is they often do not have your informed consent. Informed consent, whereby you understand the consequences of the provision of your information and what it will be used for and how it will be shared, is the standard for collecting, using, and disclosing information under PIPEDA.

Companies now are asking and beginning to ask that the consent standard be changed, largely because it impedes data gathering and big data. They will ask you to abandon informed consent as the standard that protects consumers and the reasonable expectations and conceptions of privacy. They will ask you for a risk-based model, or more implied consent. This should be resisted. Indeed, PIPEDA needs to enable the informed consent standard, and all it needs is some new rules to protect that and consumers.

Moving now to enforcement, if we are to address the problems with online privacy and big data, the Privacy Commissioner of Canada needs real enforcement powers, including a mandatory order-making power and an AMP or fining power.

PIAC advocated for these powers at the first PIPEDA review in 2008. At that time, the Office of the Privacy Commissioner did not want them. Then the OPC crossed swords with Facebook in a complaint in 2010. After that, Jennifer Stoddart asked you and the government repeatedly and loudly for order-making power and fining power. Her reasoning was that her office could not make large social media companies comply with only non-binding findings and name and shame.

Mr. Therrien, the current Privacy Commissioner, is more careful, and he may ask you only for order-making power. This will be cumbersome to enforce in court. You should also be giving him fining power.

In any case, if the Privacy Commissioner says that he or she needs it to do the job, why not give it? The OPC is up against the biggest corporations in the world right now, and needs tools. It is frankly embarrassing that provincial privacy commissioners have this power and not the Office of the Privacy Commissioner. Only by enforcing the present standards in PIPEDA can we see if it is effective or needs change. It's unfair to judge the act without enforcement.

Moving now to children, a new rule is needed regarding the treatment of children's privacy. I saw an extraordinary op-ed last week. In it, Owen Charters, the president and CEO of the Boys and Girls Club of Canada, said:

> The Wall Street Journal reports that...children's websites in the US install more tracking software than sites aimed at adults. These tracking tools follow our children as they surf the web, collecting data about their behaviour and interests. This information is often sold to marketing companies.
>
> There are endless public awareness campaigns dedicated to cyberbullying. Change is happening. But with the focus on those discussions, children's privacy rights in Canada have been placed on the back burner.

That a general children's welfare charity would underline online privacy is indeed telling. This letter closes with an exhortation to the Canadian government to pass a dedicated children's privacy act.

● (1605)

Our sentiments are similar, but we think that this protection can be added to PIPEDA. We have first-hand insights on the problem. In 2011, PIAC brought a privacy complaint against Nexopia.com, a social network based in Alberta and largely aimed at the teen audience. The Office of the Privacy Commissioner upheld all of our complaints, which were focused not so much on online safety, but on targeted marketing to minors.

Unfortunately, besides some voluntary guidelines from the Office of the Privacy Commissioner, we see no improvement in children's privacy in Canada since then. We have a detailed proposal to address this—and Europe is also adding regulations—but given our time to present, we invite you to ask about these solutions in your questions.

Ms. Alysia Lau (Legal Counsel, Public Interest Advocacy Centre): Good afternoon.

Another area that requires a new rule is data retention and destruction. Can consumers in the future be sure that the information they have provided, or that was extracted from their habits, will be destroyed or no longer used when the reasons for why they gave that consent are gone? Will they have control? Some of those present today would say no.

We say that now is the time to erase. PIPEDA states that personal information must only be retained for as long as necessary to fulfill an organization's stated purpose. However, the act only requires organizations to develop guidelines and implement procedures regarding the retention of personal data. It says that personal information that is no longer required to fulfill the stated purposes should—not shall—be destroyed, erased, or made anonymous. This is not strong enough.

The only OPC findings that Nexopia refused to implement, to the point of being taken to court by the OPC, were those requiring them to erase the personal information of teens who had left their service. As Canadians can now spend years, decades and, in the case of children, possibly their entire lives on an online service such as a social networking website, the amount of personal information collected from a user could be staggering. The more information on individuals that an organization has and the longer they keep it, the greater and more serious the risk of a data breach.

Canadians must have choice and control over the ways their personal data is used, including through consent, rectification of information, and especially the removal or erasure of their information.

A right to erasure was recognized in the European Union's recent general data protection regulation, which comes into force in 2018. The new GDPR codifies what is known as the “right to erasure”. This gives individuals the right to have personal data erased and to prevent the processing of their data when, for instance, the individual withdraws consent or objects to the processing and there is no overriding legitimate interest for continuing it.

Organizations are also required to be particularly sensitive when it comes to personal data shared by children on, for instance, a social networking site. They can only refuse in certain circumstances to erase personal data when requested, such as to comply with legal obligations or to exercise freedom of expression.

PIAC submits that the committee should consider recommending similar rules for PIPEDA that would align with the GDPR's protections. For instance, organizations should be upfront with users about how long they intend to retain their personal data and why. They should also be required to erase or destroy personal information once the data is no longer needed for a stated purpose, or when an individual withdraws consent.

● (1610)

Mr. John Lawford: In our 2012 remarks, we suggested related-party tracking and reporting of data flows, a do-not-track list, and privacy impact assessments for social networks and other businesses before they launch major services using personal information. In our recent submission to the OPC on the question of interpreting consent in the online context, we suggested the implementation of standard privacy preferences and a trustmark system.

We urge the committee to consider these forward-looking questions on how to support the present PIPEDA informed consent standard, as Canadians grapple day-to-day with the consequences of targeted marketing and big data.

We thank you for your attention, and we look forward to your questions.

The Chair: Thank you very much, Mr. Lawford and Ms. Lau. It is very much appreciated.

We now move to Ms. Gratton, please, for up to 10 minutes.

[*Translation*]

Dr. Éloïse Gratton (Partner and National Co-Leader, Privacy and Data Protection Practice Group, Borden Ladner Gervais, As an Individual): Thank you for inviting me. I am pleased to be here today. I appreciate the opportunity to share with the committee my thoughts on important issues affecting Canadians and their privacy.

I am a partner at Borden Ladner Gervais, and I teach in the faculty of law at Université de Montréal. I am appearing before the committee today as an individual.

I will be discussing two issues that have been the subject of consultations undertaken by the Office of the Privacy Commissioner in the past year: meaningful consent, and reputation and privacy. I will also say a few words about enforcement powers. I will be giving my presentation in English but would be happy to answer questions in English or French.

[*English*]

PIPEDA is based on fair information practices that were initially drafted in the early 1970s. We should keep in mind that their main purpose was to address specific concerns pertaining to computerized databases and the fact that different private sector organizations could exchange personal information more easily without the knowledge or consent of individuals. At that time, the best way to deal with these new concerns was deemed to have individuals keep control of their personal information.

Forty years later, this concept is still one of the most predominant theories of privacy and the basis for data protection laws around the world, including PIPEDA. The notice-and-choice approach is no longer realistic. Individuals are overloaded with quantities of information they cannot realistically be expected to process or comprehend. As raised by the OPC, the complex information flows and new business models involving a multitude of third parties have also challenged the traditional consent model.

A first issue, if we want to maintain that consent model, is whether we should be amending PIPEDA on the issue of consent. Jean Carbonnier, one of the most prominent French jurists of the 20th century, has stated in French, *"Ne légiférer qu'en tremblant"*. What he meant was that we should be very cautious when enacting or amending laws. We have to be careful to make sure that the amendment will not be detrimental or problematic as soon as new technologies emerge. The current wording pertaining to obtaining consent under PIPEDA is quite flexible and definitely flexible enough to accommodate new types of technologies and business models.

