HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 049 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, February 23, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Thursday, February 23, 2017

● (1530)

[*English*]

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

I know that many of us are anxious, as this is the last week of four before we go home for a constituency break week, but we have with us some very distinguished panellists to help us in the deliberations on our current study, which is on the Personal Information Protection and Electronic Documents Act, more affectionately known by Canadians on a daily basis as PIPEDA.

From the Centre for Law and Democracy, we are joined once again by Mr. Michael Karanicolas, a senior legal officer, by video conference.

It's good to see you again, Mr. Karanicolas.

As an individual, we again have joining us Teresa Scassa, a full professor at the University of Ottawa.

Thanks, Teresa, for joining us again. It's always a pleasure to have you here.

For the first time ever appearing before the committee, in his debut game—I mean, debut "appearance"—we have Florian Martin-Bariteau, assistant professor with the common law section of the Faculty of Law and the director of the Centre for Law, Technology and Society at the University of Ottawa.

As we normally do in this committee, we'll have a 10-minute opening statement from each of you. We'll simply go in the order in which I introduced you. I think everybody here is familiar with how this happens.

We'll start with you, Mr. Karanicolas. You have up to 10 minutes, please.

Mr. Michael Karanicolas (Senior Legal Officer, Centre for Law and Democracy): Thanks to the committee for your invitation to appear again.

I'd like to start by offering my congratulations to the standing committee for their recommendations to reform the Privacy Act, which were published late last year and which I thought were excellent.

It is, I believe, fairly clear that the current consent-based model of privacy protection is broken. The core dynamic that underlies this model and that drives much of the digital economy is that users may choose to trade their personal information for services. There are undeniable benefits to this model, which has assisted in the rapid spread of the Internet by lowering costs of entry. However, this dynamic relies on meaningful consent, which in turn requires at least a nominal understanding by the contracting party of what they're signing on to. In fact, virtually nobody reads their terms of service agreements, a state of affairs that significantly undermines the legitimacy of the consent obtained.

The OPC report points in part to the length of these agreements and the frequency with which they're presented to users as a cause of this lack of understanding, but it's also worth noting that these agreements are often drafted in a highly convoluted, confusing, and even self-contradictory manner that even technically and legally trained people struggle to understand. There's a vicious cycle at work. The fact that very few users read these agreements or use their substance as a basis for accepting or declining a service gives companies licence, and indeed an incentive, to draft them incredibly broadly. This drafting style and the lack of accessibility further depresses engagement with the agreements by their signatories and so on.

It's also worth noting that the company that presents the agreement and offers a service may often be distinct from the ones that actually collect and process the information. Third party data brokers play an increasingly common role in the Internet's ecosystem. A 2014 study showed that of the 950,000 most popular websites, 88% of them automatically shared visitor information with third parties, an average of 9.5 different third parties per website. The vast majority of this tracking is carried out surreptitiously, with only 2% of third parties including a visible prompt alerting users to their presence.

There's a clear problem here. However, it's important to try to look for solutions that will not derail the current digital economy. Although there are pros and cons to a system where personal information is used as a major currency by which online services are procured, potential avenues forward should be crafted with an eye to maintaining the tremendous benefits that Internet access provides.

One solution, which we strongly support, is to boost the quality of consent by improving the information available to users. A better practice here may include publishing a summary or explanatory guide of the terms of service alongside the full legal version, ensuring that the agreement is easily available for review, and clearly notifying users when a substantial change to the change of service has been made.

The OPC has an important role to play here: to promote better practice in terms of clarity and accessibility of terms of service agreements, and to audit existing agreements for their clarity and accessibility, as well as their accuracy against how information is actually collected and processed. In addition to these steps, the proposal to shift to opt-in consent as a default to the required approach is one that we support.

The move to expand transparency is another important factor to boosting the quality of consent, allowing people to look under the hood of the services and platforms they use. This may include, for example, a right to request an explanation of how their personal information has been used to customize their online experience, or what factors went into a particular decision by the company that they were subject to. However, while there is substantial room by which the quality of user engagement and of consent may be improved, these improvements alone are not sufficient to safeguard the privacy rights of Canadians. The CLD supports the creation of clearly defined no-go zones, as well as proceed-with-caution zones, as mentioned in the OPC report. One important area to consider here is the need for greater clarity on how information can be transferred out to third parties or resold, and what rules should govern these external uses. Broader investigative powers by the OPC are also needed to promote good practice in terms of information management and security.

In terms of the de-identification or anonymization of information, while I think it should certainly be encouraged, it is not a panacea for the current privacy concerns. I would add to the commentary contained in the OPC's report by noting that as anonymization gets stronger, the commercial value of information can often decline, giving businesses an incentive to pursue incomplete solutions. Moreover, the fact that information has been, quote-unquote, anonymized may create a false sense of security, prompting companies to be less vigilant in safeguarding it and consumers to assume that threats to privacy have been nullified.

I also want to speak briefly about reputation and privacy and the right to be forgotten.

● (1535)

The Internet's transformative impact on our social functions has made a person's online footprint a vital aspect of his or her identity. However, the permanence and increased accessibility of online information has led to concerns from some about the Internet's impact on privacy and reputation.

There are benefits to making people's pasts more accessible. A Holocaust museum, for example, has a legitimate interest in knowing if a person it is considering for a job has a history of making racist comments. However, we are also a society that believes in giving people second chances. There can be problems with how the digital records present themselves, such as where a decision by a prosecutor to drop charges may not generate as much coverage as the initial arrest, or where an erroneous and sensational media report may attract more attention than a later retraction.

However, experiences in Europe with the right to be forgotten should be viewed as a cautionary tale about what not to do. Namely, any move to develop a right to be forgotten should be grounded in clear and limited definitions of how it applies, strong transparency, and robust due process. I will address each of these in turn.

First, the application of a right to be forgotten requires a careful balancing of freedom of expression, privacy, and the right to information. Any such balancing will have to be based on a clear test to determine where the public interest lies. People have never had a right to control or curate their reputations. Any move to create a right to be forgotten should be aimed only at the novel aspects of reputation that have come about as a result of the Internet and should be reserved for significant and demonstrably unfair circumstances, such as when a person has been wrongly arrested.

Second, transparency is a key ingredient, including making available detailed information about how decision-making processes work and how they have been applied. There should be as much information as can be provided, short of undermining the efficacy of the processes themselves.

Third, as with any restriction on freedom of expression, due process is critically important. Search engines are simply not equipped to engage in this careful balancing of rights, and unfortunately have an incentive under the current European system to err on the side of removing the information without providing the careful due process such a tricky issue should warrant. Any order to remove material or to reduce its accessibility should be left in the hands of a court or a quasi-judicial authority, including careful due process considerations.

I want to emphasize that none of the above should be interpreted as an endorsement of the right to be forgotten. Indeed, there is a strong argument to be made that the present reputational challenges will sort themselves out over time, as people will gradually become inured to the preponderance of embarrassing or unpleasant information out there and will learn to take such information with a pinch of salt. However, insofar as the right to be forgotten is being considered, it is important that we not repeat the widely criticized mistakes of the Court of Justice of the European Union in how it handled the matter.

I look forward to your questions in the discussion.

● (1540)

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

We now go to Ms. Scassa, please, for up to 10 minutes.

Prof. Teresa Scassa (Full Professor, University of Ottawa, Canada Research Chair in Information Law, As an Individual): Thank you for the invitation to meet with you today and to contribute to your discussion on PIPEDA. I'm a professor at the University of Ottawa in the Faculty of Law, where I hold the Canada research chair in information law. I'm appearing in my personal capacity.

