HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 055 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, April 6, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, April 6, 2017

● (1610)

[*English*]

The Vice-Chair (Mr. Daniel Blaikie (Elmwood—Transcona, NDP)): Welcome, everyone.

Thank you very much to our witnesses for being patient as we resolve issues in the House.

I will just mention that because I'm the lone New Democrat on the committee, I'm going to take time to ask questions as well. When I do that, Mr. Kelly will take the chair, and then I'll come back into the chair.

With that, I'll mention briefly who our witnesses are, and then we'll go into the presentations. We have Molly Reynolds, a senior associate with Torys LLP; Paige Backman, a partner in Aird and Berlis LLP; and Alex Cameron, partner and chair, privacy and information protection group, Fasken Martineau DuMoulin LLP.

We'll start with Mr. Cameron.

Mr. Alex Cameron (Partner and Chair, Privacy and Information Protection Group, Fasken Martineau DuMoulin LLP, As an Individual): Thank you very much and good afternoon. I very much appreciate the opportunity to share with the committee some of my personal thoughts about important issues of privacy that affect Canadians. As mentioned, I'm a partner with the law firm Fasken Martineau. I've been working in the privacy law field for 17 years—in fact, pretty much since PIPEDA came in. In this case, however, I'm appearing before the committee purely as an individual today.

I have read many of the transcripts of the evidence that has been given to date before the committee, and certainly you have heard from a very wide range of perspectives and experts in the field. I share many of the views that have been expressed to date, in particular the submission by the Canadian Bar Association, of which I am a member.

In very broad strokes, my perspective on the issues before the committee is that the existing consent and ombudsperson model under PIPEDA has been proven to be remarkably resilient, adaptable, and effective in achieving the purpose of PIPEDA, which is, of course, to recognize the right of individuals to privacy and the needs of organizations to collect, use, and disclose personal information. On balance, in my view, the model should continue, absent a compelling need for some legislative change.

As for what I do want to focus my brief remarks on, one of the unique aspects of my practice and experience is privacy-related litigation. I want to suggest to you that the developments in the courts in respect of privacy-related interests and claims, which have been very significant over the last five years in particular, form a very important part of the context in which PIPEDA operates, and as I'll suggest, the context in which any deliberations about changes to PIPEDA should take place.

In addition, in my review of the evidence to date, it does not appear that the committee has heard very much about the developments in the courts. I saw that there have been some references to some developments in passing, but in the interests of trying to contribute something a bit new that you may not have heard or focused on previously, I'll focus my opening remarks on that issue, although I am happy to answer questions on other topics.

As the committee is aware, under PIPEDA there is the possibility of going to Federal Court in respect of matters addressed in a commissioner investigation and report. The court has the power to award damages and other relief, and that power gives some additional teeth to the legislation.

I want to describe what I see by referring to a bit of a story that we have seen outside of PIPEDA, which emerged starting in or about 2010.

First, in or about 2010, we started to see a handful of cases going to Federal Court under PIPEDA, in which individuals were typically awarded $5,000 or less for privacy breaches. Most of those were what I would characterize as relatively minor privacy incidents. We have seen a continuation of those types of cases going to Federal Court under PIPEDA since that time.

● (1615)

However, in terms of where the significant developments have taken place, in or about 2012 and into 2013, what we have witnessed in Canada is really an unprecedented increase in privacy-related litigation activity outside of PIPEDA. These cases are not going through the commissioner's process and on to Federal Court. These cases are being brought directly to court through tort claims, contract claims, negligence claims, and other causes of action. They've been very significant in the range of issues that are covered.

We have many cases that have dealt with cybersecurity-related issues, from computer hacking to snooping in the workplace, lost USB drives and lost devices, alleged misuse of personal information for commercial purposes, and inadvertent disclosures of information. These have crossed both private and public sector boundaries. This real proliferation of litigation started in or about that time and was something that had never really been seen before in Canada.

I highlight further that this development was unprecedented both in terms of the volume of activity—so a lot more cases were being brought—and also, in particular, in the fact that they were being brought not just by individual complainants but also through class action litigation. There are currently many cases that have been brought and a number of class actions that have been certified. A few of them have now been settled, and this litigation activity continues.

Significantly, the developments, in that respect, have meant that many cases that might otherwise have gone to the commissioner or through the PIPEDA process are, instead, just going directly to the courts. In my submission, that's something that can't be ignored in assessing some of the issues that I know are on your mind in terms of potential areas for change in PIPEDA, which I'll come to in just a moment.

The expectation, I would add, is that the litigation trend is going to continue because of the mandatory breach notification provisions, which may yet come into force in PIPEDA. The idea is that as more notifications are required to be given by organizations with respect to privacy breaches, we will see individuals seeking legal advice, and potentially more litigation claims being brought in the wake of notifications being received. That is the expectation.

