HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 053 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, March 23, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, March 23, 2017

● (1615)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Good afternoon, colleagues.

I just want to say thank you to our witnesses who are here today. I apologize for not being able to start the committee on time. We had some votes that took a while, but we are here now. We have quorum. In the interest of making sure we get through the statements and questions, we'll proceed as quickly as possible. I know a few members may still be coming in.

We're pleased today to continue our study of the Personal Information Protection and Electronic Documents Act, more affectionately known as PIPEDA.

We're pleased to have Madam Jennifer Stoddart here. Welcome, former commissioner. From the Canadian Internet Policy and Public Interest Clinic, we have Mr. Tamir Israel, who has been no stranger to this committee in all of our previous studies. From the Canadian Bar Association, of course, we are pleased to have Suzanne Morin, vice-president, privacy and access law section.

Each of you will have up to 10 minutes to present your opening remarks, and then we'll proceed immediately to our rounds of questions. We'll go in the order in which I introduced you.

Madam Stoddart, the floor is yours.

Ms. Jennifer Stoddart (As an Individual): Thank you very much, Mr. Chair.

● (1620)

[*Translation*]

Good afternoon everyone.

[*English*]

I'm honoured to be invited here. Being a retired person, I don't have a formal presentation, so I hope you will bear with me. There are some handouts, which are notes on which I based my remarks.

I've read the transcripts with great interest. You have a variety of opinions of some very expert people. I'm going to focus, in my short presentation, on areas in which I think I have more experience. I'm going to divide my remarks in a chronological fashion, that is, dealing with what's coming up, what is already extant, and what has already been suggested to you.

I'll start then with the future, the challenges for PIPEDA. You will not be surprised that I'm going to single out the effects of the general data protection regulation of the European Union. I have spent part of my retirement working with some other people on a scholarly article on the administration of the adequacy principle, so it's more recent than some other issues to my mind.

You will have already heard that there's a more rigorous test than the one that PIPEDA went through in the past: effectively equivalent. The problem is that there are no real specifics. The more serious problem is that in the European Union, in the study I made of all the adequacy decisions that had been made and the ones that had not been made for which analyses had been done, there is a very checkered history of evaluation of countries' personal information protection frameworks.

You should also realize that there's a huge amount of pressure within the European Union post-Snowden both from activists and political parties to be rigorous in imposing European standards on the rest of the world.

In looking at what PIPEDA may need for the future, I would say it's best to aim high and to remember that it also applies to the European standards, that is, the public sector use of personal information as well. There is an overlap to my mind in EU law between the right of erasure or correction, which is already in PIPEDA, and the right to be forgotten. Several of the people who have appeared here have said that they don't know whether the right to be forgotten exists in Canadian law.

It actually has existed in Quebec law, and as we are a bi-juridical country, it exists in Canadian law and has for quite a long time. I heard about the right to be forgotten when I was in law school, and I graduated in 1980 so that's a long time ago. There is jurisprudence on the right to be forgotten, and I encourage the committee to take notice of this.

I would encourage you to distinguish, as not all of your witnesses have, between the right to be forgotten, which has been interpreted so far in the European Union as the right to delink information in search engines, and an act of destruction of original information. I don't think anybody I've heard is talking about this, but it seems to be a bogeyman that comes out somewhere as soon as we talk about the right to be forgotten. That's not what is involved at all.

I would urge you too to remember, as all the witnesses in my opinion have not, that PIPEDA is a law that only governs federally regulated business. It does not govern individuals, and it does not govern a host of things that are in provincial jurisdiction.

Coming back to the right to be forgotten, interestingly in the recital—that's what they call it; we call it a preamble—to the general data protection regulation they talk about the reasons for it, including the right to take down postings that you may have made on the Internet in your youth and which you now regret. I would urge you to think about that as a reason for motivating some extended possibility of having things taken down and to think about it in the context of the human right to dignity, the right that, I think, we all have to be a person who evolves. What you do at 16 is not what you're going to do at 36 as you're contemplating running for office or something else. I think that's just taking into account human nature and a necessary respect for human dignity.

The committee has heard other ideas, such as special rules for children. Again I would encourage you to think about the division of powers, which is a reality in our Canadian constitution.

One thing you might look into is the possibility of putting within PIPEDA some kind of special mention for the Office of the Privacy Commissioner or for the commissioner to harmonize, to discuss with provincial counterparts, and to support the development of strong, compatible laws throughout Canada, given that so much personal information protection comes under provincial jurisdiction. This is because criminalizing behaviour, in my opinion, is not always the best way. That's the federal jurisdiction for personal behaviour. It's not the best way to deal with a lot of things.

I'll move on secondly, Mr. Chair, to what is trending now, and I'll refer to what are the current values of Canadians.

I think transparency is now a hallmark of democracies, post-Snowden. We've seen recent examples of demands for more transparency from public figures, and so on.

I would contrast this with the very opaque system of some 20 years ago, when it was originally devised, by which PIPEDA is administered. No real thought was put into it at the time, because there wasn't a huge public preoccupation with what the public can see or what the public can understand about the application of personal information protection. It was a convenient ombudsman model. It had been adopted by the Canadian government in the late 1970s from Scandinavia, where at the time the countries were almost totally homogeneous, ethnically and socially, and where there was and still is a huge public trust in government.

I think also that the public should know more about complaints against commercial organizations. One reason is that many things don't seem to have improved over the years with the present system. I'll refer you to the recent posting of the Office of the Privacy Commissioner on March 15 about a complaint into the use of personal information by a Canadian bank. I think there would be more impact among the public if both this particular bank and the retailer involved in this incident were named.

Again on the same theme of transparency, I'll remind you of the need for business organizations themselves to be transparent in their use of personal information that they hand over to government agencies, the police, CSIS, etc.—hopefully always legally.