We're facing what might be considered a crisis of legitimacy when it comes to personal data protection in Canada. Every day we hear new stories in the news about data hacks and breaches, and about the surreptitious collection of personal information by the devices in our homes and on our persons that are linked to the Internet of things. There are stories about how big data profiling impacts the ability of individuals to get health insurance, obtain credit, or find employment. There are also concerns about the extent to which state authorities access our personal information that is in the hands of private sector companies. PIPEDA, as it currently stands, is inadequate to meet these challenges.

My comments are organized around the theme of transparency. Transparency is fundamentally important to data protection and has always played an important role under PIPEDA. At a basic level, transparency means openness and accessibility. In the data protection context, it means requiring organizations to be transparent about the collection, use, and disclosure of personal information, and it means that the commissioner also must be transparent in his oversight functions under the act.

I'm going to also argue that it means that state actors, including law enforcement and national security organizations, must be more transparent about their access to and use of the vast stores of personal information in the hands of private sector organizations.

Under PIPEDA, transparency is at the heart of the consent-based data protection scheme. It's central to the requirement for companies to make their privacy policies available to consumers and to obtain consumer consent to the collection, use, or disclosure of personal information, yet this type of transparency has come under significant pressure and has been substantially undermined by technological change on the one hand, and by piecemeal legislative amendment on the other.

The volume of information that's collected through our digital, mobile, and online interactions is enormous, and its actual and potential uses are limitless. The Internet of things means that more and more of the devices that we have on our person and in our homes are collecting and transmitting information. They may even do so without our awareness, and they often do so on a continuous basis. The result is that there are fewer clear and well-defined points or moments at which data collection takes place, making it difficult to say that notice was provided and that consent was obtained in any meaningful way.

In addition, the number of daily interactions and activities that involve data collection have multiplied beyond the point at which we are capable of reading and assessing each individual privacy policy. Even if we did have the time, privacy policies, as was just mentioned, are often so long, complex, and vague that reading them does not provide much of an idea of what's being collected and shared, with or by whom, or for what purposes.

In this context, consent has become a bit of a joke, although unfortunately the joke is largely on consumers. The only parties capable of saying that our current consent-based model still works are those that benefit from consumer resignation in the face of this ubiquitous data harvesting.

The Privacy Commissioner's recent consultation process on consent identifies a number of possible strategies to address the failures of the current system. There is no quick or easy fix, no slight changing of wording that will address the problems around consent. This means that on the one hand there need to be major changes in how organizations achieve meaningful transparency about their data collection, use, and disclosure practices, and there must also be a new approach to compliance that gives considerably more oversight and enforcement powers to the commissioner. The two changes are inextricably linked.

The broader public protection mandate of the commissioner requires that he have necessary powers to take action in the public interest. The technological context in which we now find ourselves is so profoundly different from what it was when this legislation was enacted in 2001 that to talk of only minor adjustments to the legislation ignores the transformative impacts of big data and the Internet of things.

A major reworking of PIPEDA may be well overdue, in any event, and it might have important benefits that go beyond addressing the problems of consent. I note that if one were asked to draft a statute as a performance art piece that evokes the problem with incomprehensible, convoluted, and contorted privacy policies and their effective lack of transparency, then PIPEDA would be that statute. As unpopular as it might seem to suggest that it's time to redraft the legislation so that it no longer reads like the worst of all privacy policies, this is one thing this committee should consider.

I make this recommendation in a context in which all of those who collect, use, or disclose personal information in the course of commercial activity, including a vast number of small and medium-sized businesses with limited access to experienced legal counsel, are expected to comply with the legislation. In addition, the public ideally should have a fighting chance of reading the statute and understanding what it means in terms of the protection of their personal information and their rights of recourse. As it's currently drafted, PIPEDA is a convoluted mishmash in which the normative principles are not found in the law itself, but rather are tacked on in a schedule.

● (1545)

To make matters worse, the meaning of some of the words in the schedule, as well as the principles contained therein, are modified by the statute, so that it's not possible to fully understand rules and exceptions without engaging in a complex connect-the-dots exercise. After a series of piecemeal amendments, PIPEDA now consists in large part of a growing list of exceptions to the rules around collection, use, or disclosure with consent. While the OPC has worked hard to make the legal principles in PIPEDA accessible to businesses and to individuals, the law itself is not accessible.

In a recent PIPEDA application involving an unrepresented applicant—and most of them who appear before the Federal Court are unrepresented, which I think is another issue with PIPEDA—Justice Roy of the Federal Court expressed the opinion that for a party to "misunderstand the scope of the Act is hardly surprising".

I've already mentioned the piecemeal amendments to PIPEDA over the years, as well as concerns about transparency. In this respect, it's important to note that the statute has been amended so as to increase the number of exceptions to consent that would otherwise be required for the collection, use, or disclosure of personal information.

For example, paragraphs 7(3)(d.1) and (d.2) were added in 2015. They permit organizations to share personal information between themselves for the purposes of investigating breaches of an agreement or actual or anticipated contraventions of the laws of Canada or a province, or to detect or suppress fraud. While these are important objectives, I note that no transparency requirements were created in relation to these rather significant powers to share personal information without knowledge or consent. In particular, there's no requirement to notify the commissioner of such sharing. The scope of these exceptions creates a significant transparency gap that undermines personal information protection. This should be fixed.

PIPEDA also contains exceptions that allow organizations to share personal information with government actors for law enforcement or national security purposes without the notice or consent of the individual. These exceptions also lack transparency safeguards. Given the huge volume of highly detailed personal information, including location information, which is now collected by private sector organizations, the lack of mandatory transparency requirements is a glaring privacy problem.

The Department of Innovation, Science and Economic Development has created a set of voluntary transparency guidelines for organizations that choose to disclose the number of requests they receive and how they deal with them. It's time for there to be mandatory transparency obligations around such disclosures, whether it be public reporting or reporting to the commissioner, or a combination of both. Also, that reporting should be by both private and public sector actors.

Another major change that is needed to enable PIPEDA to meet the contemporary data protection challenges relates to the powers of the commissioner. When PIPEDA was enacted in 2001, it represented a fundamental change in how companies were to go about collecting, using, and disclosing personal information. This major change was made with great delicacy. PIPEDA reflects an "ombuds" model that allows for a light touch with an emphasis on facilitating and cajoling compliance, rather than imposing and enforcing it. Sixteen years later, and with exabytes of personal data under the proverbial bridge, it's past time for the commissioner to be given a set of new tools to ensure an adequate level of protection for personal information in Canada.

First, the commissioner should have the authority to impose fines on organizations in circumstances where there has been substantial or systemic non-compliance with privacy obligations. Properly calibrated, such fines can have an important deterrent effect that is currently absent from PIPEDA. They also represent transparent moments of accountability that are important in maintaining public confidence in the data protection regime.

The tool box should also include the power for the commissioner to issue binding orders. I'm sure you're well aware that the commissioners in Quebec, Alberta, and British Columbia already have such powers. As it stands, the only route under PIPEDA to a binding order runs through the Federal Court, and then only after a complaint has passed through the commissioner's internal process. This is an overly long and complex route to an enforceable order, and it requires an investment of time and resources that places an unfair burden on individual complainants.

I note as well that PIPEDA currently does not provide any guidance as to damage awards. The Federal Court has been extremely conservative in damage awards for breaches of PIPEDA, and the amounts awarded are unlikely to have any deterrent effect other than to deter individuals who struggle to defend their personal privacy. Some attention should be paid to establishing parameters for non-pecuniary damages under PIPEDA. At the very least, these will assist unrepresented litigants in understanding the limits of any recourse that's available to them.

Thank you. I welcome any questions.

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

We now go to Mr. Martin-Bariteau, please, for up to 10 minutes.