In terms of how this relates back to some of the questions that I know are on the table with regard to changes in PIPEDA, among the reasons that I suggest this significant development that we've seen over the last five years is relevant is that, for example, it responds to a suggestion that in the absence of enhanced powers for the commissioner, under PIPEDA, organizations will not or might not take privacy compliance sufficiently seriously. It's often touted as one of the reasons in support of doing that.

Certainly in my experience, organizations are taking privacy seriously, but I point to the litigation-related development as part of the broader context in which these issues are being addressed. Those potential claims present very real legal risk—to real dollars having to be spent to deal with those issues and, ultimately, of course, potential liability for a wide range of privacy breaches. The courts have taken on a very significant role in shaping privacy protection in Canada at a practical level in that respect.

I'd further suggest, in terms of other areas of relevance of this development—and I know it's been highlighted by the bar association—that this broader context is also important in terms of assessing the question of adequacy in relation to the GDPR that's emerging from the EU.

I'll stop my remarks at this point. Of course, I'd be happy to take questions on that topic and the others on your mind, but I wanted to contribute that piece in particular, as I haven't seen it reflected much in the testimony to date.

Thank you.

● (1620)

The Vice-Chair (Mr. Daniel Blaikie): Thank you very much, Mr. Cameron.

We'll go now to Ms. Reynolds.

Mrs. Molly Reynolds (Senior Associate, Torys LLP, As an Individual): Good afternoon.

Thank you for inviting me to appear before you today in respect to your study of PIPEDA. I'll give you a short background on me and then focus on the two issues that I submit should be part of your study of this act.

I am a privacy and data security litigator in Toronto. I counsel private sector organizations on both Canadian and American privacy law compliance. I also represent individuals who seek to enforce their privacy rights in the civil courts, including in this unfortunate area of non-consensual distribution of intimate images. I also note by way of background that I'm somewhat closer to the generation that grew up with the Internet, rather than the generation that saw the first office fax machine. That's part of the context that I bring to my perspective today.

Let me start with the top priority in my submission.

The single most significant reform that could be made to PIPEDA is to permit advance compliance rulings. We can do more to protect the personal information of Canadians and to improve private sector compliance by explicitly empowering the Office of the Privacy Commissioner to issue compliance rulings before a new initiative is launched by the private sector. You have already heard, I believe, about advance rulings, from my colleagues at the Canadian Bar Association, but this framework would allow organizations to voluntarily submit to the OPC a new initiative that may affect personal information—that might be a new product, a new technology, or a new service structure—and then receive the OPC's feedback on whether that design will likely comply with PIPEDA.

In my view, this authorization would require legislative amendments, because the OPC's powers as they're currently framed under the act really deal only with conduct of investigations, audits, or compliance agreements where an organization is believed to be out of compliance with the act, but the power to issue advance rulings shouldn't hinge on any belief of non-compliance. It should be voluntary, and it should be proactive on both sides.

In my submission, the power to issue advance compliance rulings would have four significant impacts.

First and foremost, it would better protect Canadians. The OPC and business would be using their resources to proactively protect Canadians' privacy rather than simply investigating and penalizing compliance failures. Just as we say that an ounce of prevention is worth a pound of cure, resources are better spent ensuring that privacy law compliance occurs before anyone's information is put at risk with a new initiative.

Second, it would help more organizations and it would better help the Office of the Privacy Commissioner because, through assessing these new initiatives, the OPC would gain better insight and more current insight into new developments and new technologies that affect personal information in the Canadian economy. This would allow it to provide more technical and more current general guidance and share the lessons learned with other organizations to better promote privacy awareness across the economy.

Third, advance rulings would increase certainty for all involved. An advance compliance ruling would allow organizations to rely on the commissioner's expertise in designing appropriate personal information protection in new initiatives. This will provide them with more certainty around what the compliance requirements are and a fresh perspective on the privacy implications of their new technology or their new project without stifling innovation.

Fourth, advance compliance rulings would improve risk assessment in the private sector, in my submission. The advance ruling option would encourage businesses to implement internal privacy impact assessment mechanisms, and that would have a positive impact on PIPEDA compliance across organizations and across the industry, beyond any one initiative that may be submitted to the OPC for review. As many of you may know, the Treasury Board Secretariat already requires government institutions to perform a private impact assessment to measure the potential impact of a new initiative on individual privacy rights, but we could craft this in the private sector so that in order to seek an advance ruling, the OPC would require an organization to first submit the results of its internal privacy impact assessment. This would further the spread of PIAs as a standard practice in the private sector and lead to more consistent protection for individuals' private rights.

● (1625)

Finally, on this first issue, I would note that advance compliance rulings should not be binding for either party. They should encourage a voluntary dialogue between industry and the regulator to further this proactive protection of personal information.