Secondly under the theme of transparency, I'll talk about individual empowerment. The Office of the Privacy Commissioner has an important budget, but it is not a budget that is commensurate with the challenge of protecting personal information in this century. I believe that investigating individual complaints is a time-consuming and not very productive way of trying to enforce privacy rights for Canadians. I think the system should be modified. The commissioner should be able to do as the U.S. Federal Trade Commission does: look at the complaints that are made as a bellwether of public opinion, pick and choose the complaints he or she wants to investigate, and then give individuals commensurately the right to take their own case forward to the Federal Court.

Finally under the theme of transparency, I think we have to allow the Office of the Privacy Commissioner to concentrate on areas in which there are new and serious threats in the changing context of new technology and new behaviour, and therefore, not investigate every complaint. We, therefore, also have to give the commissioner broad audit or self-initiated investigation powers. These are necessary, I think, to strengthen the accountability principle, which is coming forward as consent becomes, for such technological reasons as big data, ever more difficult. The need to stand ready to demonstrate that you are accountable becomes a key part of a modern enforcement scheme.

I'd also mention ethics, but I think ethics need to be placed within a more rigorous framework.

● (1625)

[*Translation*]

Finally, as for the previously determined missing elements, suggestions were made long ago regarding the review of PIPEDA. As you will recall, there was a report in 2013 outlining four points, and I made a recommendation a few years ago that political parties themselves be subject to PIPEDA.

In the wake of two decisions made by the Supreme Court of Canada, one of which was handed down barely a few months ago, I believe that a review of the act should include giving the commissioner clearer powers to conduct investigations, notwithstanding the protection conveyed by jurisprudence and the legislation regarding privileges. Counsel-client privilege has evolved enormously since the 19th century in our society. I believe that privilege no longer has any reason to exist with regard to complaints or allegations of inappropriate use of personal information, and should not prevent a commissioner from conducting an investigation in that regard. The act must thus contain clearer and stronger language.

[*English*]

I would conclude by pointing your attention to some recent work, which I think is the most contemporary work on smart regulation. It's out of the University of Oxford, by Professor Christopher Hodges. It talks about what successful regulation is.

Successful regulation is really about influencing behaviour, and influencing behaviour in a variety of ways, depending on the context, depending on the issue, and depending on what we used to call the "industry" but may be the "sector" or the "activity". It could be information to consumers. It could be constant dialogue with the regulated entities. It could be creating peer pressure through action within that sector or that activity.

It's about making responses seem targeted, fair, and proportionate to what the problem is, not automatic or because the law says so: "We're going to investigate you, because I have to investigate every complaint; therefore, you're going to have to pay for a lawyer to see this through." That's not necessarily, I think, fair or proportionate. It's about rewarding those who can demonstrate compliance and about sanctioning inappropriate behaviour.

I would encourage you in moving forward to give the Office of the Privacy Commissioner more flexibility to take on a wider range of regulatory approaches, given the changing needs over time.

Thank you very much for your attention.

● (1630)

The Chair: Thank you, Madam Stoddart.

We now move to Mr. Israel, for 10 minutes, please.

Mr. Tamir Israel (Staff Lawyer, Canadian Internet Policy and Public Interest Clinic): Thank you, Mr. Chair.

Thank you for having me here again. My name is Tamir Israel, and I am a staff lawyer with CIPPIC, the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic at the University of Ottawa's centre for law, technology, and society, which is at the faculty of law. CIPPIC is a legal clinic that works to advance the public interest in policy debates that arise at the intersection of law and technology.

I want to thank you for inviting us once again to contribute to the important work the committee undertakes, in this instance in relation to its review of PIPEDA.

We note at the outset that in our view the principled framework adopted by PIPEDA has largely withstood the test of time. Its general adaptability has allowed it to keep pace with often rapid and tectonic social and technological changes. That being said, some targeted clarifications and additions to PIPEDA's consent and transparency mechanisms are desirable, while PIPEDA's lack of effective enforceability continues to hinder the full realization of the important rights it grants Canadians.

As this committee has heard, the modern era has strained one of PIPEDA's core pillars: consent. This strain arises from the increasingly complex nature of modern data practices, which in turn leads to opaque data capabilities, powerful incentives that are often directly at odds with those of consumers, and inaccessible privacy policies that seek either to capture this complexity, or at the other extreme, to obscure it in order to maintain flexibility for future organizational practices.

In light of this complexity, it is neither practical nor desirable to expect every individual to gain the necessary expertise needed to assess the data practices of every data service encountered on a daily basis. It would be equally undesirable, however, to jettison the concept of consent in favour of a risk-based accountability framework. Such a framework would effectively amount to open season on individual data. Moreover, it is likely to undermine the adoption and usage of services, as empirical research suggests that individuals' confidence in and adoption of services are greatly tied to the ability to exercise consent over data practices.

Too often, however, this confidence is misplaced. Frequently, individuals' expectations are simply not reflected in the unintuitive privacy policies and data practices to which they implicitly consent on a regular basis. In this regard, formalizing some elements of PIPEDA's existing principled framework could assist in realigning practices with expectations.

PIPEDA generally recognizes that more explicit forms of consent are required where such a disconnect occurs, and especially where sensitive data is involved. However, recognizing an explicit "privacy by default" approach will further underscore the need to obtain user input in relation to privacy practices, helping to narrow the gap between individual expectations and actual practice.

Formally empowering the Privacy Commissioner to impose context-specific restrictions may encourage greater use of PIPEDA's current power to designate certain practices as generally unacceptable, and create context-specific regulatory policies. Greater recourse to such tools would enhance certainty and consistency on the business side, while allowing for more frequent proactive policies from the Privacy Commissioner. A formal procedural mechanism for their development would in turn strengthen the quality and legitimacy of such policies.

Finally, some measures might be considered to address specific data protection challenges raised by data brokers. Such entities amass detailed profiles on individuals from disparate online and offline sources, typically without the knowledge or input of the affected individual, who is usually far removed from the collection process. Information held by data brokers is increasingly used by a range of secondary entities to make decisions that often have serious impacts on individuals. A 2014 report issued by the Federal Trade Commission recommended that data brokers be obligated to create readily accessible portals that would allow individuals to easily determine whether their data is being held by a particular broker and that data's initial source. This would then act as an avenue for the exercise of other rights, such as the rights of correction or erasure, that are already integral components of PIPEDA's existing data quality mechanisms.