Prof. Florian Martin-Bariteau (Assistant Professor, Common Law Section, Faculty of Law, and Director, Centre for Law, Technology and Society, University of Ottawa, As an Individual): Thank you, Mr. Chair.

● (1550)

[*Translation*]

I would like to thank you for this opportunity to contribute to your work on the review of the Personal Information Protection and Electronic Documents Act (PIPEDA) and thus offer me the chance to share my thoughts with you about an issue of importance to Canadians.

I am an Assistant Professor of Law and Technology at the Common Law Section, Faculty of Law of the University of Ottawa, where I teach Digital Economy Law, and am the Director of the Centre for Law, Technology and Society. Nonetheless, I appear before you today in my personal capacity.

My comments will be built upon the letter sent to you by the Commissioner last December 2. I will focus on the issues of enforcement powers and reputation. I will then move to the scope of the act, before concluding with some reflections as to its accessibility and readability.

Throughout my presentation, I will draw references to new European Union's General Data Protection Regulation, GDPR, particularly due to the adequacy issues raised by the Commissioner.

As to the enforcement powers, I believe it is essential to strengthen the Commissioner's powers in order to ensure the effectiveness of the act, in particular by granting the Commissioner order-making powers and the authority to impose administrative monetary penalties. The ability to impose fines appears to be the most effective way to ensure protection.

As with everything, the protection of personal information is subject to a cost-benefit analysis. It is now a matter of either investing in a protection by design or choosing the possibility of a slap on the wrist. With the risk of monetary penalties, the cost-benefit analysis will favour a protection by design approach. Obviously, the amount of the fine will be a critical parameter for its effectiveness—a prohibitive amount is required. For example, if a $500,000 fine may seem significant—and it will be for small and medium-sized businesses—it will be an insignificant amount for companies like Amazon, Facebook or Google. In that respect, it was by imposing a $22.5-million fine that the U.S. Federal Trade Commission succeeded in getting Google to modify its DoubleClick advertising program.

In order to prove effective against big players, we need the maximum fine to be specified based on a percentage of worldwide turnover—for example, 1%. To ensure that the fine is not ludicrous for small and medium-sized enterprises, a second limit should be provided—for example, $500,000; with the greater limit to be retained. Incidentally, the GDPR is based on such a mixed approach.

In my view, this does not threaten the collaborative relationship between operators and the Commissioner. On the contrary, I am of the opinion that strengthened powers will encourage a greater co-operation within actors, before any damage. Besides, such powers seem necessary to obtain an adequate decision of the GDPR.

In order to avoid the appearance of conflicts of interest, fines should be made payable to the Receiver General. So as to protect small businesses and not slow down innovation, we could provide a procedure for a preliminary conformity assessment. In the event of damages, sanctions would only be imposed after an issued recommendation has not been acted upon within a reasonable time.

Finally, I am of the view that none of the Commissioner's powers, including those of order and sanction, should be limited to the receipt of a formal complaint—the totality of these powers evidently remaining subject to possible judicial review.

As to the rights of individuals and online reputation, many favour the creation of a “right to be forgotten”. In the way it is imagined and requested by some, I find this proposition dangerous. The Internet is the archives and the libraries of tomorrow, the new collective memory. Archives have never previously been erased because they were disturbing—at least, not legally in a democracy. This is dangerous ground, and similarly, it is dangerous to want to delegate censorship powers to private actors or to give the power to decide what should be accessible or not to a select few. In the same vein, the right to de-index seems illogical to me, in that it would entail the removal of the index entry, but not the content itself.

Legislation protecting personal information should not be used as a reputation management tool to remove what is embarrassing, but only to remove anything that is unjustified or inaccurate. Otherwise, I am not sure that such a mechanism would satisfy the charter test.

The actual problem with Canadian law is that PIPEDA recommends, but does not require, the erasure of inaccurate or unnecessary data. Certainly, in its recent and already famous Globe24h decision, the Federal Court circumvented this deficiency through the illegitimate and unauthorized nature of the disclosure.

Nevertheless, the erasure of data should be compulsory—and not simply recommended—once it is no longer necessary or accurate through stricter controls of the retention of data over time. One could also provide for an actionable right of erasure of outdated and inaccurate information. I should point out that this need does not only relate to the Internet, but to all databases, computerized or not.

It seems to me that these amendments are necessary—but sufficient—to the GDPR adequacy.

As to the scope, Canadians should be ensured that any harmful collection, use or disclosure of data be subject to strict standards of protection.

The definition of the scopes of the two federal statutes does not meet the citizens' expectation of protection in a global and interconnected world, including protected data and in particular with respect to the subjected organizations.

A solution for organizations would be to redefine the scope of PIPEDA in such a way that would render it applicable to all organizations operating under federal jurisdiction and that are not covered by the public sector act or any other federal law. Evidently, and analogously to our partners, the law shall retain exemptions for personal or journalistic use.

As to the issue of access to law, if it is undeniable that the law requires modifications in view of new realities, the legislator must seize the opportunity of this reform by performing a complete overhaul of the law, instead of making simple amendments.

Indeed, PIPEDA belongs, undoubtedly, in the hall of fame for the worst drafted federal laws—and we know that there is, in that matter, some competition there. The cornerstone of PIPEDA lies in an appendix copy-and-pasted from a document drafted by a private standardization organization. The act only supplements this document and other appendices by making constant references to them.

This poses a problem in terms of the public's access to law. A rewrite of the law, clearly explaining the right and obligations of each, would therefore be welcome—especially to make mandatory all that is presently recommended.

In terms of drafting, the act should remain conceived according to the principle of technological independence and be principles-based. Such an approach is essential to enable the Canadian legal framework to adapt to future social and technological changes, including the development of robotics, of the Internet of objects and artificial intelligence.

In terms of readability, the limitation of the legislation to the protection of personal information would be welcomed. Functional equivalence rules for electronic documents are irrelevant and should be transferred elsewhere.

Conversely, it would be desirable for a single act to contain the entire framework for the protection of personal information, that is, for both the private and public sectors. The concomitant reconsideration of these two acts by this committee offers this opportunity. This would also allow for the creation of a coherent framework for both the protection of personal information and the role of the Commissioner—even if it means providing several sections if it was considered necessary to maintain a public sector exemption regime.

As a final thought, I would like to draw your attention to the need of providing statutory rights of actions and damages. Equally, I would like to underline that it is necessary to update our law in order to satisfy the GDPR's suitability test, but that we must nevertheless consider two important factors: first, that the test does not require a carbon copy of the GDPR and secondly that this applies to all protection frameworks, and not just PIPEDA.

I hope that these few thoughts and recommendations will be useful to the committee. Sadly, I wasn't able to finalize on time a short bilingual brief with examples and recommendations. However, I could send it to you afterwards.

Thank you. I'll be happy to answer any questions that you may have.

● (1555)

[*English*]

The Chair: Thank you very much.

Colleagues, we'll now proceed to the seven-minute round.

Our opening time allotment goes to Mr. Bratina, please.

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

Thank you to all.

Ms. Scassa, I loved your phrasing that it was a “convoluted mishmash”, a “piecemeal” document. Is it because of the dynamic nature of law-making, where the technology has been evolving and they've been adding things on that makes the whole thing unworkable, in the end?

Prof. Teresa Scassa: I think it's really due to the legislative history of the statute. It arose at a time when there was a need to put legislation in place quickly. Europe had just passed its first data protection directive, and there were concerns about cross-border flows of data. We're in a similar situation again.

It was clear that we needed legislation. There wasn't a lot of comfort with legislation. It was decided that if it were built around the CSA model code, there would be a greater acceptance of it, both here and south of the border, in terms of the obligations it imposed on businesses.