The second area in which, I submit, PIPEDA reform would have a significant effect is to establish a clear threshold for when information has become sufficiently anonymous that it's no longer defined in the act as personal information. The Privacy Commissioner did address this somewhat difficult issue in the discussion paper on consent and privacy, which, I believe, has been discussed here before. One of the essential features, which I know you've heard about time and again, is that PIPEDA was designed to be, and is, technology-neutral, but as technology develops, we're actually creating new forms of information. You think of metadata. You think of the results of data analytics. We have new categories of information, and it's often challenging for the private sector to determine whether the data it is creating or it is handling is personal information at law.

We could improve certainty here if PIPEDA or the regulations thereunder actually codified the threshold for what is identifiable information. The Privacy Commissioner's discussion paper refers to two thresholds that could be considered: whether there is a serious possibility that the individual could be identified—that's the one that Canadian courts have looked at before—or whether identification from the information is likely, which is the threshold that the U.K. commissioner has used previously.

The issue of de-identification does link back to my first point. If the Privacy Commissioner is given the authority to provide advance rulings to businesses, organizations could then test their assessments of whether the information they are handling is so unlikely to be associated with an individual that it's actually taken outside of the scope of the act, and they could do that before they finalize their program designs. If the OPC says they're wrong, safeguards could be put in place well before any information is actually put at risk. This is very consistent with the Privacy Commissioner's mandate to protect and to promote privacy rights.

In addition, on this point, a standard for de-identification is relevant to the right, in Canada and abroad, to have personal information deleted. As technology continues to develop and the storage of information becomes more decentralized, it's often becoming impossible to permanently delete every copy of every record that may contain an individual's personal information, especially where that definition of personal information may change with the context or with the technology we're using.

The act already contemplates that information should be destroyed or erased or, importantly, made anonymous when it's no longer required, and it contemplates that an organization may be required either to delete or to amend personal information when an individual requests that.

This is consistent with the idea of having a strict threshold for de-identification or what constitutes anonymized information. The value of that existing framework is that it is still technology-neutral, and we can protect individuals' privacy rights even where the technology we're using to store personal information doesn't allow us to permanently delete it. The alternative way to eliminate personal information in that context is to anonymize it. In my view, these options around amending or anonymizing information already exist in the act and can be held to be essentially equivalent to the EU general data protection regulation as it relates to the right to erasure, but individuals, organizations, and the regulator would benefit from a statutory threshold that governs when data is no longer deemed to be personal information at law.

By way of brief conclusion, I do note that many of my colleagues who have appeared before you on previous days have addressed the EU GDPR in some detail, and I don't want to dwell on that for too long. But as it relates to this issue of anonymizing personal information and whether the existing retention requirements under the act are equivalent to this right to erasure in the EU, I would just urge you to focus your study on the interests of Canadian consumers and Canadian businesses that are operating under both Canadian and international law. I respectfully submit that the focus of this study should not be reforms that would merely encourage an adequacy ruling from the EU, but rather areas in which harmonization of international standards with Canadian privacy law would truly help consumers and businesses protect information more consistently and with more certainty across jurisdictions.

● (1630)

I look forward to my colleagues' comments and any questions that you might have.

The Vice-Chair (Mr. Daniel Blaikie): Thank you very much, Ms. Reynolds.

We'll pass it now to Ms. Backman for 10 minutes.

Ms. Paige Backman (Partner, Aird and Berlis LLP, As an Individual): Good afternoon and thank you for inviting me here to contribute to your study on PIPEDA. The task facing this committee is challenging but extremely important.

Unlike Mr. Cameron and Ms. Reynolds, I'm a corporate lawyer. Among the three of us, there are two litigators and a corporate lawyer.

I am the co-chair of our firm's privacy and data security group, but I'm also a director of the CyberSafety Foundation, which looks at the protection of individuals with regard to cybercrimes and online activity. Those two positions, I would suggest, are often not in alignment, but I would suggest that with some thought you can further both interests—the advancement of business and the protection of individuals.

My submissions this afternoon are my own personal ones, and I welcome and I applaud Ms. Reynold's and Mr. Cameron's insights. I think they're very valuable.

The pace of technological advancements since the introduction of PIPEDA over 17 years ago has been staggering as has been the way in which businesses have created and continued to create new business models applicable to all ages and all demographics to take advantage of the new technologies. This results in an equally significant evolution in the ways in which individuals interact with technology; the nature and scope of personal information being collected, aggregated, reidentified, used, disclosed and sold; the manner in which businesses can commercialize this information; and the resulting impact on individuals arising from the foregoing.

As I think everybody who has offered submissions has probably noted, this has created quite a challenge for the application of PIPEDA and its evolution over the last 16 years.

While there are additional areas within PIPEDA to which I can propose amendments, for the purposes of my submission, I'm focusing on three key areas: a framework for consent, oversight of minors, and a limited right of erasure. While I will not provide recommendations regarding enforcement powers of the OPC, I will conclude with a consideration regarding the same.

For the audience at hand, it goes without saying that valid consent is the foundation of PIPEDA and of all privacy laws around the world, and my experience supports the numerous studies and extensive submissions to the committee that conclude that privacy policies and the way in which they are currently used are highly ineffective at communicating important information and obtaining the requisite consent.