This framework could be imposed by the Privacy Commissioner as a sector-specific regulatory policy under subsection 5(3) of PIPEDA, but legislating it may provide a stronger and clearer mechanism.

● (1635)

With respect to enforcement, PIPEDA's recommendation and *de novo* enforcement model is significantly out of touch with the realities of modern data protection. The individual stakes and counter-incentives under which many organizations operate require a serious and responsive regulatory regime. PIPEDA's enforcement mechanism is procedurally difficult, unnecessarily time-consuming, and lacking in deference to the expertise of the Privacy Commissioner.

Personal data is the commodity of the information age and requires a regulatory framework of commensurate formality. It is unsurprising that most jurisdictions with data protection regimes have included enforceability measures in recognition of this basic truth. Imbuing the Privacy Commissioner with order-making powers will assist the office in its interactions with large multinational organizations, enabling it to better carry out its mandate with the authority of a regulatory body.

Further, the prospect of incurring damages under PIPEDA violations remains currently distant, and the anticipated quanta of such damage is minimal. We have seen recent developments in tort law that have supplemented this gap to a certain degree and have led to a notable improvement in proactive compliance, with privacy implications being subject to class actions.

Class actions in tort are, however, limited in scope to certain types of privacy invasion, and there remains little incentive for robust and proactive compliance with other critical elements of PIPEDA. We would therefore encourage imbuing the Office of the Privacy Commissioner with the power to issue administrative monetary penalties comparable in character to those recently allotted to the Canadian Radio-television and Telecommunications Commission.

We would further recommend examining the development of an independent private right of action, which would allow for individuals and classes of litigants to advance their privacy claims directly. This could be supplemented with statutory damages covering some or all of PIPEDA. It could apply to specific principles and violations or to all of the act, and that would facilitate an analogous regime of private enforcement, further incentivizing compliance.

Finally, some transparency mechanisms would address specific and pressing problems under PIPEDA's current regime. It has become accepted practice in many industries, and particularly those industries engaging in facilitating electronic communications, to periodically report on the scope and nature of state agency requests for customer data. While such reporting is arguably required under PIPEDA's openness principle, we would recommend adopting a legislative mechanism that would explicitly empower the Privacy Commissioner to designate transparency reporting obligations on a sector-by-sector basis and also to impose detailed obligations as to the substance of the obligations. This would lead to more consistent and standardized transparency reporting in lieu of the current incomplete and ad hoc reporting.

A secondary transparency mechanism that would benefit from legislative adoption relates to algorithmic decision-making. Automated processes are responsible for a growing range of determinations that significantly affect individuals' lives. Academic and legal literature has demonstrated that algorithmic decision-making often operates as a proxy for decision-making that is discriminatory on religious, ethnic, racial, disability, gender-based, and other protected grounds. Algorithmic decision-making can also gloss over important individual distinctions in favour of broad generalizations, leading to incorrect outcomes for affected individuals. More generally, algorithmic decision-making often obscures the reasoning that animates a given output, making it impossible to determine precisely why a teacher was fired, a consumer was denied particular advantages, or an individual's credit request was rejected. It then becomes difficult to assess whether a decision is accurate, fair, or discriminatory.

Transparency in algorithmic decision-making intersects directly with core and long-standing data protection principles designed to ensure the quality of data used for decision-making. In PIPEDA this is encoded through the data accuracy principle and the right of individual access to personal information held by an organization. However, commercial secrecy is increasingly used as a means of obscuring the underlying logic of an algorithmically determined outcome. In addition, and in the absence of strong transparency obligations, more sophisticated algorithms are now evolving that wholly obscure underlying considerations even from the companies relying on them.

● (1640)

CIPPIC would therefore recommend the addition of a distinct right of access to the underlying logic of any automated decision-making process, and in particular in relation to automated decision-making with a substantial impact on individuals' lives, their access to economic opportunities, and their treatment on the basis of protected grounds.

The committee may further wish to consider the need to undertake a broader study of automated decision-making in both private and public sectors.

Those are my comments for today. I welcome any questions.

The Chair: Thank you, Mr. Israel.

Last but not least, we have Madame Morin from the Canadian Bar Association.

The floors is yours. You have 10 minutes.

Ms. Suzanne Morin (Vice-President, Privacy and Access Law Section, Canadian Bar Association): Thank you. I've been using this timer to keep us honest, because last time both Tamir and I went way over.

We spent the 30 minutes or so that we were waiting having quite a good debate here beforehand.

Thank you very much, and good afternoon, Mr. Chair, and honourable members of the committee. We appreciate your invitation and are very pleased to be here today on behalf of the national privacy and access law section and the Canadian Corporate Counsel Association, both sections of the Canadian Bar Association, to present our views on the Personal Information Protection and Electronic Documents Act, which as you all know is called PIPEDA.

The CBA is a national association of more than 36,000 lawyers, law students, notaries, and academics. An important aspect of the CBA's mandate is seeking improvement in the law and the administration of justice. It is that capacity and perspective that brings us before you here today.

Our members of both sections are lawyers with in-depth knowledge in the areas of privacy and access to information law from every part of the country. They are lawyers in private practice, they are in-house counsel working for public and private companies, crown corporations, government and regulatory bodies, municipalities, hospitals. You name it, we have it covered.

My name is Suzanne Morin. I'm vice-chair of the national privacy and access law section, and I work for Sun Life.

The sections have made numerous submissions on PIPEDA since its enactment in 2001. We continue to support the existing consent and ombudsperson models in PIPEDA in the absence of the compelling need for legislative change, while carefully continuing to monitor Canada's European Union or EU adequacy status, as mentioned by Madam Stoddart.

Within these existing models, we suggest that targeted amendments are needed: one, to the concept of "publicly available information" to ensure that our PIPEDA framework remains technology-neutral; and two, to allow the Office of the Privacy Commissioner to issue non-binding advance opinions.

I will briefly address each of these issues.