The normative core is the CSA model code, which is in the schedule. In the legislation itself, all the exceptions and modifications are found, as are the enforcement powers and so on. For an ordinary individual who is trying to work his or her way through the statute, it's not intuitive. It's not easy to find. As amendments get made, the interaction between the two documents becomes even more complicated.

I think it's in large part due to that history that we have the legislation we have. I think we're mature enough now in our evolution in terms of our data protection that we can walk away from that and fix the statute.

● (1600)

Mr. Bob Bratina: We've heard in testimony about the European Union's general data protection regulation. Relatively, PIPEDA falls short on the right to be forgotten. I'm going to ask Mr. Karanicolas about this, because he made a comment, but I'll ask you first.

Did you review the European Union's general data protection regulation, and how do you feel about that compared to what we have?

Ms. Scassa, I'll ask you first.

Prof. Teresa Scassa: On the right to be forgotten, I would draw a distinction between the right to be forgotten, which is talked about a great deal in the context of a particular court decision in the European Union, and the right to erasure, which I think is more what is present in the data protection directive. I think those are very different things.

The right to be forgotten, in a sense, goes so far as to talk about what search engines have to delist, so it affects how you search and how you find information on the Internet. That is very different from the right of people who no longer want a company they perhaps dealt with in the past and which collected their personal information to have their personal information, because they no longer wish to deal with that company. They're asking to have that personal information removed and no longer dealt with.

The right to be forgotten and the right to erasure are very different things. The right to erasure seems to me to fall within the scope of PIPEDA, whereas the right to be forgotten goes beyond it, and I think, as my colleague pointed out, it implicates freedom of expression rights.

Mr. Bob Bratina: Mr. Karanicolas, is it possible to track how data moves around? I made this comment another day about the offshore havens of money. Can there be offshore havens of data, where things can be slipped over to other servers and hidden away and used at the pleasure of those people? With the current technology, can you follow that data as it travels around?

Mr. Michael Karanicolas: If I understand you correctly, it's possible to impose data localization rules. Different governments have experimented in different ways with those kinds of requirements.

That's not necessarily something I would recommend for Canada, but it is possible to control how information is routed. Those kinds of controls tend to raise significant concerns about the functionality and operability of the Internet as a whole, which is designed to allow information to flow by the most efficient route.

I'm not sure if I'm answering your question, or if you're—

Mr. Bob Bratina: To me, as technology evolves so rapidly, we're trying to set in stone wording for legislation that may miss the next feature of technology, which would allow it to side-swipe that, if you will.

Mr. Michael Karanicolas: Okay.

Technological neutrality is an admirable goal to aim for. I think what the drafters of PIPEDA were originally aiming for was to try to keep it as neutral as possible, as far as I understand it. Whether they succeeded is different. I think there have been some fair points brought up by my colleagues, particularly about how the Internet of things has so dramatically changed the way information is being collected. It has opened up all these new avenues that are vastly beyond what was conceived at the time PIPEDA was drafted.

As a general rule, I think that technological neutrality in legislation is a good thing to aim for. In crafting a new law or in revising a law, one should aim to avoid falling into that kind of pitfall as far as possible.

Mr. Bob Bratina: Can I ask you about the comments you made with regard to the European Union's right to be forgotten, etc.? You didn't seem to be too supportive of its approach. We've heard the opposite testimony.

Mr. Michael Karanicolas: The right to be forgotten is not something I strongly oppose. I'm sort of undecided on that issue specifically. I see arguments either way as to whether some sort of right is potentially a good idea, because I do see a problem and I do see a change in the way information is recorded, which the Internet has wrought.

That being said, there are huge problems with the way it's been rolled out in Europe, partly because the decision, when the European Court of Justice first handed it down, didn't provide a huge amount of clarity on how it should be applied. It provided vastly broad categories for what could be susceptible to the right to be forgotten, which led to a huge amount of confusion. I think the last I saw, something like 150,000 or 170,000 websites had been taken down as a result of that. Huge numbers of applications have been made.

I see problems with the way it has been rolled out in terms of a lack of clarity. I also question the wisdom of bundling it with the search engines themselves. As private sector actors, they're not well equipped to engage in that kind of balancing. When you impose this kind of potential for liability on them, without their necessarily having the proper processes in place to respect the freedom of expression interests that are engaged, what you end up with is a tendency to remove information whenever there's a complaint. That's a problematic approach.

● (1605)

The Chair: Thank you very much.

We now move to Mr. Jeneroux, please, for seven minutes.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thanks to all three of you, two of you for coming back, and to you, Mr. Martin-Bariteau, in your first time here, welcome.

My first question was going to be about what all of you think of PIPEDA, but it's pretty clear. Nobody here in the room is too pleased with it, so I'll move on to my second question.

In terms of order-making powers, Ms. Scassa, you made your thoughts clear in the last answer, but could we get the other two gentlemen on the record in terms of their thoughts on providing the Privacy Commissioner order-making powers?

You're first, Mr. Martin-Bariteau.

Prof. Florian Martin-Bariteau: I'm not sure I understand....

[*Translation*]

Like my colleague Teresa Scassa, I am fully in favour of the idea of granting the Commissioner order-making powers.

[*English*]

Mr. Matt Jeneroux: Mr. Karanicolas.

Mr. Michael Karanicolas: I'm not entirely convinced of the need for order-making powers. It's not something that I necessarily oppose, but I do think it raises some issues in terms of the procedural fairness of investigations, which the OPC itself has mentioned.

To me, the bottom line is necessity. I think the reason I'm not completely sold on the order-making power is that we've previously heard from the Privacy Commissioner that most of their recommendations are ultimately complied with. If that's the case, and if you have a system in which the recommendations are already being complied with, I'm not sure why you need a strengthening of the powers.

It was mentioned that recommendations are often very slow in being implemented, which is a significant problem. Some people have suggested a hybrid model, whereby the companies would need to apply to the court for permission to not comply within a particular time period. I'm not sure why a specific order-making power would solve the problem more than a hybrid model, which is I think why I'm not necessarily opposed to it but not fully convinced of the need for an order-making power either.

Mr. Matt Jeneroux: We're going to try to pin you down on some answers here, Mr. Karanicolas. I'll skip to the right to be forgotten, where it sounds like you're equally on the fence. It sounds like the Privacy Commissioner is also struggling with the same focus as to what type of law he should put in place, if any. I find it personally fascinating. I think that somebody's right to be forgotten is somebody else's argument that, no, they should be remembered.

You gave a bit of an on-the-fence argument. I'll start with you and go around the table to see if there's any guidance or support you can provide us. The Privacy Commissioner is coming out with a position paper on this, but unfortunately not until after our study is done. We're looking for some advice or support in terms of our recommendations to the Privacy Commissioner.

Mr. Michael Karanicolas: At the moment, I wouldn't make a recommendation in favour of the right to be forgotten.

The reason I'm a bit couched in that is that I do see some potential problems that could be addressed, but if you want a recommendation on whether or not to legislate that, I would be against it. I think there's a huge amount of potential to do harm, and a huge amount of potential to craft it in a way that has the negative impact on freedom of expression.

I do see the problem there, but there are a lot of ways that the legislation could be done badly, which is why I would be concerned.

● (1610)

Mr. Matt Jeneroux: That's a little better.

Ms. Scassa.

Prof. Teresa Scassa: I'll make clearer the distinction I'm making between the right to be forgotten and data erasure.

Let's say you've joined a social networking site, and you've created a profile, you have photographs, and you have information on your profile, or let's say it's a dating site and you've created a profile for that. You have that up for a couple of years and you decide you no longer want to be part of that site. You don't want to do business with it—this happens all the time—and you say to the company, "Remove my account and get rid of my personal information, because I'm done." That's the right to erasure. That's different from the right to be forgotten.