However, the downside of this flexibility is that it creates uncertainty. Therefore, policy guidance on enhancing transparency and obtaining valid consent is increasingly necessary to address some of this uncertainty and allow organizations to innovate without taking major legal risks. Businesses look up to the OPC to provide such guidance and its recent guidance on online behavioural advertising, app development, and the Internet of things is quite useful. These documents are, more than ever, relevant and timely.

Under PIPEDA, in determining the form of consent to use, organizations shall consider the reasonable expectations of the individual. What these expectations are in any given context, and whether certain activities are legitimate from a privacy perspective, is often a function of many factors, including the prevailing social norms. Another argument against amending PIPEDA on the notion of consent pertains to the fact that social norms in connection with any new technology or business practice may not yet be established. The OPC has, in recent years, commissioned certain surveys meant to explore the awareness, understanding, and perceptions of Canadians on certain issues and new technologies. These studies are increasingly important, since they allow us to gain a better understanding of consumers and their expectations and help evaluate how the social norm in connection with a given technology or business practice is evolving.

Over the last few years, I have proposed, through various publications, that perhaps part of the solution to address some of the challenges pertaining to the consent model could include the adoption of a risk-based approach or interpretation, under which we would focus on obtaining express consent only for data collections, uses, or disclosures, if such activities might trigger a risk of harm to individuals. For instance, express consent would be required when using personal information to make an eligibility decision impacting the individual, a disclosure that would involve sensitive or potentially embarrassing information, or a practice that would go against the expectation of the individual.

A risk-based approach may allow organizations to streamline their communications with individuals, reducing the burden and confusion on individual consumers, since they would receive fewer requests for consent. These requests would be meaningful in the sense that they would focus on what matters to them. Although this type of approach would imply rethinking PIPEDA's current consent model to some extent, it could be further explored in the foreseeable future.

● (1615)

Regarding online reputation, the Office of the Privacy Commissioner of Canada recently chose to make reputation and privacy one of its priorities for the next few years, and launched a consultation last year in which it asked if there were a way to apply a right to be forgotten in Canada. With Internet technologies, there is a temporal shift, in the sense that pieces of information can outlive the context in which they were initially published and considered legitimate. Security expert Bruce Schneier stated a few years ago: "We're a species that forgets stuff.... We don't know what it's like to live in a world that never forgets."

The right to be forgotten is the right famously coined by the Court of Justice of the European Union in its May 2014 landmark decision, in which it authorized an individual's personal information pertaining to past debts to be removed from accessibility via a search engine. While this right may sound appealing at first, especially in view of the protection granted to the privacy and reputation of individuals, this issue is more complex. Aside from the constitutional challenges that a right to be forgotten would raise, there are significant risks with entrusting private entities, such as search engines, with the task of arbitrating fundamental rights and values. A decision to de-index content is quite complex as it would require considering numerous criteria. It would fall to search engines to enforce this right, and these companies would have an incentive to err on the side of more removal rather than less in order to reduce costs or to avoid potential legal liability.

Courts, unlike private sector entities, have the expertise and independence to strike an appropriate balance between the two fundamental values that are often opposed in these types of requests, namely freedom of information, freedom of expression and privacy. On this issue, the Federal Court of Canada recently issued a decision in the Globe24h case, illustrating that courts should be the ones issuing orders to remove information from Google search results.

Quebec has a very stringent privacy and reputation legal framework in place. The right to privacy has been elevated to the rank of a fundamental right, protected by the Quebec Charter of Human Rights and Freedoms. The Civil Code of Quebec prohibits the publishing of someone's "name, image, likeness or voice for a purpose other than the legitimate information of the public". While recovery for defamation in common law jurisdictions may be barred if the statements are true, in Quebec the fact that information published is true does not suffice to avoid liability.

This said, even with this stringent legal framework in place, some challenges in addressing online reputation issues remain. First, the notion of *res judicata* may prevent an individual from going before the courts and asking that certain information be removed if this request was made in the past and already decided upon. Periods of limitation must also be revisited to ensure that this legal framework can adequately address the fact that with the Internet, data legitimately published may, after a certain period, become irrelevant, or the fact that the data that was once considered outdated may become relevant again over time.

Second, pursuing litigation can be quite expensive, which may not make this type of tool or recourse always accessible. Perhaps efforts should be directed to improving our legal framework, notably by increasing access to justice or implementing a fast-track system for online removal requests, rather than by copying a European-style right to be forgotten.

Finally, the right to be forgotten includes extraterritorial issues that should be considered. The Federal Court of Canada, in its recent decision, opened up an important debate on the jurisdictional reach of privacy laws. All eyes are now on the Supreme Court of Canada, which will be rendering its decision dealing with these issues in the Equustek v. Google matter in the near future.

Regarding enforcement powers, the former Privacy Commissioner of Canada, Jennifer Stoddart, has asked for stronger enforcement powers under PIPEDA, which could include order-making powers and the power to impose penalties or statutory damages. In foreign jurisdictions, privacy regulators have such powers. This could provide an additional incentive for Canadian businesses to protect the personal information under their control. This being said, I wanted to raise one concern. As mentioned earlier, PIPEDA is based on flexible technology-neutral principles. The benefit of this flexibility is that it can accommodate new types of technologies and business models, but the downside of this flexibility is that it creates uncertainty: it is not always clear for businesses how they must comply with PIPEDA, especially when launching new products or services or innovative technologies. If on top of this uncertainty, there is also the risk of statutory damages or penalties, I am concerned that businesses will hesitate to launch new products and services and that in the end this will affect innovation and our competitive advantages as a nation driven by research, development, and innovation.

● (1620)

I am of the view that any enforcement powers, penalties, or statutory damages should come into play only once a certain practice is clearly illegal and once the organization has been advised of such and is refusing to adjust its business practices.

As a final thought, I have some concerns with the adequacy test that Canada will undergo in the coming years. The European general data protection regulation coming into force in 2018 will include certain new rights that are not currently in PIPEDA: a right to be forgotten and a right to data portability, to name a few.

We have important issues on our plate to ensure that our current data protection regime will survive and remain relevant in the near future. We have some challenges with our current notice and choice model, and perhaps addressing these issues should be our priority.

I have made written submissions in response to the OPC's consultation on privacy and consent and their call for essays on online reputation. My submissions are available on the OPC's website.

Thank you, and I welcome questions.

The Chair: Thank you very much, Madame Gratton.

We now go to Mr. Dickson, please, for up to 10 minutes.

Mr. Robert Dickson (Consultant, Former Saskatchewan Information and Privacy Commissioner, As an Individual): Good afternoon, Mr. Chairman and members.

My comments will be focused specifically on the four issues identified by the Privacy Commissioner in his December 2, 2016, letter to this committee.

The overriding concern I'll commence with is ensuring that PIPEDA works better when it comes to small and medium-sized businesses. For brevity, I'll refer to them as SMEs in the course of my presentation. I was involved in the development of PIPA in Alberta. I co-chaired a working group of Alberta privacy lawyers who were providing advice to the people drafting the legislation that became PIPA. Much of the input from the lawyers participating was animated by a focus on small and medium-sized businesses. PIPEDA, at least at the time, was seen as better suited to large banks, airlines, and national corporations but not so well suited to the neighbourhood bookstore.

When I was the Saskatchewan Information and Privacy Commissioner, my office partnered with the Privacy Commissioner of Canada's office to undertake a program called privacy made easy. This was focused on businesses on the Prairies. In meetings with business organizations, we found a remarkably low level of PIPEDA compliance by small and medium-sized enterprises. In fact, I'm disappointed to say, we found even a remarkably low level of PIPEDA awareness.