This is an issue for both organizations and individuals. This is not simply an issue for individuals. Organizations relying on privacy policies have a false sense of security that they've obtained the requisite consent. If individuals cannot reasonably understand how their personal information will be used or disclosed, or if they don't understand if and when a business' information-handling practices go beyond what is required to fulfill a legitimate purpose, there is no consent. If we fix this element, it's going to be a critical pathway forward to both sides of the party coming together.

It would be unrealistic to suggest that we can find an approach that will satisfy every individual across all demographics. However, proper framework for consent will allow businesses to have greater certainty that they've established the requisite consent and will also provide individuals with meaningful information on which they can provide or not provide their consent.

To that end, I recommend that the following four-part framework for supporting consent be adopted. One, define information-handling practices for which consent may be implied, and incorporate the same into a model code attached to PIPEDA. Certain suggestions for terms to include in this model code are attached to schedule 1 in my written submission. This will clarify practices on which organizations can rely on implied consent, and to the extent an organization's practices deviate from such a model code, the organization's privacy policies would focus on those supplemental practices.

Two, require expressed consent for those practices that deviate from or are in addition to the model code.

Three, practices relating to secondary purposes should be specifically delineated within privacy policies, and a clear and readily available opt-out right for each secondary purpose should exist.

● (1635)

The Vice-Chair (Mr. Daniel Blaikie): Ms. Backman, can I just ask that you slow down a little bit for our interpreters?

Ms. Paige Backman: Sure. My apologies.

The Vice-Chair (Mr. Daniel Blaikie): They're having a hard time keeping up.

Thank you very much.

Ms. Paige Backman: If anybody missed words of wisdom, let me know.

Voices: Oh, oh!

Ms. Paige Backman: For each instance where express consent is required, a copy of the privacy policy should be provided to the individual who provided express consent in a form that can be retained by the individual. This is consistent with consumer protection legislation across Canada.

The second area for which I'll provide recommendations involves the oversight of minors. I represent a number of large education-focused businesses as well as other non-education businesses whose online sites and apps are used by minors. One of the most consistent and significant issues they grapple with is when it is appropriate to obtain consent from someone under the age of majority, and when and how to obtain the consent of the minor's parents or guardians.

I incorporate into my submissions some studies, as referenced in my written submission, that find that a significant percentage of young children are participating in online activities. I also incorporate a reference to a recent report by the Children's Commissioner for England reflecting on the terms and conditions of Instagram, an app that has been used by over 50% of children between the ages of 12 to 15; and 43%, or almost 50%, of children 8 to 11 years old in England.

Instagram's terms and conditions were 17 pages long and contained 5,000 words, with language and sentence structure well beyond the capability of the average youth—and, I would suggest, the average adult. When asked to read through the terms and conditions, the children and the youth were frustrated and understandably confused. While young Canadians may be text-savvy—as I can attest from my own young sons, who are perhaps more text-savvy than I am—children and youth are often not able to comprehend the terms of the policies even when these are brought to their attention, and often lack the knowledge and understanding of the business processes and consequences of those processes required to provide informed consent.

To that end, I recommend that organizations be required to obtain verifiable consent of a parent or guardian of individuals under 16 years of age. Any method to obtain verifiable consent should be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent or legal guardian. While the age of 16 is not a magic number, it is consistent with domestic laws as well as international laws, such as the GDPR. In relation to the approach to obtain the consent of the parent or guardian, our recommendations are consistent with the U.S. FTC's children online protection rule as well as the GDPR requiring organizations to make reasonable efforts to obtain verifiable parental consent, taking into consideration the available technologies.

The third area to which I will recommend amendment to PIPEDA relates to a limited right of erasure. We've heard a lot about it. There are definitely pros and cons to both sides. With that in mind, my recommendations are to a limited right of erasure.

To this end, I incorporate reference to studies, included in my written submission, that reflect the extensive use by young children of websites and online application that involve the collection of highly sensitive information, such as photos, videos, journal-type entries, and location, and posting the same publicly. Either they are posting it or others are posting it and reposting it.

There are significant benefits to children and youth engaging in online resources through social media. However, an error in judgment of a minor, or judgment of another that involves the information of a minor, can have significant short-term and long-term consequences for both the minor and society. More frequently, we are seeing that an online footprint, whether placed there by the individual, the minor or child themself, or someone else, can be central to online bullying. Such bullying can significantly impact the physical and mental health of the child and can lead to long-term consequences for both the minor and society.

While the parental consent recommendation above addresses the protection of minors at a particular point in time, we need to also address the ongoing information sharing and use of minors' information in commercial activities. Remember, this is all in the course of commercial activities that occur throughout the child or youth's involvement in the online environment, which often goes without parental involvement.

To that end, I recommend that the right of erasure be enacted in relation to minors where their personal information has been collected, used, and disclosed in the course of commercial activities.