Regarding consent, the CBA sections recommend maintaining the consent model in PIPEDA in the absence, we would argue, of a compelling need for legislative change, and the continuing use of a multi-faceted tool kit approach to privacy protection in Canada. Canadian privacy rights, obligations on business, and remedies available to individuals exist in an extensive legal framework in this country that encompasses federal and provincial, private and public sector privacy laws, criminal and human rights legislation, emerging common-law and civil actions, and civil liability regimes in Quebec.

PIPEDA speaks directly to the principle of consent, laying the foundation that businesses must seek meaningful and valid consent and cannot force individuals to consent to the use of personal information beyond legitimately identified purposes. PIPEDA's consent model comes with 10 fair information principles. As an umbrella, all treatment of personal information is subject to the "reasonable person" test, which limits the use of personal information to what is reasonable in the circumstances. This goes to the context that we heard just moments ago.

The PIPEDA consent model, supported by the broader legal framework, in our view continues to be both robust in its protection of the privacy of Canadians, including vulnerable groups, and flexible for business in the face of rapidly evolving technologies, business models, and evolving customer privacy expectations.

Regarding the ombudsperson model, the CBA sections recommend maintaining this model unless, once again, there is evidence that a change to the OPC's enforcement powers is actually needed. The OPC enforces privacy rights by leveraging the powers that exist in PIPEDA today: one, to investigate and issue formal findings, including the naming of names when doing so is in the public interest; two, to audit the practices of organizations when they have reason to believe that an organization is not complying with its obligations under PIPEDA; and three, to take organizations that fail to uphold their privacy obligations to court.

In turn, our Canadian courts have proven to be well placed to assess damages uncovered by OPC investigations, and they have recognized new civil actions or common law torts, adding to the Canadian privacy legal framework. Taken together, this tool kit approach has proven to be powerful, actually, in forcing domestic and foreign organizations of all sizes to revise their privacy practices through the great efforts of former commissioners such as Madam Stoddart.

● (1645)

It would be prudent to wait to see how the OPC's new power to issue and enforce binding compliance agreements through the courts is interpreted and used, and how the new breach reporting regime—which is still not yet in force—with the potential for fines unfolds over the next year.

Third, concerning non-binding advance opinions the CBA sections recommend amending PIPEDA to clearly authorize the OPC to issue non-binding advance opinions to organizations proposing new programs, technologies, methodologies, or specific transactions. While the OPC currently offers general guidance, such as investigation summaries and interpretation bulletins, it chooses not to provide organization-specific guidance in the absence of an investigation or an audit.

Providing express authority would make it clear that the OPC is expected to perform this function, providing clear guidance for and confidence in the privacy compliance of some new initiative and, through the publication of anonymized opinions, adding to the body of guidance available to organizations.

Fourth, concerning publicly available information the CBA sections recommend amending PIPEDA or its regulations to ensure that they are technology-neutral and able to accommodate both existing and evolving business models and customer expectations when it comes to the use of personal information that customers choose to make publicly available.

PIPEDA was indeed carefully drafted to be technology-neutral, and after more than 15 years I too agree that it continues to stand the test of time, allowing organizations to evolve their practices to reflect all of these changes. While PIPEDA is consent-based, it also offers specific exemptions to consent when obtaining consent is either not practical or not necessary, including exemptions for publicly available information.

However, unlike PIPEDA, the regulations that accompany PIPEDA miss the mark in certain respects and have created uncertainty about what level of consent is required to use personal information that individuals have chosen to make public. In our submission we've identified several options for you to consider.

Fifth, concerning EU adequacy the CBA sections recommend carefully monitoring Canada's EU adequacy status. We caution, however, that amending PIPEDA to anticipate changes that may be required to maintain the status would be premature. Canada has enjoyed adequacy status under the EU's 1995 data protection directive since 2001. This status has enabled the convenient transfer of personal information from the EU to organizations in Canada.

Recent developments in the EU are indeed raising questions about whether Canada's adequacy status is at risk. It's unclear what the EU's new approach will be; we just don't know. However, when the time comes, they will examine, as Madam Stoddart identified, the entire Canadian legal framework, including public and private sector legislation, and including laws concerning public security, defence, and national security; our criminal law; and Canada's other international obligations or commitments.

PIPEDA is only one part of Canada's privacy legal framework and may not be the only or even the appropriate vehicle for addressing adequacy concerns that may arise. Adequacy is great, but not at all costs, and we caution on making amendments at this early stage.

Finally, we leave a word about the right to be forgotten. We have not made any recommendations on whether a specific right to be forgotten should be included in PIPEDA or introduced into our broader legal framework, but it is an issue that merits attention. The right to be forgotten as it has evolved in the EU is not addressed directly in PIPEDA; however, PIPEDA includes the right for an individual to withdraw consent or to delete certain information and the obligation upon organizations to use published personal information for consistent purposes and to delete information that they no longer require.

We need to be mindful that PIPEDA and other private sector laws are not the catch-all for issues that arise from the ongoing evolution of technology, and that beyond PIPEDA there are numerous other considerations, such as the right to freedom of expression, which is a critical piece of the democratic fabric found in the charter.

The CBA sections, once again, appreciate the opportunity to share our views with you on PIPEDA.

● (1650)

[*Translation*]

It will be my pleasure to answer your questions.

Thank you.

[*English*]

The Chair: Thank you, Madame Morin.

We have about 40 minutes left in the meeting, colleagues, and I think we should allocate all of this time for questions. We'll get through the seven-minute round and about halfway through the second round, if that's suitable for colleagues.

We will start with Mr. Saini, for up to seven minutes, please.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon. I'm sorry about being late today. This is a very important and I think necessary discussion.

I want to start with the bogeyman, as Madam Stoddart called it. We've heard very differing opinions on the right to be forgotten. We have even heard questions about whether such a right would withstand a charter challenge. The CBA submission has said it is not addressed directly in PIPEDA, but that PIPEDA allows an individual to withdraw consent. You say that there is already within its provisions the right to be forgotten.