Dealing first with enforcement powers, I support the commissioner's recommendation that his office have order-making power. That aligns his office with most of the major international data protection authorities as well as the Canadian provinces with private sector privacy laws.

I want to acknowledge that the current ombuds office probably works quite well for large corporations in Canada, which achieve a high level of PIPEDA compliance, I think. That may be because of more capacity and it may be attributable to a more sophisticated recognition that privacy compliance is a good business practice.

I'm interested in the conclusions of a 2010 study that had been done for the Privacy Commissioner of Canada. It concluded that there's a differential impact on different sized businesses by the role of the Privacy Commissioner of Canada, as SMEs tend to be more sensitive to financial risk and penalties. Furthermore, the deterrent effect of avoiding intervention by the Privacy Commissioner would be more effective with SMEs if the Privacy Commissioner of Canada had order-making power and the ability to impose penalties.

Another reason I support order-making is that it leads to the creation of a body of precedents, more detailed orders than the current summaries provided by the office. These would serve to provide businesses with much clearer direction as to how PIPEDA is being interpreted and applied.

In terms of the GDPR—the general data protection regulation—alignment makes sense from the perspective of international trade. I would submit, however, that it's important not to lose sight of the private sector privacy laws in Alberta, British Columbia, and Quebec, as well as the substantially similar health information laws in jurisdictions such as Ontario, Newfoundland and Labrador, New Brunswick, and other provinces that will soon achieve the substantially similar designation. Any changes to PIPEDA would necessitate a similar review of each of those substantially similar provincial and territorial laws.

I'm not sure that data portability and privacy by design are not already captured by PIPEDA. Data erasure appears to have no PIPEDA counterpart, however.

On reputation and privacy, I don't support a right to be forgotten. I simply don't think it could survive a charter challenge.

As a former commissioner, I was very concerned with the issue of public registries that were created long before we started to worry about data profiling, data matching, and identity theft. The response needs to be to encourage more scrutiny at the time registries collect the information and ensure non-collection of anything not essential to the purpose of the registry.

● (1625)

When Chantal Bernier was assistant privacy commissioner of Canada, I recall that she led a collaborative initiative with provincial commissioners to create a set of guidelines dealing with the Internet publication of administrative tribunal decisions. So there certainly is an issue that can be addressed, but I'm just not sure the right to be forgotten is going to be the answer.

I think freedom of expression in the charter limits what could be done. If you cannot compel a media outlet to take down content, then I contend you cannot stop a search engine from communicating to the world that the content exists.

Regarding meaningful consent, I'm going to submit to you, Mr. Chairman and members, that some useful privacy lessons have been learned from the Canadian experience with electronic health records, where the role of consent has been significantly diminished, notwithstanding the fact that we're dealing with some of the most sensitive and prejudicial information that Canadians have. I'm thinking particularly of Alberta and Saskatchewan, which have a largely completed electronic health record for every citizen. This allows thousands of providers in all parts of the province the opportunity to look at prescription drug profiles, laboratory test results, diagnostic imaging pictures, radiology reports, clinical notes from providers in hospitals, and immunization information on anyone in the province. Of course, they're not supposed to be viewing this material unless they have a legitimate need for the purposes of diagnosis, treatment, and care, but the point is they have the ability to be able to access that information. With funding from Canada Health Infoway, all other provinces are working to develop a similar system which should be interoperable with that of all other provinces and territories.

And we've certainly learned over the last decade that apart from the question of consent, there's a compelling need for other privacy enhancing features. At the top of my list would be a privacy management program to ensure a coordinated approach to PIPEDA compliance, because what you tend to see too often among health care providers is a fragmentation: a policy here, a policy there, and not appropriate coordination and leadership. So a privacy management program is an important feature.

There's also a need for a proactive audit program that's made known to all employees. Too often, organizations like to boast that they have an audit capability with the electronic system they've got. That isn't very helpful or very useful if there isn't an ongoing proactive program and all staff that have access to that sensitive information are aware that this capacity exists in the organization.

Furthermore, we need strengthened regulatory oversight both by commissioner offices and also regulated professional bodies.

We could spend hours talking about the development and expansion of secondary use of personal health information and big data. The historic view is that if you're dealing with identifiable patient information, if you're using it for the original purpose—namely, that it was collected for diagnosis, treatment, and care—you don't require additional consent, but if you're using it for research purposes, you would then typically require the express consent, unless you have approval from a research ethics board that says consent isn't necessary.

There are significant issues around that and then the need for hard safeguards.

Unlike Australia and the system they have there known as My Health Record, where there's a requirement that patients must opt in to the electronic health record system, in Canada we have compulsory enrolment of all Canadians and uploading of their personal health information to the system. They're not invited or asked whether they consent. The system of electronic health records is based on implied consent, not express consent. Moreover, implied consent typically requires transparency at the point of collection about the kind of PHI that's collected and how it will be used and disclosed. Implied consent typically requires that an individual can elect to opt out. The kind of masking that's offered in the electronic health record system we're building in Canada usually offers patients something quite different, and certainly something much less than an opt out.

● (1630)

Patient privacy, as we've seen in our experience over the last decade, is typically reinforced by a number of soft safeguards, including an oath or pledge by all health care workers to protect privacy; written policies and procedures for the collection, use, and disclosure of personal health information; training of staff; and an audit trail of those who view anyone's PHI.

The experience, though, is that despite these soft safeguards, we've experienced something of a rash of snooping incidents. You have read about that, because we have, I think, pending class actions in at least five Canadian provinces that come from unauthorized people snooping in patients' personal health information. This has sharpened the focus on hard safeguards to backstop the soft safeguards.

I'd recommend that if you're looking—as the commissioner has invited you to do—at possible alternatives or enhancements to consent, you might want to consider the kinds of hard safeguards that have been developed for electronic health records. These would be dismissal for cause or other disciplinary action by employers, prosecution, and fines—if you look at the stand-alone health information laws, they have huge fines—class-action litigation, and disciplinary action by professional regulatory bodies.

I say that on the issue of consent and determining whether there are some alternatives, there's some valuable experience to consider and to draw from when we look at electronic health records as we see them now in Canada.

Thank you very much, Mr. Chairman.

The Chair: Thank you very much.

We've heard from four witnesses, colleagues, and already we have a whole bunch of testimony that is conflicting or.... This is going to be an interesting study.

I'm sorry; I shouldn't be adding any commentary, but I'm sitting here trying to go through everything you just said, Mr. Dickson, and I'm thinking, “Oh, my goodness”, because if this is true, then we're going to have a great many issues arising out of this study.

Without further ado, though, I'll turn it over to my colleagues here in the committee.

Mr. Massé, you have up to seven minutes, please.

● (1635)

[*Translation*]

Mr. Rémi Massé (Avignon—La Mitis—Matane—Matapédia, Lib.): Thank you, Mr. Chair.

I'd like to begin by thanking you for contributing to the committee's important work.

I had a host of questions, but something in particular you said, Ms. Bernier, caught my attention. You referred to an issue you considered urgent: the preservation of the adequacy of the act under the new General European Data Protection Regulation. You said that Canada was the only North American state with the status of suitability to Europe but that our status was at risk because it would be subject to review every four years. According to you, the Canadian act needs to be raised to the level necessary to preserve the advantage that adequacy status with Europe affords Canadian businesses.

What steps do you recommend we take to raise the level of the Canadian act?

Ms. Chantal Bernier: Unfortunately, it will take legislative measures. I say "unfortunately", because legislative measures require the most effort.