You're not saying that there are newspaper stories about you out there that you don't want anyone reading anymore and you want them de-indexed. You're saying that you've had this relationship with a private sector company that you're terminating and you want the data that you have provided as part of that relationship to be removed. In many circumstances that has been very difficult for people to achieve. That's the right to erasure.

I think that's very important. If we can strengthen the right for people to be able to take those kinds of measures with the private sector organizations that have been collecting and using their personal information, I think that's important.

The other aspect of the right to be forgotten, I have substantial misgivings about.

Mr. Matt Jeneroux: Fair enough.

If I could jump in here, and I hope to bring Mr. Martin-Bariteau into this as well, let's say a 16-year-old posts something on a Facebook account. Fast-forward 20 years and they decide to, I don't know, do an honourable profession and run to be a member of Parliament perhaps. Even though they've entered into that contract, what's not to say that somebody hasn't gone and screen-captured that particular story, with a news story perhaps written about it? I guess that's where I'm struggling with the right to be forgotten piece. It's not necessarily the contract you've entered into with that organization, it's the fallout, the public fallout, I guess, after that.

I used the example of a member of Parliament only because I know that there are people around the room here who would agree with me that it's prevalent.

Prof. Teresa Scassa: I think that's a serious issue as well. I'm not sure it's a PIPEDA issue. In some circumstances, issues like that have been dealt with through the tort system. Where it's been done maliciously, they've been dealt with through other mechanisms, because I think they raise issues that go beyond simply data protection.

While I agree that it's an important issue, I'm not entirely convinced it's as much a PIPEDA issue as it is a problem that maybe requires multiple different solutions, depending on the circumstances. I mean, revenge porn falls into that category. That's clearly a tort and also perhaps criminal activity and so on.

Mr. Matt Jeneroux: I think I'm out of time.

The Chair: You certainly are, buddy.

Voices: Oh, oh!

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

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Thank you very much.

Mr. Karanicolas, I want to start with a couple of questions about the right to be forgotten. You mentioned that the rollout of that in Europe has not gone very well. I was just wondering if, for the benefit of our record and testimony, you could provide a couple of the best examples of what didn't go well, what didn't work, in the European context.

Mr. Michael Karanicolas: I'll start by endorsing the distinction that Professor Scassa made between data protection and a right to deletion and a right to be forgotten, because that is a key distinction.

The way it was handed down was the first problem we saw. There was a decision by the European Court of Justice that didn't even really mention freedom of expression, and included statements that, for example, the right to privacy generally trumps people's right to obtain information. There was a lack of proper consideration of the rights that were being infringed. That would be the first one. With that decision, which was relatively bare, providing the only guidance at the outset at least that Google was going to have in implementing that, it was hugely problematic, because you create this enormous new responsibility without a huge amount of guidance on how it's supposed to be implemented.

As I mentioned briefly before, putting this on the private sector is hugely problematic, because this is a very tricky decision. It involves balancing different rights against one another, and it involves considering the overall public interest. Google is absolutely not equipped to do that. Even for a company of their size, this is something that you need judicial or quasi-judicial decision-makers to take on. Saddling it onto the private sector was also a significant mistake. I think you saw that the floodgates sort of came open. I looked it up in the interim, and I saw 348,000 requests to remove links by Google.

When I say that I have a certain amount of sympathy with regard to a few limited cases of where the right to be forgotten could be applied, I think it's a challenging thing to implement in terms of just applying it to those extreme cases. I think the European example shows that once the right is implemented, the floodgates kind of come open, and you have a huge amount of legitimate or accurate information, or perfectly relevant information, that people would request deletion for.

● (1615)

Mr. Daniel Blaikie: This comes from a decision of the European Court of Justice. Without a great background on this subject, is there anything in the general data protection regulation about the right to forget?

Mr. Michael Karanicolas: My understanding of the way in which it's applied is based on the initial rollout of the ECJ decision. I believe the data protection regulation does address that, but I haven't reviewed that specific aspect.

Mr. Daniel Blaikie: For me, the next question, and perhaps some of our other witnesses have an idea on this, is that when we talk about worrying about whether our privacy laws are adequate under the European test so as not to disrupt the commercial data flows, is having some aspect of a right to forget a necessary component of meeting the adequacy test for Europe?

[*Translation*]

Prof. Florian Martin-Bariteau: No. Absolutely not.

Even in the new GDPR, which addresses the issue of the right to be forgotten, it is in quotation marks. In that context, it is called "the right to erasure". The Regulation makes the distinction that Professor Scassa mentioned. In fact, the right to erasure provided for in the GDPR is somewhat in line with the one already in the 1995 directive, which was in force in most European Union countries.

It is possible to request that data be deleted, but only for the data whose collection, communication or disclosure violates the Regulation. However, the Regulation sets out exceptions for freedom of expression, freedom of the press, the right to information and so on.

Mr. Daniel Blaikie: The right to erasure already exists in Canada. I wonder whether it fits in with the European model or whether the option should be there.

Prof. Florian Martin-Bariteau: Like Professor Scassa, I think PIPEDA should clearly provide for the right to erase inaccurate and erroneous data so that it is not just a recommendation.

I would also like to point out that the second paragraph of article 45, which talks about adequacy, does not mean just doing a cut-and-paste; it means considering effective and enforceable rights. Direct rights would therefore be appropriate. In terms of data protection, it does not directly relate to any right to erasure, but indicates that the country's rules on human rights and fundamental freedoms will be taken into account. In this case, we are talking about the Canadian Charter of Rights and Freedoms.

[*English*]

Mr. Daniel Blaikie: Thank you.

On the issue of consent, I'm just looking for some practical advice. I think it's pretty clear that the current consent model really doesn't work very well. Anyone who has signed up for software over the Internet and been confronted with user agreements has a pretty good sense that these are opaque and long and technical. Even when you do start to read them, they tend to be overly broad and you feel like you're signing up for just about anything when you click "I agree".

How do you have a model that isn't overly prescriptive but nevertheless offers something that ordinary Canadians who don't have a background in that particular kind of law can digest so they can feel comfortable that they know what they're signing on to? Do you have template agreements, or is that overly prescriptive and you would then have agreements that wouldn't fit the kinds of services being offered? How do you write something into law that actually accomplishes a viable consent model?

● (1620)

Prof. Teresa Scassa: That's a very good question.

It's challenging. I think there are small fixes in terms of tools, direction, and guidance in drafting better privacy policies and more condensed or short-form privacy policy templates, as you suggest.

In terms of ubiquitous and continuous collection, people have suggested that there should be pop-ups from time to time to remind people that their information is being collected by the toaster, for example, and that they might want to think about whether they still want that to be happening. There are those types of things. Some of those could be mandated in legislation. Some could be done through guidance from the Privacy Commissioner.

There are others who suggest, as you know, broader fixes, such as moving all sorts of data collection and considering it fairly routine, and consent wouldn't be required. What worries me about that, of course, is the threshold that there be no risk or no harm. I think that in the big data environment, we're still trying to figure out exactly what the risks and the harms are. It's not always obvious at the outset what the implications of the collection of certain types of data are going to be, depending on what is then subsequently collected by someone else and put together.

I think there are some very serious challenges there, and I wish I could say, "Here are the three things that need to be done", but I'm still struggling with it myself.

The Chair: We are out of time for Mr. Blaikie's allotted time, but I know that if there are others who want to get in on this, there will be an opportunity, I'm sure.

We'll now move to Mr. Saini, for the last of our seven-minute rounds.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you very much.

I want to start off with one point. Canada, having recently signed CETA, is going to be under some pressure to rise to the level of the GDPR, general data protection regulation, that will come into effect in May 2018 in Europe. There are stark differences between what we currently have and what has been indicated in the GDPR. One is data erasure and privacy by design and by default.