Consistent with this recommendation, I note that the GDPR also supports the increased need for the right of erasure when personal information of a minor is involved. Specifically, we recommend the following, and in a manner consistent with the GDPR.

● (1640)

Individuals whose personal information is collected, used, or disclosed in the course of commercial activities, and that is or was collected, used, and disclosed during the time such individual was a minor, should have the right—and their parents and guardians should have the right—to have such personal information deleted without undue delay, except in those limited instances that I have set forth in my written submissions. To the extent that such personal information has been disclosed or transferred to a third party or otherwise made public, the organization that originally collected the information and all parties who are using or disclosing such information should take reasonable steps, including the use of reasonably available technology, to delete all copies and links to such personal information.

My last comment involves the enforcement powers of the OPC. I will not provide recommendations supporting specific enforcement powers. However, for purposes of discussion around the same, I reinforce that the general principles upon which PIPEDA is based, while creating flexibility, create great uncertainties around an organization's compliance obligations. Without greater certainty surrounding the compliance requirements under PIPEDA, it will be unfair and highly prejudicial to impose additional penalties and fines on such organizations.

In conclusion, I reiterate that the task facing the committee is challenging but extremely important. I commend you for your time and effort in modernizing PIPEDA and ensuring the amendments to PIPEDA are relevant and valuable in achieving its purposes. The effort to modernize PIPEDA and ensure the protections afforded thereunder are relevant and valuable will not come without roadblocks; however, decisions not to modernize and amend PIPEDA in a way that results in clarity and protections for businesses and individuals also come at a very high cost.

I hope my submission is of some value. While I limited proposed changes to three key areas, I welcome questions on those or other topics.

The Vice-Chair (Mr. Daniel Blaikie): Thank you very much.

I thank all our witnesses for their presentations.

Our first committee member to pose questions is Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Thanks to all of you for your opening remarks.

Ms. Backman, I've read your brief, and in your opening comments you've already answered a couple of my questions.

One point you mentioned was the need to improve parental consent for minors. Can you give us an idea of some ways to ensure this happens? You've also mentioned in your brief that 16 should be the age. I know that in the United States the age in COPPA is 13, and you've said 16. I thought that was unique. You said 16 because of the Ontario health guidelines, which I thought was unique from that perspective. Can you give us an idea of how the parental consent model might work?

Ms. Paige Backman: Sure, and let's be clear about this. If someone's going to commit fraud, it's tough to guard against that, so let me address two points: one, how to do that, and two, the age of 16.

I think the age of 16 is consistent with laws across Canada. It's also consistent with the GDPR. To me that makes more sense. Just from a practical perspective, I don't think that children of the age of 13 can provide informed consent. To me, that's a non-starter. I question whether even at the age of 16 you can provide informed consent, but at some point you want to show respect for the youth as they grow up and mature, which is why I've also tied in the right of erasure to 18, which allows people to provide consent but then also recognizes that there may still be errors being made by children or by youth.

In terms of how this can be effected, when you sign up for a practice or sign up to an app or a website, you would be asking for a parental email account. One, you'd be confirming the age of the child, and you'd be asking for a secondary email account to verify the consent of a parent. It's not just that you go online but that an email is sent that is somehow verifiable and attributed to a parent, and they would have to also confirm.

● (1645)

Mr. Raj Saini: But on a practical level...? The reason I say this is that I've read your report here. You've given some pretty strong statistics: 24% of grade 4 students and over 50% of grade 7 students have their own cellphones.

Mrs. Paige Backman: Yes.

Mr. Raj Saini: How...?

Ms. Paige Backman: Let's look through this. Absolutely, there are practical challenges. I'm sure that some of the businesses, including some of my clients, may not be thrilled with your suggestion, but I'm looking at these statistics. These are children. They're not sophisticated youth, no matter how technologically savvy they are. They are children who are engaging in this.

When you download an app, you have some sign-up obligations. Part of that would be an obligation to provide information such as a parent name and parent contact information where a secondary.... It's like an email that you may get, to verify that you've accessed an account. It would be redirected to a parental email, and they would have to click that they approve of it. Can that be circumvented? Any of it can be circumvented, but we need to take some additional steps so that it's not simply a young child or a youth. There has to be something else that provides a backstop for that.

Mr. Raj Saini: You've also written in your remarks about the right to be forgotten.

Ms. Paige Backman: Yes.

Mr. Raj Saini: Do you think it's something that should be applicable to children up to a certain age?

Ms. Paige Backman: Yes, I do, up to the age of 18.

I'm not suggesting that the right to be forgotten shouldn't be applicable to adults. I get calls where adults have been slammed on the Internet and have material on the Internet that they reasonably should have removed. For children, this is something that I think we should tackle. We're talking about the use of children's information in a commercial activity. Whether it's the child who puts the information online, a friend of theirs who puts it online, or somebody else who puts it online, this can have serious consequences for the development of the child. This can affect their mental health and their physical health. We're seeing great trends of self-harming of children, because in the online environment they can't get away from the mistakes that are out there.