As Ms. Gratton mentioned, the new European regulation recognizes the right to erasure, whereas the Canadian act makes no mention of it. The new European regulation also recognizes data portability, in other words, a consumer will have the right to request that their personal information held by an organization be transferred if that person wishes to work for another organization or become the client or consumer of another company.

Mr. Rémi Massé: Would the transfer happen with or without the individual's consent?

Ms. Chantal Bernier: Let's assume I do business with organization X but I now want to deal with a competitor. I will have the right to tell organization X to transfer my data to organization Y, with whom I will be doing business going forward.

I can give you another example. In some cases, a privacy impact assessment will be required before a practice or program can be introduced. The regulation is creating a whole slew of new rights that do not exist in the Canadian legislation. I am going to speak frankly, if I may. The European Union has learned from its mistakes. In fact, Europe may have granted adequacy status somewhat randomly. Currently, the new regulation sets out stricter criteria, so it is necessary to align with European law.

Further to its review of Canadian law, the EU will study PIPEDA to determine whether it meets the desired standards for adequacy status. If the answer is no, it will have consequences for Canadian companies looking to receive information from European companies —and that includes something as simple as having a website that Europeans can access. Canadian companies will have to negotiate standard contractual clauses, which are very burdensome binding clauses approved by the European Commission, negotiate binding corporate rules, which are internal rules, or obtain individual consent, which is not easy to obtain in the case of every transaction.

Canada has adequacy status, while the U.S. does not. The Americans just negotiated the Privacy Shield for that, but the coverage is legal, not territorial. Mexico does not have it either. We have a competitive advantage that I don't think we want to lose.

Mr. Rémi Massé: Thank you. That's much appreciated.

Now, I'd like to get into consent because it's an even bigger concern for us. This question is for Mr. Lawford and Ms. Lau.

PIPEDA of course requires organizations to obtain people's consent in order to collect, use, or disclose information. In the digital information age we live in, Canadians give their consent to a number of organizations, allowing those organizations to collect, use, or disclose their personal information.

I'd like to know your thoughts on a particular situation. In order to use an application or a tool, Canadians will, often automatically, tick the little box hastily to give their consent. I'd like you to comment on that and tell us your view on how to deal with the situation in order to protect Canadians' personal information.

● (1640)

Mr. John Lawford: Right now, at the Public Interest Advocacy Centre, we are exploring ways to fix that problem.

As I said in my opening remarks, we considered the possibility of having standard parameters to make sure that, as soon as people visit a site, be it a social media or other site, the same options are always presented to them, where possible. That's one idea.

We are also working on a report in which we examine ways to present users with options in a much clearer fashion that requires less effort from young and old alike, particularly for those accessing app-based services.

There are steps, then, that can be taken to make things better. That said, problems in this area persist around informed and valid consent, but I don't think that's a reason to throw in the towel. The principle is sound, so we shouldn't throw the baby out with the bathwater.

Mr. Rémi Massé: Thank you, Mr. Lawford.

Ms. Gratton, you piqued my curiosity when you talked about the provisions in force in Quebec. The adjectives you used to describe Quebec's framework made it sound rather effective.

I'm not a lawyer, but I'd like you to comment on measures in place in Quebec that should guide us in producing our recommendations.

Dr. Éloïse Gratton: Yes, absolutely.

It's a privacy and reputation framework. In Quebec, privacy rights are protected by the Quebec Charter of Human Rights and Freedoms, which applies to the private sector. The civil code also has provisions to protect privacy and reputation rights.

The cornerstone is the measure prohibiting the publication or dissemination of certain personal information such as an individual's name or photo without their consent. The underlying principle is the individual's consent, unless the information is in the public interest.

If the information is disseminated, the courts review the published material in order to determine whether it was in the public interest at the specific time in question. They also weigh freedom of expression and information against the right to privacy and reputation.

Some of the case law is over a hundred years old. It's fascinating to see how things have changed over time, what is in the public interest and what is not, and what is acceptable and what is not. One last point I'd like to make with regard to reputation is that the information cannot be published merely because it is true. A test is administered to determine whether the information is in the public interest.

Despite this framework, two issues persist with respect to the right to be forgotten and the right to erasure.

The first issue is *res judicata*, or the matter judged. Say my personal information was published and I went to court to have a judge consider the matter. A different decision could be handed down in 10 years, but the court could consider the matter judged, in other words, already decided upon by the courts. That's something to keep in mind in order to move forward within this legal framework and deal with online reputation issues.

Clearly, the other problem is—

[*English*]

The Chair: Ms. Gratton, we're several minutes over Mr. Massé's time. I was waiting for a break and one wasn't coming. We'll have to take an opportunity to finish that later.

We'll now move on to Mr. Kelly.

[*Translation*]

Dr. Éloïse Gratton: Very good.

[*English*]

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you.

To begin, Mr. Dickson, I'd like to zero in one part of your opening remarks. You spoke about conducting compliance audits in, I'm not sure where—if it were in Saskatchewan or Alberta, or both—and about finding a generally low level of compliance and even awareness of PIPEDA. I'm not surprised that you have found that.

Not complying with certain required practices or protocols is certainly a potential problem, but I'd like to know whether you found actual breaches of privacy, widespread breaches of privacy, and evidence of harm done to Canadians as a result of non-compliance with PIPEDA.

● (1645)

Mr. Robert Dickson: First, for clarity it was in the province of Saskatchewan that we were undertaking this. Saskatchewan does not have a PIPA and is subject fully to the federal PIPEDA.

I first have to stress that in this pilot project, which was launched by the Privacy Commissioner of Canada and my office partnered with it, we weren't specifically looking to determine who was compliant and who wasn't. The focus was on determining whether there were things that could be done firstly to chart to what extent people were conversant and compliant and then to chart some strategies for those who were not.

Chantal wasn't directly involved at the time with the project, which was done by the federal office. The pilot project didn't end up producing a final report. I think we would have to say that there were some problems with the process, and so the pilot project did not get to a final report.

Certainly we found organizations that didn't have a privacy officer, that didn't have appropriate policies and procedures for their staff to follow to ensure that privacy was being protected. These are requirements, for organizations to be able to meet the requirements of the statute.

I'm not sure I'm being entirely responsive, but we weren't keeping track of people who were in violation; we were having meetings with groups of people and determining their level of awareness. We found that the level of awareness was not satisfactory and then found that there were a number of supports and tools and resources that they didn't have and needed to have, to be compliant.

Mr. Pat Kelly: I'm certainly not surprised that you would go to a small business with, say, a dozen employees, and find there was perhaps not awareness that someone in each had to be designated as a privacy officer and had to undertake certain functions to be compliant.

What I really want to know and what I didn't get was whether even by anecdote, since you mentioned this process didn't have a final report, you saw evidence of harm done to the customers of these small businesses. Did you see evidence of breaches of consumers' privacy?

Mr. Robert Dickson: Because we weren't dealing so much with consumers—our dealings were with organizations—we didn't have a lot of organizations coming forward and—

Mr. Pat Kelly: You talked about focusing on small and medium-sized enterprises at the beginning of your remarks.

Mr. Robert Dickson: Well, that's right.

Mr. Pat Kelly: Were these small businesses that you went in to?

Mr. Robert Dickson: They were small businesses. What we found, generally speaking—though there were some exceptions, as you would expect—that there was an incredibly low level of awareness of PIPEDA and what was required of an organization to ensure that it was collecting the least amount of information needed for the purpose, and that it didn't keep personal information longer than it had appropriate need for it, and those kinds of things.

We found that those rules weren't being followed.

● (1650)

Mr. Pat Kelly: Again, you don't know whether harm resulted from the non-following....