Could you give a broad outline to the committee as to what significant or important areas we should focus on? I guess ultimately we'll have to rise to that level to do business with Europe. Are there any key indicators you feel we should focus on?

Prof. Teresa Scassa: Maybe I'll pass the floor to our resident European.

Voices: Oh, oh!

Mr. Raj Saini: I have a lot of questions. I can ask another question.

[*Translation*]

Prof. Florian Martin-Bariteau: In my view, PIPEDA should clarify the issue of the retention of data over time, provide for an obligation for organizations, and also provide a direct right to litigants. The direct rights of litigants are one of the conditions for adequacy. As with the enforceable orders and fines, paragraph 45(2)(b) of the Regulation tells us to look at whether the supervisory authority is truly independent and has adequate enforcement powers.

[*English*]

Mr. Raj Saini: Ms. Scassa, do you have anything to add?

Prof. Teresa Scassa: Yes. I would agree with that. I certainly think the biggest weakness in PIPEDA in terms of conformity with European norms is on the enforcement side. There are simply not enough powers for the commissioner.

Mr. Raj Saini: Mr. Martin-Bariteau, you mentioned a structure for fines within Europe under the GDPR right now. The fine structure is either 4% of annual turnover or 29 million euros, whichever is the higher number. Do you think we should follow some sort of mechanism? Right now, as you've very aptly said, there is no fine procedure. The Office of the Privacy Commissioner cannot fine.

Ms. Scassa, in your writings, you've mentioned Globe24h. In that Romanian case specifically, the fine imposed was only $5,000, and there was no way to collect on that or to even prevent Romania from stopping the indexing of files on the CanLII website.

Do you think the fine procedure should be there, and at what levels?

[*Translation*]

Prof. Florian Martin-Bariteau: I think the GDPR's mixed approach is the good one, regardless of the percentage, because even at 4%, I think it's still calculated based on the number of citizens affected by potential breaches of confidentiality and depending on the area.

We know that there are fewer citizens in Canada than in the European Union. On the other hand, it is important not to have a simple percentage, because 4% of a small structure, for example a start-up company, is not much. The company might want to take the risk with its investors and tell them to go ahead. If anything were to happen, at most, it could be about 4% of $500,000. That's peanuts. That's why it has to be doubled.

For example, in France, until 2016, the maximum amount was $150,000 for the first fine and $300,000 afterwards. It did not work. France has just raised this to a single amount of $3 million. This was adopted almost at the same time as the Regulation, which in my view also reflects the number of citizens concerned within the boundaries of a certain territory.

● (1625)

[*English*]

Mr. Raj Saini: Ms. Scassa, in your opening preamble, you mentioned business. Right now, the difference between the GDPR and Canada is that we don't have a privacy-by-design or privacy-by-default mechanism. Do you think that's important, or is that a first step to making sure not only that businesses are somewhat concurrent with GDPR but that the relevancy is there?

You also mentioned SMEs. Do you think that, by process, there should be some sort of privacy document or privacy agreement that would be standardized across the Internet, to the extent that we can do it, whereby privacy trust marks could also be used? In this way, we would be helping consumers when they interact with certain businesses to have the confidence that the company has a privacy-by-design or privacy-by-default mechanism and, more important, that it has been authorized by some sort of body so that they would have confidence and there would be a privacy trust mark there. Would that be something that you think would be viable?

Prof. Teresa Scassa: I know that in the very early days of PIPEDA there was a lot of talk about trust marks and trust seals and so on. People tried them. They haven't really gone very far. I think there have been concerns about the counterfeiting or faking of trust seals and trust marks as well. I'm not sure how viable that is as a solution.

There are interesting technological developments as well. People are working on codes and apps, for example, that will scan and rate privacy policies, so I would be hesitant to go with a trust mark solution when there may be other technological tools that would be more useful and more effective in terms of helping consumers understand what the privacy policies are.

That said, I know that for some time we've been talking about privacy by design and privacy by default. Those are important principles. It may take amendments or changes to the law to get people's attention on them.

Mr. Raj Saini: Okay.

Mr. Karanicolas, you mentioned that Google had 350,000 or 340,000 requests for the right to be forgotten. In those cases, 42% were removed. You mentioned the case in Europe, so I'm thinking you probably meant the Google v. Spain case. Is that what you were talking about?

Mr. Michael Karanicolas: That was the original case at the ECJ, yes.

Mr. Raj Saini: Do you think the Google v. Spain case, and the judgment from that case, should be used in a way? The judgment was clear on the right to be forgotten and the right to erasure. Do you think that was the right judgment, and is that something we should use, or not at all?

Mr. Michael Karanicolas: No. I think the judgment of that specific case was terrible. That's a lot of what I was speaking to in terms of the lack of clarity and in terms of the solution that was proposed.

As well, specific to that case, I don't think it's a very good test case in terms of the right to be forgotten. In my opinion, the specific information that's at issue in that case, which is a person's bankruptcy or some sort of financial difficulty that they were in 15 or 20 years ago, is absolutely relevant. That information should certainly still be available. I think what they—

Mr. Raj Saini: But—

The Chair: But we're out of time, Mr. Saini.

Voices: Oh, oh!

The Chair: Mr. Kelly, you have up to five minutes, please.

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

In listening to the witnesses we've had so far, including today's witnesses, I'm struck by the sheer number of different kinds of organizations that this law applies to, and how many different contexts or different anecdotes and examples are discussed that fall under the same law, and yet it would seem virtually meaningless, perhaps, to the different types of businesses and organizations that this law is subject to. You have professional services like law firms, financial services, accounting firms, and my own business from before I became a parliamentarian, the mortgage brokerage business. These are businesses that have long, long understood the need to keep client information private. They do not try to share information publicly or to profit from doing so. It would be completely counter to all the principles which the many different professions that must collect information work under, and yet the same law is also for a social network, for whom the product is the information that is shared.

Do we need to have two different laws? We have personal information and privacy, which seems like one thing. Electronic data, or the deliberate sharing or communication of electronic information, strikes me as something quite different.

I'd like any of you to comment on whether or not, with so many different things going on and the different types of activity that this law tries to regulate, this needs to be split up.

● (1630)

Prof. Teresa Scassa: I could jump in on that.

I think there would be dangers in splitting it up. Increasingly over time the commissioner's approach has been to try to create guidance that is specific to particular sectors or particular contexts so that you have one law that applies to all, but how it applies in particular contexts may be different. The commissioner's office has given attention to mobile apps, and has given attention to fitness devices, and has looked at various specific things with guidance to small businesses and guidance to businesses in particular sectors.

The code of practice model is one that I think is also getting more attention now. This is the idea that perhaps some sectors could work together to develop codes of practice around certain types of information collection use and disclosure within the context of their particular operations, and that this could somehow be developed in consultation with the OPC and approved by the OPC. You would start to shape norms and guidance around particular sectors under the umbrella of one law and one commissioner. It seems to me that this would be a preferable approach to dividing it up and having separate laws.

The other thing, of course, is that some companies start out being brick and mortar companies, then go online, and then they develop apps. Businesses are constantly changing in terms of their information practices and needs.

Prof. Florian Martin-Bariteau: I have nothing to add.

Mr. Pat Kelly: Okay.

Mr. Karanicolas.

Mr. Michael Karanicolas: [*Inaudible—Editor*] against relying on market incentives or thinking that companies that have a direct interest in keeping their users' information secret or following better practices will necessarily do that. Ashley Madison is a great example of a company that had a direct interest in having strong security and strong privacy protections, had nothing good in place, and didn't follow any industry best practices to safeguard user information or protect users' privacy.