I'm perhaps not as close to the technology era as perhaps Molly is. I certainly made mistakes growing up, and I can tell you that had that been videotaped or uploaded, I'm not sure I'd be standing here before you, or been called the bar.

We all need to allow our youth and our children to make those mistakes and move on from them. To my mind, the right of erasure applicable to minors, when their information is involved in commercial activities, strikes the balance.

Mr. Raj Saini: Do I have any time left, Chair?

The Vice-Chair (Mr. Daniel Blaikie): You have a couple of minutes.

Mr. Raj Saini: Mr. Cameron, I want to ask you a quick question specifically with regard to your remarks on the Globe24h case. You wrote that the case had “the potential to introduce in Canada a right similar to the 'right to be forgotten' which has emerged in the EU”. Can you highlight for the committee how you feel that might be a precedent? Especially with the GDPR new rules coming out in 2018, do you think that's something we should formulate in Canada for adequacy?

Mr. Alex Cameron: I think there are two questions there. First, is it a topic to be addressed in the legislation? Second, what are the courts doing?

Maybe I'll address the legislative piece first. Frankly, I haven't thought about it in the same terms that Ms. Backman has in respect of a potential limitation to children in particular, but there's no question with regard to the sentiments expressed in terms of the concept. There's not a person among us, of course, who hasn't done things in their past that they may have been deeply embarrassed about or may regret, or who hasn't made mistakes. It's an important issue when someone is forever haunted by easy access to the records of those things.

That is a unique phenomenon that has emerged in the online context in particular. It's not new in the sense that there have alway been issues of skeletons in the closet and things that could be brought up, but it's a very challenging one from a legislative perspective. I don't have a particular perspective on whether or not it's a necessary component of an amended PIPEDA, but it's certainly one that merits a close look.

In terms of what the courts are doing—

● (1650)

The Vice-Chair (Mr. Daniel Blaikie): I'm sorry, Mr. Cameron, I have to jump in here. The seven minutes are up, and I want to make sure that other committee members get their opportunity to pose questions.

Mr. Alex Cameron: Of course. No problem.

The Vice-Chair (Mr. Daniel Blaikie): We'll proceed now to Mr. Jeneroux.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Perfect. Thank you very much.

Thank you, everybody, for being here today. Thank you for your patience while we voted.

I'd like to come back to some of the comments that my colleague Mr. Saini was asking you, Ms. Backman, but I'll also open it up to you, Ms. Reynolds, and to you, Mr. Cameron, on some of the stuff that you started talking about.

First, Ms. Backman, you used “right to be forgotten” and “right to erasure” almost interchangeably, it seemed to me. Going back to your point, what is also clear to a lot of us in the room is that if there are certain things in our past that we feel should be erased, somebody else might not feel that way. Particularly for members of Parliament, in running for public office there may be certain things that other people may find relevant to voting that maybe aren't necessarily what we would like to put out there—myself excluded completely, though.

Voices: Oh, oh!

Mr. Matt Jeneroux: I do want to get your comments on how we're struggling with that—

Ms. Paige Backman: Sure.

Mr. Matt Jeneroux: —because I believe that the Privacy Commissioner is also going through a similar struggle, if you will. He's committed to putting forward a position on this, but it's going to be after our study is done. Hopefully you will be able to provide some insight, and I will also open it up to the other two witnesses.

Ms. Paige Backman: Thank you. I'll take maybe just a minute or two, and then Ms. Reynolds can respond.

It's a good question. It is a struggle to deal with that, which is one of the reasons that I limited my submission to it being applicable to minors. Let's think of the instances in which this may be relevant, such as a criminal record or some sort of a breach of law. Those are not erased simply by taking it offline, so, if you have a criminal past, that will still be accessible. It's just not there for the entire public to see.

What we're seeing more of, or where we're seeing the pressure point, is with poor judgment, which we all experienced as children, whether it's photos from a party with alcohol...which can really have an impact on your right to employment or to getting into educational institutions.

For me, the balance is that I understand that struggle and I think it's a legitimate struggle. I think it becomes more relevant once you become more able to correct your behaviour as an adult.

A child has very limited ability to really understand those consequences and, therefore, to correct the behaviour before this happens. The more significant issues that a child would be involved with, which you would want to know about legitimately, are going to be in a record somewhere. This is simply the additional bad judgment, which we all experience, that is just going to be removed from online.

I think given that this is in the context of a commercial activity, the balance really weighs more in favour of protecting the minor, letting them make those mistakes, and then allowing them to move on.

Mr. Matt Jeneroux: I guess there are degrees of bad judgment, though. We could probably poll the room here and someone would think that something was bad judgment, and something else was stupidity or whatever you want to call it.

● (1655)

Ms. Paige Backman: Sure.

Mr. Matt Jeneroux: I also think there may be other groups out there that may feel that one example of bad judgment was a worse in degree than a previous example of bad judgment. I guess it's a slippery slope with regard to what we do.