Perhaps I will let you answer the question, then. Mr. Dickson didn't seem to have—

Ms. Chantal Bernier: Absolutely.

One investigation that pops to mind was of a new start-up selling widgets on the net. They were clearly very excited about their new business and didn't think about privacy. What they were focused on was being a nice start-up on the internet, until one of their customers said, I've been defrauded of so many thousands of dollars. The start-up did not find the breach themselves. Then another customer said, I've been defrauded. Then everyone tracked it down to them, and sure enough, it was them.

There are tons of examples like that. In fact, many big companies will tell you that their weakest link is the SMEs that are in their supply chain. Much of the attention is turning there.

The answer to your question, then, is yes, absolutely there is harm.

Mr. Pat Kelly: Okay. Excellent.

The Chair: You have about a minute.

Mr. Pat Kelly: I don't know if we can really tackle a big topic in a minute, but I'll maybe just throw it out. I don't know if we have time to address it, but could you talk about some of the distinctions between informed and implied consent?

We have talked about quite a bit of this, and in any enterprise, particularly a small one, when you are at a point of sale or are trying to disseminate information that may lead to a sale, complying with requirements under law while being able to give the customer what they want—information—is a difficult business.

Perhaps in the next round....

The Chair: When I tell you that you have a minute left for a question and you make your question a minute long, you run out of time.

Some hon. members: Oh, oh!

The Chair: Mr. Blaikie.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): I recognize that you are all here as privacy experts and not as trade experts, but we just came off a third reading vote on the comprehensive economic and trade agreement. It is supposedly an agreement to eliminate non-tariff trade barriers between Canada and Europe and to give some assurances to Canadian companies that when they are trading with European companies, they are not going to run into difficulties of the kind that have come up.

As the only person on the committee who voted against that agreement, I'm interested to hear that there are some considerable issues with respect to what would be called non-tariff trade barriers that weren't addressed in CETA.

Can you expand a little bit more on what's missing from that agreement and on how we make it so that Canadian companies are not going to lose an advantage that they currently have, in spite of having just signed an agreement that's supposed to facilitate trade with Europe?

Ms. Chantal Bernier: The only way we can protect them is to work now at making sure that by the time our adequacy status comes under review in Europe, we have shored up our privacy protections to that level. It doesn't mean that they're exactly the same, but that the Europeans will find them adequate. Otherwise, every time we want to deal with Europe—a market of 500 million people who have money, so we want to have that competitive advantage—we will have to go through very onerous clauses.

The answer to your question goes back to what I said to Mr. Massé: we need to shore up the act now so that it passes the test after 2018.

Dr. Éloïse Gratton: Perhaps I could have a few words?

The Quebec data protection law was deemed substantially similar to PIPEDA. We've had this law since 1993. It's probably the most stringent across Canada. Europe looked at our law in 2014 and decided that it was not adequate—that there was question mark in its regard. So I have an issue with the adequacy of Europe's assessment or methodology.

Ideally, of course, we would like to pass that test, but I still have some concerns.

Mr. Daniel Blaikie: Thank you very much.

Madame Bernier, you mentioned that if the commissioner were to have the power to fine, it would make sense to base it on the company's global revenues.

Then you talked briefly about profits. Just for clarity, are you talking about a percentage of profits or a percentage of revenue?

● (1655)

Ms. Chantal Bernier: Actually, if we follow the European model, it is annual revenues. The Chair was speaking about divergent views, but I think there's some congruence here between us. Ms. Gratton said that we have to make sure that we take into account the circumstances of the organization. Gary Dickson spoke of SMEs and how they are more sensitive to fines. Using a percentage, I feel, is fairer because then you don't slap a million dollar fine on a small company. A percentage would fit the gravity of an offence and would be fairer in practice.

Mr. Daniel Blaikie: This question is for our friends at the Public Interest Advocacy Centre. Can you elaborate a bit for the committee on your comments about having either a separate act or having this act target more specifically the privacy rights of children?

How do you think legislation could try to target the kinds of sites, for instance, that children use? What do you have in mind to be able to pick out the kinds of concerns and activities that would be specific to children online?

Mr. John Lawford: I believe our proposal doesn't try to pick out which sites. It's based more on an adjustment to consent. In the United States, as you know, there's a requirement not to take the information of children under the age of 13. That should be standard here in Canada. It's not in the act. Europe now, with the general data protection, is going to require parental consent up to age 16 for most matters.

There is a body of social sciences research on this, on the developing maturation of the teen brain and at what point they can understand to give valid consent. It's similar to medical consent. There could be just basically those sorts of rough rules so that, as a teenager under 16, you would be protected from handing out your personal information to, for example, third-party processing. We did a paper on this, called “All in the Data Family”, which is on our website. It goes through a proposal that we made.

The last thing is, for children who may have given consent under the age of majority, our proposal was also that they have a choice, when they reach the age of 18 or 19, depending on the province, about whether to authorize the company that collected it to continue to use the information. We call it a “get out of data jail free” card. That might be something for the committee to consider.

Those were the kinds of proposals we were thinking about.

Mr. Daniel Blaikie: Thank you very much.

The Chair: You have one minute.

Mr. Daniel Blaikie: Oh, just one? Well, I'm all right, then.

The Chair: Thank you very much, Mr. Blaikie. I appreciate it.

We'll now move to the end of the seven-minute round, with Mr. Saini for up to seven minutes, please.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you very much to all of you for coming here today. You've given us a lot of information.

Madame Gratton, you wrote something in a submission before about shifting social norms and keeping the technology that's coming out neutral, and making sure that PIPEDA is not amended. You cited the quote:

[*Translation*]

"Ne légiférer qu'en tremblant" in French, loosely translated as legislate tremulously.

[*English*]

That quotation is from by a jurist, Mr. Carbonnier, but he stated that in 2001, so we're 16 years ahead now.

In 2001, I don't think he could have anticipated all of the technological changes that would come forward and how quickly technology would increase. If you don't believe that we should deal with privacy in PIPEDA, is there another mechanism? With technology, we don't know what's going to happen two years from now or even five years from now, just as he could not have imagined 16 years ago what would happen by today.

Dr. Éloïse Gratton: His quote is still relevant today. What he meant was that when you're enacting a law, you're fixing things. You're making things more permanent; therefore, they're less flexible. That's why I think his quote is still relevant today.

PIPEDA is flexible, so if we want to move forward with a consent model, let's not touch it. We can do whatever we want around it. We can use interpretation. We can get policy guidance from the OPC. That's why I thought it was relevant to mention him, and that's why I think it's still relevant today.

Mr. Raj Saini: The other question I have is about something we discussed in our other study and now are discussing in regard to PIPEDA—that is, data retention and data destruction. Since we're at the outset of our study, it's good now to get this information to help guide us in going forward.

I open this to everybody. What do you think should be the norm? Do the Europeans have a better model, or do the Americans have a better model? What can we institute to have people's data retained in a safe way? Also, when that data is not necessary anymore, should there be a timeframe to destroy that data?

● (1700)

Dr. Éloïse Gratton: There should be a timeframe. That said, organizations need, in some cases, to keep the data to address risk. Maybe you're going to get a lawsuit so you need to keep it for a certain period of time. You have to keep that in mind. There's also a patchwork of laws that will apply to different types of data.

As a matter of fact, it can be quite a big job for an organization to put together a detailed retention policy. These can be quite expensive, but I'm all for retention and delays that are reasonable, that take into account the fact that the information is no longer in use. You need to get rid of it. You need to destroy it.