I do think that the idea of building a degree of flexibility into how —

Mr. Pat Kelly: If I may, I'll stop you on that example. I'm not familiar with exactly how that breach happened. Was that a failure of legislation or just a failure of that particular company?

Mr. Michael Karanicolas: Certainly, it was a failure of that company, but I think you could say that the fact the company was allowed to operate the way it did, with such shoddy security practices, was potentially a failure of legislation or a failure of enforcement, in the sense that there were basic security mistakes being made that weren't necessarily being monitored or followed up on.

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

We now move to Mr. Long, please, for five minutes.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Chair.

Welcome back to some of our guests, and welcome for the first time to Mr. Martin-Bariteau.

Mr. Karanicolas, I want to start with you with respect to meaningful consent and how that relates to children.

I talked about this at our last committee meeting, too. I have friends with younger children. We were at their place last weekend. The children were on their computer going through things and clicking on this and clicking on that. What protection does PIPEDA need to ensure that our children are being protected?

I'll start with you, Mr. Karanicolas, and go to Ms. Scassa after that.

● (1635)

Mr. Michael Karanicolas: It's well established to have different rules in place for protecting children in terms of gathering their information and tracking their information. I think there's a huge challenge online in implementing that, because it's quite difficult, I think, in terms of people who navigate to a particular website to know how old the users are. You can require them to enter their birthdate, but again, that's not a particularly difficult hurdle to overcome—

Mr. Wayne Long: I'm going to jump in there, if you don't mind.

One of the articles I read recently stated that a lot of U.S. websites have more tracking software on them for children than they have on sites for adults—the clickbait. Again, what can we do to ensure that our children are being protected?

Mr. Michael Karanicolas: Because you can't necessarily know how old the person is who's on the website, I think the best option is to look at those websites that are directly targeting children, or that have a target audience geared towards younger web users, and to maybe expect a stronger standard to be imposed on them.

Mr. Wayne Long: Thank you.

Ms. Scassa.

Prof. Teresa Scassa: The American approach has been to have legislation specifically addressing children's privacy. The Canadian approach has been to deal with it under PIPEDA and to recognize that children may be a special case, so as a matter of interpretation, we take into account the fact that a website might be targeting children.

I guess the issue is, do we want to have something very specific in the legislation that makes it clear that when you're dealing with children, the rules are different or the rules are stricter? I see some merit in that: in being very explicit and up front that the rules for consent may be expressly different when you're dealing with children.

In that a lot of websites that target children are based in the United States, where they actually have to comply with the American laws, we've benefited to some extent. In Canada, we're simply not clear and explicit about the steps that have to be taken to protect children's privacy.

Mr. Wayne Long: Mr. Martin-Bariteau.

[*Translation*]

Prof. Florian Martin-Bariteau: I would say the same. American legislation already exists but there is a problem with enforcing it. It does not work. We know full well that, normally, under the age of 13, additional rules apply. Children under 13 are on all social networks in America, as in the rest of the world.

[*English*]

Mr. Wayne Long: Thank you.

Mr. Karanicolas, I want to get your feedback and opinion on Globe24h and that ruling. I'll be honest. I don't know a lot about it, but my spin on it is that it does pave the way for a Canadian version of the right to be forgotten. Can you elaborate for the committee on Globe24h and the impacts and ramifications of that ruling?

Mr. Michael Karanicolas: I haven't examined the case. I haven't read the case. I've read only second-hand accounts of it.

What I will say is that one of the things that struck me was that it demonstrates some of the challenges in jurisdiction you have in these kinds of cases. This is not specific to the right to be forgotten. It impacts a lot of online speech, where there are going to be challenges in enforcement and also challenges in imposing a particular Canadian standard on websites that might be operating elsewhere but targeted at Canadians.

Mr. Wayne Long: Ms. Scassa, could you comment on that?

Prof. Teresa Scassa: Yes. I would hesitate to say that it really creates a Canadian right to be forgotten. The very particular context of the case is that it was dealing with court decisions that had been made publicly available by the courts under specific restrictions that weren't being respected, and—

Mr. Wayne Long: Those decisions were accessible, but they just weren't linked to Google. Was that it?

Prof. Teresa Scassa: That's right. They were accessible but not indexed, and the courts made them available on the basis that they would not be indexed.

Mr. Wayne Long: Okay. Fair enough.

Prof. Teresa Scassa: They were scraped and then indexed by this other site. I would hesitate to say that it's really a right-to-be-forgotten case.

The Chair: Thank you very much.

We'll go back to Mr. Kelly for five minutes.

Mr. Pat Kelly: Thank you.

In the discussions around the right to be forgotten, that version of being forgotten—being de-indexed by a search engine—sounds more like a right to be lost than a right to be forgotten. It's certainly not erasure. I'm glad that we're finally getting to some distinctions between these different things.

Ms. Scassa, I was pleased to hear in your testimony and get into the record the acknowledgement of PIPEDA being onerous for small businesses and certainly unloved, probably misunderstood and, I would say, probably feared by many. Small business owners I've talked to are certainly not conversant with privacy law. They know there is a privacy law out there. In many cases, they're probably at a loss as to how to comply and, yes, it's beyond the reach of many businesses to have expert advice on how to comply, as you mentioned in your testimony.

In your opening remarks, though, you characterized the consent model as a joke. If so, what's the answer?

● (1640)

Prof. Teresa Scassa: Yes, well, I don't know, but I certainly know there's a huge volume of personal information about me that is out there now and is being collected and transmitted probably right now by my phone, information that I don't want to share. I don't even know what it is or how it got there. For me, that makes consent a joke, in that even somebody who's educated in law, has law degrees, and who works in the field of privacy can't get a handle on what's happening to their personal information. To me, that says the system is broken.

How do you fix it? I think the commissioner's consultation produced some interesting suggestions, ideas, and possibilities. I think it's a question of trying to find the right combination. I don't know. I'm sorry. I really wish I could say, “This is what's going to do it.”

Mr. Pat Kelly: Consent surely has to be the basis on which consumers and businesses interact with each other.

For anything from going to the local bowling alley, to applying for a mortgage, to signing up for a cellular phone, to choosing to post pictures on Facebook, yes, the vendors of these services must recognize and be aware of privacy expectations on behalf of their customers. Customers have to be able to consent, or not, to these services. I don't know how we get around this idea that consent must end up being the principal basis of these commercial relationships.

Go ahead, Mr. Karanicolas.

Mr. Michael Karanicolas: I think consent is certainly a prerequisite, and I think you must have some form of consent within any system, but in a lot of the examples that you mention, consent is not the only thing that comes into play. There are also regulations and rules that govern these relationships.

I think there are ways to boost the current model of consent through greater transparency—that's a big one—on what exactly is being done and also through presenting what's being done to users in a way that promotes engagement and accessibility. Again, that's the opposite of the way things are being done now, with terms of service that are overly legalistic and complicated. I also think there's room for centralized rules to be put in place about what can or can't be done, or particular models that should be followed.

Mr. Pat Kelly: Go ahead, Mr. Martin-Bariteau.

[*Translation*]

Prof. Florian Martin-Bariteau: I don't think that we have a magic solution in the case of consent. Of course, it must remain at the base, but people also have to know what they are consenting to. There was a problem on the consumers' side and we know that the provinces have legislated in the matter.

Perhaps it would be wise for consumers to know that they are consenting to something to do with protecting and managing their personal information. This is because confidentiality notices actually go in the opposite direction, in the sense that they deal with all the ways in which confidentiality is lost.

In addition, clearer legislation would perhaps help small companies to manage this. Principles could be set, with policies then established to reflect them. For each principle in the legislation, there could be an explanation of how to comply with and adhere to it.