Ms. Paige Backman: It is, but I think the line in the sand is that until you are an adult, we're going to give you some leeway here. Let's keep in mind that this is in the course of commercial activity. Someone is making a profit off this information.

Mr. Matt Jeneroux: Yes.

Ms. Paige Backman: This is not a news report. This is not for journalistic purposes. This is in the context of someone making money off this information.

I think that whether in my view it's inappropriate or in your view or in the view of the 50 other people here, the minor or the minor's parent should have the right to say, “You had the right to make money off it. Now I want it gone”.

Mr. Matt Jeneroux: Okay.

Ms. Reynolds.

Mrs. Molly Reynolds: The only thing I would add to Ms. Backman's comments actually relates to one of the points Mr. Cameron made in his initial submission, which is that there is a context in which we look at what the legislative requirements are and what the court's enforcement powers are.

I think it's quite right, as PIPEDA currently does, to place an onus on the source holding the personal information to delete that information when it's no longer necessary or upon request from an individual, but when we're talking about the right to be forgotten, we often start talking about third party intermediaries like search engines. Where we are not going to the source but are going to the organization that's holding that information or maybe just allowing access to it or indexing it, that really should be a matter for the courts to exercise their jurisdiction in terms of injunctions or mandatory orders.

I don't believe that the legislation should be addressing any organization other than the holder.

Mr. Matt Jeneroux: That's fair.

Mr. Cameron.

Mr. Alex Cameron: If I could add one final comment, PIPEDA has built into it, of course, the reasonable purposes concept in subsection 5(3). Irrespective of consent and other provisions, you can do only those things that a reasonable person would consider to be appropriate. That's quite a generic standard, but of course it has to be interpreted, which is the way that the commissioner and the courts have approached it.

It's not without precedent. I'm not saying it's an easy concept to scope, in terms of whether or how that type of right could be scoped, but there are standards to which you could point in terms of how that could be assessed as to what's on which side of the line.

The Acting Chair (Mr. Pat Kelly (Calgary Rocky Ridge, CPC)): I'm going to interrupt now. We have bells now that indicate that a vote must take place in the House of Commons. There would have to be unanimous consent to continue. We have 30 minutes to get to our seats in the House to vote. Unless there is unanimous consent to continue, I will suspend the meeting.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): We're not likely to get the witnesses back. Fifteen minutes should be enough to get to the Hill.

The Acting Chair (Mr. Pat Kelly): Is there unanimous consent to continue for 15 minutes?

Some hon. members: Agreed.

The Acting Chair (Mr. Pat Kelly): Yes? Is there anybody who is opposed to continuing?

Okay. Then we will continue.

Mr. Daniel Blaikie: Thank you very much.

The Acting Chair (Mr. Pat Kelly): We are out of time, so I will go straight to Mr. Blaikie.

Mr. Daniel Blaikie: Thank you very much.

The Acting Chair (Mr. Pat Kelly): If I may, perhaps I'll keep it with Mr. Blaikie, and then the first, if we have two seven-minute interventions.... We'll go to Mr. Blaikie and we'll see.

Mr. Daniel Blaikie: Thank you very much.

Ms. Backman, I wanted to follow up with you. You suggested some ways that we could improve the consent model. I am always curious to hear how, because when we talk about this at the policy level, what I often imagine is an expanding consent form when we talk about what else should be included.

I am wondering if you might be able to describe how you think your reforms would look from a user perspective. What would change for the user when they interact with that?

Ms. Paige Backman: First of all, there is uncertainty about on what basis an organization can rely on implied consent. I think that needs to be clarified. That can be included in a model code that's simply attached to PIPEDA, and organizations can simply refer to that. That would shorten the privacy policies. Really, then, the content of the privacy policies of organizations would focus on the supplemental information-handling practices.

I would then suggest that those practices be split into two parts, those which, although they deviate from the model code, are still necessary for the provision of the products and services requested by the individual, and then those that are secondary purposes, such as third party marketing.

● (1700)

Mr. Daniel Blaikie: Okay.

Ms. Paige Backman: From a user perspective, you're going to get shorter privacy policies and more direct information in terms of what is the secondary purpose, and then the opt-out right from those secondary purposes becomes easier.

Mr. Daniel Blaikie: Thank you very much.

In some of the earlier testimony, I think we heard a clear preference on the part of some witnesses to stick with the current ombudsman model. One of the debates we've been having here at committee is whether it would be appropriate to give the Privacy Commissioner order-making power. Obviously, that would be a deviation from the current model.

I appreciated your suggestions, Ms. Reynolds, about giving powers to have advance rulings. I am wondering if perhaps you and Mr. Cameron, and Ms. Backman, as well, if she wants to jump in on this, could speak to how the power for advance ruling might actually work well—or not—with order-making powers.