Mr. John Lawford: I would just add that, in a lot of the discussion around the right to be forgotten, which we've termed "the right of erasure", I think there's a lot of scope for consumers to have information removed from marketing databases in the future. The right that the Europeans are focusing on is really that, a lot less about trying to take your information off Google, and a lot more about, "I'm tired of getting ads based on what my preferences were 20 years ago." There's a big scope for adding that to the act, that right to erasure. At the moment, privacy policies are written without it.

Nexopia, the company I was talking about, didn't have a retention policy. Nobody knew how long they were going to keep their personal information. That just leads to conflicts.

Yes, you should have a more specific retention policy; but yes, it should be backed up with the right to remove your data within the borders of constitutionality, freedom of expression, and all the things that people have mentioned.

Mr. Robert Dickson: I might just add that when I was in Saskatchewan, overseeing health trustees and their management of personal health information, it was surprising how often you would find inactive health files in a granary, left behind in an abandoned office. You had providers retiring and so on never having properly disposed records. Often the problem with abandoned health records is these would be records that weren't active treatment and they should have been destroyed. There should have been a record retention schedule. It certainly brought home the importance and the value of not only having an appropriate record retention schedule, but then following that, and destroying those records in a timely way when they're no longer required. It's been a significant issue right across Canada, particularly with health records, as physicians retire not having properly disposed of the records at appropriate times.

Mr. Raj Saini: Anybody else? No? Okay.

Do I have any time?

The Chair: Two minutes.

Mr. Raj Saini: Two minutes?

I also want to touch on something else that was brought up, the online behavioural advertising that you mentioned.

The Office of the Privacy Commissioner has said that it's a legitimate business objective. The other part of it is, though, that it must be based on a consent model that corresponds to the sensitivity of the information. How do we determine what is sensitive and not sensitive? What's the threshold? Is there any advice you can provide on that?

Ms. Chantal Bernier: Perhaps I can give you a bit of a history of how we've evolved at the OPC. The first investigation that dealt with OBA, online behavioural advertising, was of Facebook in 2009, when the OPC said that since you get Facebook for free, you should expect advertising because that's the only way they can live. That was a business model that the interpretation of privacy law had to take into account. As long as Facebook did not disclose personal information to third parties, and only used it for its own use to filter ads and send them on the basis of interest, it was within the law. Then we moved to Google in 2014, and in our decision found that Google had served ads to a gentleman who had trusted Google not to serve him ads, as they said they would not in their privacy policy on the basis of his sensitive information, but did. In his case it was medical information, and they served him ads. They discovered, in fact, it was a third-party adviser who was not following Google's rules. The problem there was that even though it was a free service, it was outside the bounds of the privacy policy, first, and the Privacy Act, second, which requires a company to refrain from tracking on the basis of sensitive information.

To go to your point of what's sensitive and what's not sensitive, really—and this goes to Maître Gratton's point—it's very much decided on the basis of harm. Think, what is the harm if this information were revealed? If the harm would be high, with financial information, you can be defrauded. If it's medical information, it's a grave intrusion. That's sensitive. That's what we usually use: what's the harm in disclosure? Then, again, the last decision on that was the Bell investigation, which you've referred to, in which the OPC said that Bell does not have a free service. Contrary to the decision on Facebook in 2009, it's not free. Users have already paid for the service; therefore, if the company, on top of that, is going to be taking their personal information, that's an additional payment, let's say, and there has to be express consent.

● (1705)

The Chair: Okay. We have to move on. Keep your thoughts.

We'll move now to our five-minute round.

We start with Mr. Jeneroux, please.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Perfect.

Thank you, Mr. Chair, and thank you everybody for being here today.

Ms. Bernier, welcome back—maybe not in this room, but welcome back to Parliament.

Mr. Dixon made some comments about this “right to be forgotten” piece notwithstanding the charter challenge. We'd love to get your perspective on that.

Ms. Chantal Bernier: As you've seen, I've framed it very tightly because the charter challenge could be about the curtailment of freedom of expression in an excessive manner, which would therefore violate the charter. I believe the right to erasure—and I understand PIAC to be of the same view—can be framed in such a manner that it would protect privacy without infringing upon freedom of expression, as, in fact, in my view, the Protecting Canadians from Online Crime Act does as well. In the latter act, we criminalize an expression, if you can say so—for example, putting someone's intimate images without consent on the web. So far, it has not been challenged or not been declared unconstitutional, because the privacy violation is so egregious as not to warrant freedom of expression at large.

Mr. Matt Jeneroux: Do you know of other provinces? You mentioned that there's a tie-in to the provincial level, that it's not so easy and that we can just do it at the federal level. Is this on the provinces' radar? Do you have any sense of that?

Ms. Chantal Bernier: Nova Scotia preceded the federal government in regard to Rehtaeh Parsons's suicide, and we followed. The Nova Scotia legislation goes further and did indeed run into a constitutional challenge.

The other legislation I mentioned is that in the four common law provinces, it is an actionable tort to violate privacy. Then in Quebec, as Madame Gratton has described so well, that is perhaps the most cogent and robust measure.

However, to go back to Mr. Massé's point on whether we could use that for PIPEDA, I would remind you that all of that provincial legislation applies to individuals, whereas PIPEDA applies to organizations. This is why I say that if you want to use PIPEDA, you need to go through organizations. How can organizations help to reduce harm to reputations online? It would be through an obligation to erase when the dissemination of information has been declared to be illegal on the basis of these other pieces of legislation.

Mr. Matt Jeneroux: I apologize to the other members, as I think we could spend a whole day here with Ms. Bernier, Mr. Chair.

The Chair: We'll invite her back.

Mr. Matt Jeneroux: We should invite her back. Walk me through what and how it happens now if somebody requests that their information be removed. They have that right through agreements.

Ms. Chantal Bernier: That's only in Europe. A person applies, say, to Google because Google was the one platform that was protecting it anyway. The European court went quite far out on a limb. You could see that they wanted to have the right to be forgotten recognized. Some could say that they stretched the law a little for that.

So a person goes to Google and says that they want to have their information de-indexed and made non-searchable. There are some criteria that have to be met. It has to be genuine. There has to be some value to it and if the person passes the test, it is therefore made non-searchable.

● (1710)

Mr. Matt Jeneroux: That's good.

The Chair: Thank you very much.

Mr. Bratina, please, you have five minutes.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): Thank you.

Thanks to everyone.

I assume that the Public Interest Advocacy Centre interfaces with the public more often with regard to issues like this. Does this come up or has it come up much in your daily work?

Mr. John Lawford: Our experience with data retention and the right to erasure largely arose as a result of our complaint against a children's website and the company's absolute refusal to remove personal information. We did get contacted by former members of that social network, once we brought the complaint. We had a number of them call us and say that they had this problem with the site, and yes, that it was a difficulty.

Occasionally, a person will email us and say that they don't like the privacy policy of company X or Y and can that company really do this or that. So, yes, we do have some contact with people, but on this particular issue it was more after we raised it that people said they didn't know how to get their information erased, and could they?

The answer, unfortunately, at the moment is no, they can't. Although the Privacy Commissioner did say in that case at the end that they would like the site to remove the information. That was the first time I ever saw it. Nexopia waffled on that. They subsequently sold themselves to other owners, who promised to remove it. I'm not sure if it's been done.

Mr. Bob Bratina: Then we get into the issue of would or should, as I think Ms. Lau mentioned: there should, instead of shall, and would and so on....

Mr. John Lawford: Correct.

Mr. Bob Bratina: Does this relate to an order-making model for the Privacy Commissioner? Would you lean toward that?