With all these differing opinions, I'd like to hear from each of you exactly what you think about the policy of the right to be forgotten. The reason I say this is that with the GDPR, the reason the right to be forgotten came in is that it was codified by a judgment. I'm sure you're aware of the Google Spain case.

Was that an overreaction on their part, or what should we be doing here in Canada? Should we have a right to be forgotten or not have it? If the GDPR has it already and the GDPR is going to be coming into effect in 2019, we will have to somehow deal with this, if we want to maintain the adequacy status.

I'd like, then, to know from each of you what you're thinking on the right to be forgotten so that we can clear the air once and for all.

Ms. Jennifer Stoddart: First of all, with great respect, honourable member, I don't think the air will be clear on this for probably a generation.

Mr. Raj Saini: I was hoping to be encouraging.

Ms. Jennifer Stoddart: Yes, I know. I hate to put such a damper on your observations, but I think we have to put this into perspective.

As I said, the right to be forgotten does exist in Canadian law. The easiest parallel to it in law of common law origin is a pardon. A pardon, I think, still exists in Canadian criminal law whereby, if you haven't done anything wrong for...it used to be five years, you can apply to the Governor General for a pardon. That then shields you. It used to shield you from inquiries into your past, except for the police. I don't know now, with the evolution of security checks and so on, what it is, but we have had that principle in our law for a very long time.

The idea is redemption, rehabilitation. I think it's a valuable part of a society that values people, so I urge us to look at the right to be forgotten as it has evolved more recently in Europe—in a civil not a penal law context—in that perspective, given that we already have a right of correction that could be strengthened into a right of erasure.

Mr. Tamir Israel: We as an organization continue also to struggle. We have yet to come to a conclusion on what a properly formulated right to be forgotten could look like. What we've done is go through and identify some of the things it should address and some of the hazards it should avoid.

Maybe I'll give you that and it will help a little.

Mr. Raj Saini: Sure. That would be great.

Mr. Tamir Israel: Hopefully it won't muddy the water further.

We actually view it less as a right to be forgotten, as others have said, and more as related to PIPEDA's data accuracy component. What we hear from people who have issues of a "right to be forgotten" type is that it creates a skewed perception of their reputation by highlighting specific things that are not necessarily the definition of their reputation.

We prefer at the outset to even not really think of it. Their solution is not necessarily to make the information disappear but to obscure it, to some degree, so that it's not the first thing that people learn about them, in a way that skews their perception of their reputation.

That being said, reputation is a tricky thing. Many of us have things out there about us that we wouldn't want to define us but which should, for legitimate reasons, be part of our reputation. There's an objective component to it. That's where the struggle, in our view, comes. It's about how we formulate something that addresses what is a challenge for some people.

In relation to the EU right, we think that a Canadian right would probably be narrower in scope, in the sense that it would at the very least apply to a smaller subset of subject matter. It might not apply to every piece of information about me that's outdated, but maybe to the more sensitive types of information, information that is having a demonstrably negative impact—medical conditions, financial information that got out there in a way that wasn't necessarily within my control, or information like that. The scope would be narrower, I think, for a Canadian-formulated right, and we have some judicial decisions that have talked about what a privacy harm is in that context, which are relevant there.

There are also additional problems with respect to how this becomes implemented.

The EU relied on intermediary search engines to carry out the right. Those engines are responsible for removing or delisting. We've seen many problems with this intermediary model in many legal contexts. I've heard that, similar to a recent decision of the Federal Court, Globe24h, the Privacy Commissioner went instead after the host site and said it could keep the information up—so it's not forgotten, it's still there—but that it needed to shield certain things from certain types of search exposure.

Something like that, which looks at the primary site as opposed to the intermediary, might be more appropriate and might get at some of the concerns that arise in this context.

That's as far as we've gotten. I hope it helps a little.

● (1655)

Ms. Suzanne Morin: They may have gotten a bit further than we have. We've kept our remarks more on the cautionary side because there's a desire to quickly think about how we can change our PIPEDA law to make sure we're adequate, and I would rather flip it on its head and say let's decide whether or not the right to be forgotten is actually something we need and want in Canada, keeping in mind freedom of expression and other rights that we value in our democratic society. Then we can address to what extent we meet adequacy or not, because the rest of the world that doesn't have adequacy is still having transfers of data between countries.

Once again, I guess maybe what I would repeat is that adequacy is great and it's very convenient, but we shouldn't do it to contradict the democratic values that we have.

Mr. Raj Saini: I have another major question, which hopefully I'll get a chance to ask, but I want to thank you all very much for your consensus.

The Chair: Thank you, Mr. Saini.

We now move to Mr. Kelly.

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

Before I question these witnesses and have the floor, Mr. Chair, I'm going to move the motion that I put on notice at the last meeting that the committee invite the President of the Treasury Board, the Honourable Scott Brison, to appear before it as soon as possible to discuss the recent decision to postpone his proposed reforms to the access to information legislation.

The Chair: Mr. Kelly, your motion is in order, and it is now past the 48 hours, so it is now the motion that's before the floor.

Would you like to speak to your motion, Mr. Kelly?

Mr. Pat Kelly: Yes, I would.

We spent quite a bit of time at the beginning of this committee. We worked very hard together to prepare a report that I think we all felt good about and that addressed the concerns that were raised by many witnesses, including today's witnesses. All three of you, I believe, participated in that study.

The President of the Treasury Board, in his mandate letter, is asked to proceed with these reforms. There was urgency expressed by many of the witnesses that appeared then on those reforms. When the Liberal Party ran, their platform contained a promise to initiate these reforms, and the minister has delayed. He appears to be thus far failing to keep his promise, and with the timeline he's now giving himself, looks to be well on his way to breaking that promise of achieving this before the next election.

I think it's important that we hear from him. I move that we call him to explain himself.

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

I have a speaking list that has now started.

Mr. Jeneroux, please.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, Mr. Chair, and thank you witnesses for being here today.

Although this is of utmost importance to the committee, it has been something where we thought we had goodwill from the minister. When he came before the committee, he even made a change to the act prior to coming to the committee in the reversal of the five-dollar fee, which we thought was an act of goodwill. We thought we had started a good relationship with the minister. However, now, through the media, it seems that he has announced that he won't be going through with changes to the Access to Information Act, which should be of priority to this committee because, quite frankly, that's what we have spent a lot of time doing.