One of the disadvantages of conferring order-making powers, we're told by people who don't want that route, is that it becomes cumbersome, it's complicated, and you're creating a bureaucracy. However, if the Privacy Commissioner had those order-making powers, it might incentivize taking advantage of advance rulings, and advance rulings might help mitigate the quantity of order-making instances, if you will. I'm wondering if you could speak to that point.

Mrs. Molly Reynolds: My primary perspective on it is that the current ombudsman model is very close to an effective order-making power. At the end of a regulatory investigation, the Privacy Commissioner will discuss with an organization subject to an investigation ways to remediate whatever failings they found. Although it's often framed as a remediation that the organization has agreed to, the OPC certainly has persuasive power there, and much of what they might order, I believe, if they had that explicit power, we are already seeing in these results of investigative findings. I don't see that it's a necessary gap right now.

Mr. Daniel Blaikie: Do you think it would help with compliance, though, if there were also the ability to attach fines or penalties to orders of the Privacy Commissioner? Or do you think that wouldn't have an effect on compliance?

Mrs. Molly Reynolds: I don't disagree that if there's a bigger stick at the end, the carrot of the advance ruling may be more enticing, but I don't know that there's really a compliance gap that's so large now that additional penalties or additional proactive order-making is really necessary. What you would see with an order-making power or any power to fine is the need for some kind of administrative or judicial appeal model or review model, which would actually make it a lot more cumbersome and probably more costly overall for the public.

Mr. Daniel Blaikie: Mr. Cameron, would you like to speak to that point?

Mr. Alex Cameron: Yes. I'd echo those sentiments. I don't think there's a problem, in my experience, that it would be solving. That's similar to the CBA's submission. If you were to go that route, of course, there would be a lot of things to consider in terms of how the office currently operates versus how it would have to operate under that kind of model.

I suppose I would be coming back to the questions of “To what end?” and “What's the purpose of this?” In my experience, and my feelings are the same as those expressed by Ms. Reynolds, if you're even at the point of being investigated by the Privacy Commissioner, you're not, typically, looking to pick fights or end up at a place where you're feeling like you need to do something that you can't do for business purposes, etc. You're seeking to find a way to work with the regulator in a way that meets your obligations, as you may accept them at the end of that process, under the act. Maybe you agree to make certain changes. We do have the new mechanism of the compliance agreements. It's very new and untested. We may see that this addresses part of what you're getting at.

In terms of the stick, as I addressed in my opening remarks, I think the stick is already there. In serious cases, complainants are going straight to court and suing organizations for privacy breaches in any event, so I don't see how changing the commissioner model would add anything to that.

Mr. Daniel Blaikie: Okay. Thank you very much.

Ms. Backman, do you have anything?

Ms. Paige Backman: [*Inaudible—Editor*] Mr. Cameron and Ms. Reynolds.

● (1705)

Mr. Daniel Blaikie: All right.

In the interest of time, then, I'll conclude my section.

The Acting Chair (Mr. Pat Kelly): Thank you. You're giving us an extra minute there. I appreciate that.

Now we'll go to Mr. Bratina.

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

Mr. Cameron, I was interested in your opening remarks with regard to the model continuing. We heard more discussion about that. You've been in the field since PIPEDA started 17 years ago. That was April 2000. I looked it up. Are we still waiting for further stages of technology? I'm wondering what the state of your work was 17 years ago, when you started doing this privacy stuff. Is it really ultimately technology's role to solve the problems that we're discussing right now?

It's a bit complicated, but first of all, tell me about how the business of litigation with regard to PIPEDA was 17 years ago. Has it changed much? Is there something further down the road that you would anticipate technology to solve some of the problems we're talking about?

Mr. Alex Cameron: There was virtually no litigation activity 17 years ago in relation to privacy. In my practice, and I'm sure in that of the other witnesses who were around at that point, the focus was on compliance. You have a new statute coming in with a new set of rules. How do we write a privacy policy? How do we develop policies and procedures, consent documents, etc.? It was very compliance oriented.

There has been a tremendous evolution since that time in what I would call a mature and maturing privacy profession. There are organizations like the International Association of Privacy Professionals. Don't quote me on the number, but I think they have somewhere in the range of 20,000 members worldwide. A great deal of maturity has evolved over these years, so certainly the work and the issues have become more focused on specific types of projects and specific types of proposed activities, which are often emerging in a new technological or innovative context. We are trying to apply those facts to the law that we have.

The point I'm trying to emphasize is that I think PIPEDA has proven very adaptable to those evolving technological contexts to this point.

Mr. Bob Bratina: Right.

Mr. Alex Cameron: I'm not saying there may not be room for tweaks here and there, or improvements such as those that have been made, but largely the model we have has worked quite well.

Mr. Bob Bratina: You've answered my question.

Thank you very much.

The Vice-Chair (Mr. Daniel Blaikie): Thank you, Mr. Cameron.

Thank you very much, witnesses, for your patience at the beginning of the meeting and at the end as well.

I'm afraid that we rather unceremoniously have to run from the meeting, but we thank you for your understanding.

We are adjourned.