Mr. John Lawford: Yes, absolutely. If there were a requirement to either produce a retention policy or to erase information, and a company refused after that time to make the policy or to erase the information, then we're looking at.... If people are concerned about jumping straight to large fines, you've seen the anti-spam legislation and the do-not-call list. The authorities in those cases have a spectrum of enforcement. They don't have to start with a million dollar fine, but can start with warnings and notices and guidelines, and work up from there to fines and various larger fines. We think it could work.

Mr. Bob Bratina: What we heard in part throughout today's discussion is the issue of how do you write legislation that anticipates the evolution of technology? That's a tough one, but because of the notion of a retention schedule, could you write legislation that would force companies to request your approval for an extension of their holding your information they had been given in one way or another? In other words, you would hear back within five years from all of the places that somehow had your information, to the effect that they would have to sunset it unless they got your approval. Does that sound like something the legislation could include?

Mr. John Lawford: I think you could include that. I imagine the Privacy Commissioner might give you an interesting point of view on this, perhaps on Thursday. It may involve a lot of auditing and checking up on the matter, but to at least have this would give some certainty.

It's rather like saying that there shall be a five-year retention policy by default; it's similar. It's possible, then. You might ask the Privacy Commissioner when he is here.

Mr. Bob Bratina: I have to refer back to the problem of writing legislation; it's so hard. I can see that we have an interesting bit of a conflict in what has been presented.

Mr. Dickson, you said that if you can't tell media to take stuff down.... What is your feeling about our ability to take command of the issue?

Mr. Robert Dickson: I think it's difficult, for all of the reasons that have been discussed already. You see the Privacy Commissioner of Canada attempting to address the mischief, recognizing a problem and attempting to deal with it. We've seen the Federal Court attempting to address this through the one case. I'm afraid it doesn't admit of an easy remedy—or a foolproof solution, if you will.

● (1715)

Mr. Bob Bratina: Why did you give up on or not complete the report in Saskatchewan?

Mr. Robert Dickson: All I know is that the Privacy Commissioner of Canada had hired an organization to do the work. I had liaised with the assistant commissioner Denham in developing it, we rolled it out in Saskatchewan, there were a number of meetings with business organizations and small and medium-sized businesses, and we certainly received intelligence and input and feedback through that process. Then there was some issue, I think, between the consulting firm and the office that had hired them, and at some point I think the contract was terminated. I wasn't directly involved in that.

It was unfortunate, because it was an interesting exercise and helped to probe in a part of the country in which there isn't a provincial private sector privacy law and PIPEDA was the law that applied. It's important that it have traction in all parts of Canada, and we found lots of evidence—it was manifest—that there wasn't a great deal of traction in that one province, and I suspect not only in that one province.

Mr. Bob Bratina: Thank you very much.

The Chair: Thank you, Mr. Bratina.

I'll be doing the next five minutes on behalf of my political organization. I'm going to ask all my questions up front. I have a question basically for each of you.

First of all, PIAC, you mentioned Mr. Owen Charters, president of the Boys and Girls Club of Canada. In your submission you said that these tracking tools follow our children as they surf the web collecting data about their behaviour and interests and that it's often sold to marketing companies.

Do you have a source for that? I'd like to know where that information is.

Mr. John Lawford: That's a quote from him. I'd be happy to provide the *Wall Street Journal* article to the clerk.

The Chair: That would be great. I would appreciate it.

Mr. John Lawford: Yes.

The Chair: We might want to invite him here to talk about that kind of information.

Mr. John Lawford: Sure.

The Chair: The next question I have for you—and I'll go directly to you—has to do with paragraph 25 of your submission to the OPC. You mention the implementation of standard privacy preferences and a trustmark system.

I will ask you my question and then I'll move on and you can answer it later. Is there a voluntary or industry-led preference or trustmark system right now?

Mr. Dickson, my question for you deals with medical health records.

Is it not in the public interest to retain public health records for a very long time even in the case of individuals, simply because I don't know whether some day down the road any of my genetic information might be useful to my children, my grandchildren, and my great-grandchildren, and so on? For health research and all those other kinds of things, it might be a good idea to keep those electronic health records in perpetuity, balancing the weight of the public good.

My question for you, Ms. Gratton, deals with the European Union.

I believe it's a policy of the European Union not to have any of their own directives or initiatives within the European Union influence the domestic policy of other countries they are dealing with; for example, in regard to non-tariff barriers. I'm wondering whether the European Union's privacy legislation is going to do exactly that: influence our ability to trade with them, simply because their own internal directive is forcing a conflict between foreign and domestic policy for Canada.

My question for you, Madame Bernier, is this. You talked about the offence being commensurate with the revenues of the organization. A not-for-profit organization might have lots of data but doesn't have a lot of revenue; a voluntary organization might have a lot of data but doesn't have any revenues; you may have a small company that has a lot of data that might do a massive amount of harm but which has small revenues; and you might have a large corporation with large revenues that does a small amount of harm, and they might be paying more for an offence than a small organization would that does a lot more harm.

Could you square that circle for me?

I'll leave it up to you guys to go with your questions.

Mr. John Lawford: I guess we'll go from our left to our right. There are some private trustmark systems. Some have come up and gone down over the years. I know there is AdChoices, an American example, which is also followed by the Association of Canadian Advertisers. I believe Alysia mentioned Ann Cavoukian leads one for Privacy by Design.

Ms. Alysia Lau: Yes, there is one. It's a partnership between Ryerson University and Deloitte.

Mr. John Lawford: Overall, we think that if there is a trustmark system, it would be good to have. Let's call it a blessing by the Privacy Commissioner, who has looked at this voluntary one and believes it's a good approach that would be helpful because it would increase consumer trust.

● (1720)

The Chair: Thank you very much.

Go ahead, Mr. Dickson.

Mr. Robert Dickson: Generally speaking, when it comes to record retention, privacy laws provide that it's not appropriate to retain information because somewhere down the road you may come up with another purpose for the information. You collect information for a specified purpose. This is fundamental to all privacy law.

When the original purpose for retaining the information has been met, you destroy it.

In practical terms, that means that in virtually every province with a stand-alone health information law, there's a requirement that custodians or trustees must set a record retention schedule. It's usually influenced by legal advice about how long there's a potential legal liability and then the records are to be destroyed.

There's also a provision in every one of those stand-alone health information laws that provides that application can be made to a research ethics board or a research ethics committee for access to information for specific projects.

As the law currently stands, it is not appropriate and not lawful to retain information, because somewhere down the road my personal health information may be useful to my grandchildren or their children.

Part of what's happening is that, as genetic science increases, that information about my health or your health today becomes more valuable. That's going to be a challenge for you and legislators going forward. Currently, there's not the kind of provision that you might like to see.

The Chair: Fair enough.

Your turn, Ms. Gratton.

Dr. Éloïse Gratton: Yes, I believe that the EU, clearly, is imposing its privacy standards. I do have some concerns with that.

Moreover, I think we have to consider the fact that every four years, it's going to be re-evaluated, not only in light of PIPEDA but also in light of our national security legislation. That's something to think about.

Last month, there was an article published by Gabe Maldofff and Omer Tene, U.S. academics, who noted that, in light of the recent European decision in Schrems, it's not clear that Canada still passes that test.

So I think we should be focusing on our issues and not bending that much.

The Chair: Madame Bernier, if we could have your response quickly, please.

Ms. Chantal Bernier: First of all, just to clarify, on fines PIPEDA only applies in the context of commercial activities, so there is always a revenue attached to the personal information.

Secondly, using a percentage, in my view, would be precisely the proportionate and, therefore, fair manner to impose equivalent penalties to all organizations.