He was given the priority to do this and to do this fast. I believe he said he would have those changes in early 2017. Unfortunately, it is now early 2017, and he has reneged on those changes.

As this committee is familiar—I have quoted it many times before—in the “Real Change” document that the Liberal Party ran on, number one under the section on open and transparent government were the words, “We will update the Access to Information Act”. It seems to be yet another example of backing away from this promise. There seems also to be a bit of a trend for this particular government to do this.

We would like to nip this in the bud, catch it before it goes anywhere, and have the minister come before us and explain why he has decided to renege on this promise.

● (1700)

The Chair: I see no more speakers on the list. I will therefore call the question.

(Motion negatived)

The Chair: We'll return to Mr. Kelly. You have 30 seconds used up. You have six and a half minutes left to propose questions to our witnesses.

Mr. Pat Kelly: Thank you, and I'll probably share part of my time with Mr. Jeneroux.

I'll start with Mr. Israel. You referred to the act as generally well adapted but lacking enforcement. Can you tell me exactly what you think is most important? Is it just simply a matter of establishing order-making power and the power to impose monetary fines that is needed?

Mr. Tamir Israel: We propose some specific tweaks that we think will help improve the overall ability of the act to address modern challenges, but we think enforceability and including the incentive to proactively comply constitute the biggest step that needs to be taken, in part because it has far-reaching implications. It makes organizations take it more seriously and start looking at their own practices proactively and not necessary wait until there is a complaint before the commissioner or the commissioner comes knocking.

From what we've heard from lawyers who regularly advise businesses of different sizes and from our experience working with companies internationally on this, we think they simply take it more seriously when there is a potential penalty.

We think that's the single biggest thing.

Mr. Pat Kelly: I'll turn it over to Mr. Jeneroux.

Mr. Matt Jeneroux: Thank you.

Thank you again for being here. I'm sorry for the delay.

Ms. Stoddart, I want to say this as politely as possible; you dated yourself already, in your opening comments, as to how long you've been around this game, if you will.

Ms. Jennifer Stoddart: I am dated.

Mr. Matt Jeneroux: I don't feel bad, then, about bringing up that you were here during the last PIPEDA review in 2007. At that time, you advocated for reforms to the act.

These were the three that you advocated: the commissioner's powers should not be broadened; the transborder flow of personal information should be controlled using the current laws and private sector contractual agreements; and lastly, the process for designating investigative bodies should be established and regulated under the act.

You've addressed a little bit of this list, but do you mind making clear here for us and for the analysts your stance on these over the last 10 years and whether your views have changed or not.

Do you want me to read them again?

Ms. Jennifer Stoddart: I forget what your first one was, but my views have definitely changed. They changed during the time I was Privacy Commissioner. This is a fast-changing world, so what I'm concerned about now is what I talked to you about here in very broad terms.

Some of these issues have been dealt with and were no longer discussed in my subsequent reports on this issue or subsequent PIPEDA reviews. I think more recent positions would be more useful to look at.

Mr. Matt Jeneroux: Okay. That's helpful. Thank you.

The GDPR is coming in 2018. It's going to be part of the European Union's privacy protections. With it ahead of us, we have talked a little bit about the right to erasure. My colleague Mr. Saini brought it up. Are there other measures under the changes being reflected in the GDPR that we should be focusing on as of importance, knowing that this is coming in about a year from now?

I'll open it up maybe to Ms. Morin to start.

● (1705)

Ms. Suzanne Morin: I would maybe flip the question on its head, as I did at the end of my earlier remarks. We should be looking to make the changes we think we need to make to our privacy legislative framework based on our values and our own democratic system in both our common and civil law jurisdictions.

Mr. Matt Jeneroux: Let me interrupt. I'm sorry to do that.

The concept of my question is, knowing that this is coming already in the European Union but recognizing that while our laws and our values here in Canada are important, this could or will have an impact on us here in Canada too, is there something we should be focusing on specifically, coming through this, that would force us to focus perhaps a bit differently from the way you're focusing now.

Ms. Suzanne Morin: Europe is catching up in many respects to things we've had as part of our privacy regime for a long time, such as the accountability principle. Breaches is an area that exists here that is newer in Europe. Privacy impact assessments and privacy by design, those are terms and practices that were coined here in Canada. They're actually playing catch-up and have tried to leapfrog in some respects.

The position the Canadian Bar Association is trying to present to committee members here is that we should not change our laws simply because the EU is doing so. Will it have an impact on us? Inevitably, I think it will. The fixation on adequacy, as I mentioned before, was wonderful, it was convenient, and it was very good for Canadian business, because it simplified the transfer of information. It's not the only way to do it. There are other mechanisms and the rest of the world is using those other mechanisms.

If we could get it easily, absolutely I think a lot of people would support doing so, but I don't think we want to do it at all costs. I think some of the things we're seeing in the GDPR may actually go too far.

Mr. Matt Jeneroux: Okay.

Any comments, Mr. Israel?

Mr. Tamir Israel: I just want to say that it's hard to predict, as my colleagues have said, how those obligations will also translate through the adequacy. It's not likely to be a direct cut-and-paste, so it probably will be easier to make a case for adequacy if we have elements addressing key new developments there, but that are also aligned with Canadian laws. Again, not to sound like a broken record, I think that enforcement will be potentially challenging in this particular process because that is one area where we are out of step with other data protection commissioners around the world, and where the EU has made substantive improvements recently.

The Chair: Thank you very much.

We now move to Madame Trudel for up to seven minutes, please.

[*Translation*]

Ms. Karine Trudel (Jonquière, NDP): Thank you.

Good afternoon everyone.

First of all, I have a special request, Mr. Chair. Since there is a lag before we hear the interpretation, when there is a vote I would like us to take into account the fact that I may answer a little later. I believe you missed my answer during the first vote.