Regarding harm, harm is not indicative of fault. You can have a hugely harmful hack; for example, let's take Carbanak. Carbanak hit 100 financial institutions for billions of dollars and the Kaspersky auditors went through it and found the most unbelievably sophisticated hack behind it and stated that they could not find any flaw in the security systems of the 100 banks that were hacked. It was just really bad luck. Therefore, we should not correlate harm and guilt.

Finally, I believe that the best place to assess and award damages is the courts.

The Chair: Thank you very much.

Mr. Erskine-Smith, you have five minutes, please.

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

My first question is with respect to something we haven't discussed much yet, namely the civil remedies under PIPEDA. How effective do you think they are and do you believe there's a model jurisdiction we might look to that has a better structure?

Ms. Chantal Bernier: There are no civil remedies right now.

Mr. Nathaniel Erskine-Smith: Sections 14 and 16 together.

Ms. Chantal Bernier: Well, you go to the OPC, and then you can go to court.

Mr. Nathaniel Erskine-Smith: That's the civil remedy and—

Ms. Chantal Bernier: Yes.

Mr. Nathaniel Erskine-Smith: —it seems to me potentially insufficient. Is there a model jurisdiction we might look to in order to improve upon our current regime?

● (1725)

Ms. Chantal Bernier: As I mentioned in my opening remarks, there's quite an array. You have the U.K., where the fines go up to 250,000 pounds. You have France, where it goes to 300,000 euros.

Mr. Nathaniel Erskine-Smith: I don't mean to cut you off, but that's if the Privacy Commissioner is engaging in establishing penalties....

Say there's a consumer group that has been wronged in some way. We wouldn't necessarily have to wait under.... Well, we have to wait for a report from the commissioner, I understand, under section 14, but upon receiving that report, we can take the issue to court.

I understand that the OPC probably should have fining powers, but in addition should we expand upon the civil remedies?

Ms. Chantal Bernier: The civil remedies are there. In fact, Maître Gratton, Richard Dickson, Gary Dickson and I were just talking about how class actions are proliferating. That is there, that is used, and that is big money at stake. We've seen Casino Rama. There's been a big settlement. We've seen some that are in the works right now with big numbers attached to them. So that does occur.

Mr. John Lawford: You might want to consider what they're doing with the anti-spam legislation, which is giving a private right of action, with a set amount per violation up to $200. It's the same sort of thing. That enables class actions, because it's hard to show harm. There are a number of class actions testing the waters now in Canada to see if you can get damages where there's no real harm. If you put something in the act, you could look at the anti-spam legislation as a model, and that would attract private enforcement of the regime. If the other enforcement done administratively isn't adequate, then the private bar could take cases.

Mr. Nathaniel Erskine-Smith: I think that's also the case in a copyright.

Mr. Dickson or Ms. Gratton, do you have anything to add?

Mr. Robert Dickson: I have nothing to add to Chantal's comments.

Dr. Éloïse Gratton: No, I have nothing to add.

Mr. Nathaniel Erskine-Smith: With respect to the right to be forgotten, there are different ways it can come into play. If I, for example, could publish an article about someone and post it online, and perhaps they would say there's a right to be forgotten—and freedom of speech, as you suggested, Ms. Bernier, would be the competing value.

With respect to indexes, though, it strikes me that it's not just about freedom of speech. There's also a public interest in accessing information in archival records. Certainly, individuals may want information about themselves to be forgotten, but the public may not want it to be forgotten.

You mentioned the EU, Ms. Bernier. Have they struck a fair balance with that idea of a public interest in indexes in particular?

Ms. Chantal Bernier: In fact, earlier on, Gary Dickson mentioned the work we did together on guidelines that are applicable to the Internet posting of administrative tribunals, which goes exactly to your point. We wanted the privacy of the parties to be protected, but we also wanted judicial transparency to survive for the reason you say, because there is a public interest in getting the information. One solution is simply to use initials rather than the full names and identifiers. Therefore, you have the tribunal being in full glare, but the privacy of the parties, whom you don't need to know, being protected.

In Europe, the right to be forgotten is quite narrow compared to a discrete right to say that I want it taken down. It still has to be based on irrelevance, inaccuracy. I mean, there are criteria.

Going back to the congruence between us, I certainly have heard that it needs to have parameters so that it encroaches neither on the right to know—the freedom of access to information—nor freedom of expression. There is definitely a way to find that right spot.

The Chair: Okay, thank you very much.

We have our last three-minute round for Mr. Cullen, and then I'll excuse the committee. We'll have to quit because we're past our time.

In advance of that, I would just like to thank all of our witnesses. I know that some people have some tight deadlines.

Mr. Cullen, for three minutes, please.

Mr. Nathan Cullen (Skeena—Bulkley Valley, NDP): I'll be right to the spot and the chair will help me out.

Thank you for the testimony. I've been reading over some research. My apologies if anything I ask has already been queried, but a politician, a microphone, and some time is a hard combination to completely resist, and ignorance has never stopped me from speaking before.

I have one question about this right to be forgotten, technologically speaking. We've seen with some technological advancements that you can rent a movie, for example, with a delete option built into it. After a certain amount of time it simply expires. Has this ever been explored with personal information, so that once such information is granted to a private company, there is a built-in algorithm to automatically delete it after a five-year period? Is this a technology that's ever been explored successfully, and is it something that could be built into law? You've talked about the onerous nature of having to audit five years later whether information is actually being destroyed or, as I think you said, ending up in a granary in Saskatchewan. I find that far too typical, somehow. Is there a technological fix to this that's been explored?

● (1730)

Mr. John Lawford: I am not sure if anything has been commercialized, but certainly you could build an algorithm like that. I think there would be no trouble doing that.

Dr. Éloïse Gratton: We should be encouraging the use of technologies that don't retain data forever, and here I can think of ephemeral messaging apps, such as Snapchat. So it's definitely possible.

Mr. Nathan Cullen: I have a second question. Recently we had a petition on electoral reform that went through Parliament. This was an official parliamentary petition. One thing I noticed—and it's one of the first times I've noticed it—was that a lot of people were writing and asking me, will the information on their signing the petition be going to the parties? They ask because that's been the experience. Political parties use petitions for gathering data.

How much work has been done on that side of things, the retention of data both by government and, by extension, political parties—not parties as an extension of government but as another form of civic engagement? Have we seen any evidence of Canadians and certain populations of Canadians choosing to disengage from civic engagement out of fear that their data will be retained? I'm thinking of our neighbours to the south right now. If I were a Muslim American, would I want to be signing some petition that could end up in the hands even of the Government of the United States?

Mr. Robert Dickson: You raise a question that was explored by this very committee in looking at the Privacy Act. One of the presenters was Professor Colin Bennett from the University of Victoria, who is Canada's leading expert on privacy in the context of political parties and elections. I know that the Canadian Bar Association is doing some work on this. I know that the Chief Electoral Officer has made a recommendation—actually, it was maybe two CEOs back—that this is an issue to be looked at. This could be a great discussion, but it would be a lengthy one. I think that recommendations would come forward, if not from this committee, from other organizations, requesting that Parliament, at long last, address the protection of private information by political parties.

The Chair: Friends, we're at the time. Here's what I'm going to do. To our witnesses who are here today, because I know we have to shut the committee down—and I want to thank you, Mr. Cullen, for your questions—if there are any answers that you were not able to get out today, please feel free to jot those thoughts down and submit them to the committee and they will be included as the response to the questions that were asked in the testimony. If there's any other information, things that you wish you would have said or think about afterwards, by all means, please submit that to the committee as well.

We thank you very much for your time. We apologize for the late start. But thank you so much, and if we call upon you again, I know you'll help us out.

With that, the meeting is adjourned.