So, when there are votes, I would ask you to think of me and to the fact that there is a brief delay before we hear the interpretation.

[*English*]

The Chair: No worries.

[*Translation*]

Ms. Karine Trudel: Thank you.

[*English*]

The Chair: Your vote counted.

Some hon. members: Oh, oh!

[*Translation*]

Ms. Karine Trudel: Thank you.

[*English*]

The Chair: Just for the record, it was three to six.

[*Translation*]

Ms. Karine Trudel: I apologize for this intervention, but I have to find a way to be heard.

Welcome to the committee.

I also apologize for the delay; we were held up at the House.

Thank you for your presentation.

You spoke about the right to be forgotten. I know that there will be other questions, but this is a topic that drew my attention in the documentation. I'd like to go back to that question. I'm not a lawyer by training, so please forgive me if I do not use precisely the right terms.

My question is addressed to all three of you.

Concerning the right to be forgotten, children and adolescents are the most vulnerable. With tablets and telephones they have access to almost everything. Children and adolescents may sometimes do things that will last, and that could have consequences later.

Could PIPEDA include some specific provisions concerning consent for the collection of information and the online reputation of children and adolescents?

● (1710)

Ms. Jennifer Stoddart: I can begin to answer.

I would say that the answer is no. We are looking at a lot of constitutional challenges. There is less of a risk regarding the right to be forgotten and the right to freedom of expression than there is regarding federal initiatives concerning children. Generally speaking, this falls under provincial jurisdiction. Although this is a very important matter, it is better to approach it from the angle of strengthening the principle of consent. We might have to look at the notion of sensitive data, which is present in the European regulation.

Ms. Karine Trudel: Did you want to make some other comments, Mr. Israel?

[*English*]

Mr. Tamir Israel: Yes. There was a recent provision that was added to PIPEDA that strengthened consent in situations where it's not clear that the people consenting have a full understanding of the impact of their decisions. I agree with, I won't say the commissioner, but the former commissioner, that it may be harder to draw clean, age-specific lines at the federal level than at the provincial level. However, there may be room for a more generalized policy that is framed in broader terms like that one, but that is more specifically tailored to some of the challenges that you're talking about, and to use, but without setting specific ages, like age barriers, in the way the European approach did.

[*Translation*]

Ms. Karine Trudel: Ms. Morin, do you want to speak?

Ms. Suzanne Morin: Yes, briefly.

Mr. Israel explained that the last time changes were made to the act, an element was added to the notion of consent, known as valid consent. It was already covered, but a clarification was made precisely to protect the more vulnerable groups, such as the elderly and children. The purpose was to reinforce the requirement that organizations ensure that there is valid consent when children are involved. When children are very young, it is very difficult to ensure that. You have to depend on the parents, and there are limits to what you can do.

Ms. Karine Trudel: Thank you.

[*English*]

The Chair: Colleagues, you will notice that the bells are ringing. Apparently, we have an unscheduled vote that has been called in the House. The 30-minute countdown clock has started. If we wish to proceed any longer, we will need unanimous consent from the committee to do so.

Madam Trudel still has about three minutes left in her time, and we still have about seven minutes left to finish the first round. Might I suggest that we finish the first round, if we have unanimous consent to finish the first round, to make it worth the time for our witnesses, and then proceed to the vote? Do I have unanimous consent to do that?

Some hon. members: Agreed.

The Chair: Thank you, colleagues.

Madam Trudel, please finish with your time.

[*Translation*]

Ms. Karine Trudel: Thank you.

Do technological developments have an impact on the technological neutrality of PIPEDA?

Ms. Jennifer Stoddart: I am going to ask the current practitioner to answer your question.

[*English*]

Mr. Tamir Israel: I think PIPEDA has the flexibility to address new technologies. The challenge is to do it quickly enough. Some of the things that have been discussed, and that the Privacy Commissioner's office has done in the past and is doing now, are to proactively address specific issues like the right to be forgotten and looking at consent to see whether it's keeping up. Maybe issuing context- and sector-specific policies to address specific issues that are emerging under the broader principles can help it continue to do that.

I think the potential for it to address these new technologies is there. The challenge is that it is still mostly complaint-based, even though there are many proactive measures coming out of the office. But I think the flexibility is there to do that, if that helps.

● (1715)

[*Translation*]

Ms. Karine Trudel: Do you have something to add, Ms. Morin?

Ms. Suzanne Morin: I agree. PIPEDA is sufficiently flexible to allow us to take into account the changes due to new technologies.

In 2001, there was no Twitter, Facebook, Google or LinkedIn. None of those services existed at the time. And yet those organizations and the Office of the Commissioner managed to resolve complaints and they still do. Technology does evolve, but PIPEDA is flexible enough to allow us to adapt to these changes. As I mentioned previously, the act was drafted with an eye to keeping it neutral.

[*English*]

Mr. Tamir Israel: The one thing I would add is just that in our comments we flagged the issues arising from algorithmic decision-making and automated decision-making. I think those are ones that PIPEDA has struggled with analogs of in the past. That's an area that's technologically becoming very central, so a lot of decisions are becoming automated in ways that are very opaque. The commercial secrecy that can attach to those makes it very difficult to even understand how the decision was made, and because that decision is based on personal information, that is something that PIPEDA has historically tried to address.

I think it's going to be a problem down the road that should at least be examined in a very context-specific way, and it affects children, adults, everyone.

The Chair: Okay. Thank you very much.

In order to make sure we get to the vote on time, we'll now move to Mr. Erskine-Smith. Try to keep it within seven minutes, please, sir. Thank you.

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

Thanks to all of the witnesses.

I got married a number of years ago. When I and the wedding party bought our suits for the wedding, we bought them from Indochino online. For the next few months, after I logged into my Gmail, I got a Google ad popping up, saying “Visit Indochino”. I don't recall reading the policy when I signed up for Gmail. I don't recall what I consented to. Apparently I consented to that.

Now I'm okay with that targeted advertising, but I want to ask Ms. Morin this. You say the consent model works. I think the principle-based model that we have under PIPEDA is why you have all said it has stood the test of time in its own way. Now I take your position, Ms. Morin, that we ought not to change the consent model if it's working just fine for private practice.

Ms. Stoddart and Mr. Israel, should we be looking at ways to change the consent model? The current Privacy Commissioner has a discussion paper right now that talks about big data and the Internet of things, and suggests that perhaps the current consent model is insufficient. Is it insufficient?

Mr. Tamir Israel: I think you can get to a more robust consent requirement with the principles that are there. We suggested incorporating privacy by default explicitly as a guiding principle. I glossed over it a bit because you were short on time, but I would emphasize the need—in those situations—to have a pop-up that says, “Oh, by the way, we're going to read through your emails, and if there's something that says 'suits', you're going to get suit ads. If not, go here and check over here”. Privacy by default would push a more explicit interaction there. There is a choice.

Mr. Nathaniel Erskine-Smith: That doesn't sound like a change to the law per se—perhaps in regulations. It wouldn't be a change to PIPEDA. You're saying that it would be building on the current principles in PIPEDA.

Mr. Tamir Israel: I think currently that's implied, but if it becomes more rigorous, such as something that goes to every single device you have in your house and your TV is recording you by default, I think you can get.... There's a principled way of getting there as well as the legislative way. A legislative way would provide the guidance to push you there.

Mr. Nathaniel Erskine-Smith: All right.

Ms. Stoddart, do you have any views on whether we're actually building upon the current consent model?

Ms. Jennifer Stoddart: I think we should look with interest on the work that will come out of the Office of the Privacy Commissioner, just because they have a lot of expertise and a lot of input.

I think what's interesting is what is being done in the European Union. If I understand it correctly, certainly consent is being strengthened. Consent has to be robust and forthright, and up front, but then they say there are areas where you don't need consent unless there's something that they call the overriding interests and rights of the data subject. I wonder if that would not be a clearer way to go for everybody, rather than this gradation of opt-in, opt-out, implicit consent, and upfront consent. I would encourage—

● (1720)

Mr. Nathaniel Erskine-Smith: Do we wait for the Privacy Commissioner's recommendations, consider them, and go from there?

Ms. Jennifer Stoddart: Yes, I think they probably spend more time than any of us on thinking about this.

Mr. Nathaniel Erskine-Smith: In the interests of time, for public reporting requirements with respect to data shared with law enforcement agencies, Ms. Stoddart, you recommended a change when you were Privacy Commissioner.

Mr. Israel and Ms. Morin, should we be imposing a clear transparency requirement on the information that is shared with law enforcement agencies, at least to know the number of times such information has been shared?

Ms. Suzanne Morin: My answer will be easy. We don't have a view on that.

Mr. Nathaniel Erskine-Smith: Okay. That's easy enough.

Mr. Tamir Israel: Yes, we would recommend one. We would recommend maybe not a blanket one per se, but a mechanism that would explicitly allow the Privacy Commissioner to impose sector-by-sector and scope obligations. It may be more appropriate for some.... Electronic communications is easy, I think. For others, such as the restaurant sector, maybe they get one a year, but they don't need a transparency report.

Mr. Nathaniel Erskine-Smith: My last question is with respect to the powers of the Privacy Commissioner.

Ms. Stoddart, you recommended improvements to powers, but that wasn't clear to me. You set out a range of different options: statutory damages, administrative monetary penalties, and order-making powers. Do you have a strong view one way or the other about the powers the Privacy Commissioner should have in addition to the current powers under PIPEDA?

Ms. Jennifer Stoddart: Yes. I'm on record as having fairly strong views on the powers of the commissioner. Since my retirement I've gone on to say that today I am very convinced that the Privacy Commissioner of Canada should get out of the business of investigating every complaint that comes to his or her door.

There have been some modifications, but to do smart regulation today and to do smart enforcement, I think you have to be nimble, you have to be sensible, and you have to be up to date. You have to constantly follow what's doing and you have to tailor your response to all the different situations, actors, and technologies.

Mr. Nathaniel Erskine-Smith: That's discretion to investigate complaints as they see fit—

Ms. Jennifer Stoddart: Yes.

Mr. Nathaniel Erskine-Smith: —and improve upon regulation as a result.

The U.K. Information Commissioner levies fairly significant fines, or has in the past, and we don't have powers to fine. In addition to that discretion, should the Privacy Commissioner have the power to levy fines?

Ms. Jennifer Stoddart: Yes.

Mr. Nathaniel Erskine-Smith: Does anyone disagree with that?

Ms. Suzanne Morin: We would say no.

Mr. Nathaniel Erskine-Smith: I have one last question for you specifically. One importance of such fining powers is deterrence.

You mentioned court damages being sufficient. It's been a long time since I was in law school, although not as long ago as Ms. Stoddart, but I remember the case of Ward. It was $5,000 for an illegal strip search. It struck me as terribly low. There wouldn't be a great deterrent that would come out of that. When you say court damages are sufficient, are there examples you could point to?

Ms. Suzanne Morin: Would Ward have been a criminal law case?

Mr. Nathaniel Erskine-Smith: Yes. It was a criminal law case.

Ms. Suzanne Morin: That's different, but for courts, definitely, that is part of what they do. They assess the damage, and based on the damages, they assess awards that go with it.

Mr. Nathaniel Erskine-Smith: If there are cases that are adequate —

Ms. Suzanne Morin: Most recently, there was a case where I think $115,000 was awarded.

Mr. Nathaniel Erskine-Smith: Can you share that with the committee?

Ms. Suzanne Morin: Sure.

Mr. Nathaniel Erskine-Smith: Thanks a lot.

Ms. Jennifer Stoddart: In Ontario, under provincial law, there was $160,000 recently given for damage to reputation.

Mr. Tamir Israel: Just to be clear, that was not under PIPEDA. Again, that covers a very different set of activities, not the regulatory framework that's in place.

The Chair: Thank you very much, colleagues. Thank you to our witnesses.

We apologize for starting late and ending early. If there is any information that we need from our witnesses, please feel free to submit that.

Colleagues, we have about 17 minutes to get to the House. Thank you.