● (1645)

[*English*]

The Chair: Thank you very much.

[*Translation*]

Mr. Dubourg, you have the floor for five minutes.

Mr. Emmanuel Dubourg (Bourassa, Lib.): Thank you, Mr. Chair.

My thanks to the witnesses for joining us this afternoon.

Mr. Martin-Bariteau, my questions go to you.

In your brief you say this: "In terms of drafting, the act should remain conceived according to the principle of technological independence and be principles-based."

The Privacy Commissioner has said that the act should be technologically neutral and based on principles. Given those comments, it looks like we are on the same wavelength.

However, you say that, compared to other federal legislation, there is no doubt that this act is one of the worst drafted, because it has, to an extent, been copied. That being the case, what do you suggest? How can we go about reworking it, rather than improving what we have now?

Prof. Florian Martin-Bariteau: In reality, it's only a small doctrinal debate. It means practically the same thing.

The idea that the legislation is based on principles is meant to allow greater flexibility, to set limits and, as Professor Scassa said earlier, to allow small and large companies, the mobile and health world to adapt.

The current act evokes great principles in some way, but not at the same time. To understand a principle, you need to read the text of the act in three different places. As with some laws, perhaps the idea would be to gut everything. It is a matter of trying to agree on what the main principles and the number should be. Then, after the mandatory sections in which the title is defined, the first principle can be described, then the second, the third and so on. Then it can be made very clear what the limits are and what the recourse of the users and the powers of the commissioner are.

Mr. Emmanuel Dubourg: Is that how it's done in Europe?

Prof. Florian Martin-Bariteau: I would say yes, even though I don't have the regulations or the old directive in front of me. The suite of sections includes those on collection, communication and so on. It is also a question of this famous right to deletion—and not to be forgotten—which is something that may need to be clarified.

Mr. Emmanuel Dubourg: Like Ms. Scassa, you agree to giving the commissioner more power. In terms of enforcement, you talked a lot about fines that should be imposed. However, you are also telling us that to avoid the appearance of a conflict of interest, fines should be payable to the Receiver General.

Could you expand on that?

Prof. Florian Martin-Bariteau: It is simply a matter of avoiding possible attacks by the private sector, which could claim that the commissioner would leave his role as an ombudsman to become a "sanctioner". To increase his budget and his powers, he would apply greater sanctions.

Mr. Emmanuel Dubourg: However, you agree that the commissioner would be the one to determine and enforce the penalties, but the budget would not be determined on that basis.

Prof. Florian Martin-Bariteau: Exactly.

His budget would be totally independent of the sanctions he would impose or not, and it would come back to the taxpayers, therefore to Canadians.

Mr. Emmanuel Dubourg: Right.

However, other organizations or other departments, even if they raise money, do not necessarily keep it. Take, for example, the Canada Revenue Agency.

Lastly, we are talking about the right to be forgotten. You said that it should not be used to manage the reputation of people. Earlier, you heard our colleagues talking about young people, for example, who post messages on Facebook or on other social media. In terms of reputation management, what are you telling us about that?

● (1650)

Prof. Florian Martin-Bariteau: I think my way out would be to say that I do not think it would be PIPEDA that would deal with that, but that it's more about private relationships. Some provinces have established remedies. We have the Criminal Code, which provides for a criminal remedy. However, if it was put online and it was in the public interest—

Mr. Emmanuel Dubourg: On the other hand, we know that these organizations have algorithms, that they will take this information, that they will use it, and that they will then offer services. They want to sell products. That is the point raised. Do you not think that PIPEDA should continue to regulate all of this?

Prof. Florian Martin-Bariteau: Yes, in that case, but in the case of someone who is going to get a photograph and put it elsewhere, then I don't think that person is subject to PIPEDA anymore. There is more talk about the right to the image and civil liability, which is generally a matter of provincial jurisdiction.

Mr. Emmanuel Dubourg: Okay. There's Ms. Scassa—

[*English*]

The Chair: We're actually well past the time, Mr. Dubourg.

Mr. Blaikie, for the last of the scheduled time here, please go ahead.

[*Translation*]

Mr. Daniel Blaikie: Thank you, Mr. Chair.

My next question is for Mr. Martin-Bariteau.

Obviously, there is an important economic link between Canada and the United States, and there is a real sharing of information. It may involve a transfer of information between Canadian companies and American companies. This is done even when we record data with a Canadian company, because the infrastructure we use then is in the United States. We know that American law does not give much protection to citizens of other countries.

Does our relationship as such, let alone the other deals with the United States, threaten our relationship with Europe and the judgment Europeans might pass on the protection of their personal data?

Prof. Florian Martin-Bariteau: That is an excellent question. I must admit that I haven't thought about it.

Mr. Daniel Blaikie: Could you? Maybe not today, but I invite you to think about it a bit and give us your opinion at some point.

Prof. Florian Martin-Bariteau: It would be a pleasure.

Certainly the problem at the moment is that recent decisions of the new government have made this is an issue for Canadians. I can look at how this would affect an adequacy decision.

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

[*English*]

I'd like to come back to the question of consent. I know we've tried this a couple of times.

One of the things I find as a layperson with respect to consent is that it would be nice to be able to divorce my consent for the use of my personal information from being able to use the service. You know, people can't decide to just not use computers anymore because they don't want to have that personal information shared, or they can't decide not to use a Microsoft product if they're in a work environment where often they're exchanging documents or whatever. In order to get into what have become essential tools for doing your job or even conducting your personal affairs, you can't read those terms of use and say you don't like those terms of use, so you're just not going to use that software, because then you can't actually accomplish the things you need to be able to accomplish, either in your personal life or in your professional life.

I could be wrong about this, but I think consenting to the extent of collection and then third party use of my personal data is often not really relevant to my using the service. Is there a legal way to try and divorce consent to the kind of widespread use of my personal information from what they would really need?

If you have an app like Foursquare, for instance, which uses your location, which is about where you are and about sharing that with other people, obviously collecting my location at that time, and doing that through my phone, is part of the app. With other software, however, you're often consenting to a broad statement about using your personal information that really has nothing to do with the use of that software. It's not integral to the operation of whatever service it is I'm trying to access.

Is there a way to try to carve that up that doesn't become overly cumbersome?

● (1655)

Prof. Teresa Scassa: The overly cumbersome part is the tricky thing. One of the challenges, of course, is that there are a lot of so-called free apps and free social media platforms and free services that are not free. The currency that you pay is your personal information. In that context, it does make it harder to draw a line between what is reasonably necessary, since they're the ones who are deciding what they need in order to make their business model stay afloat. I think that's another challenge as well.

The Chair: Thank you very much.

Colleagues, we're at the end of the official rounds of questioning. I know that some colleagues want to follow up with some questions.

Mr. Massé, I know that you would like to ask some questions, so I'll go to you right now.

If any of our witnesses have some things that they wished they'd said or that have come to mind, there will be an opportunity at the end to express those thoughts.

Mr. Massé.

[*Translation*]

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

I would like to thank the witnesses for appearing before the committee and for taking part in its work. I know that you must have done a lot of work in order to meet with us. It's greatly appreciated.

Mr. Martin-Bariteau, earlier you referred to the term “technological independence”. I just want to make sure I properly understand the term. Is “technological independence” the same for you as “technological neutrality”? To you, it's the same concept. Is that correct?

Prof. Florian Martin-Bariteau: Yes, it's the same concept. It's just that, in my doctorate dissertation, I have just defended that we should instead speak of “independence” rather than “neutrality” because the word “neutrality” has two meanings.

Mr. Rémi Massé: That's a good point.

In this context, what recommendations would you make to ensure that the Personal Information Protection and Electronics Documents Act, commonly referred to as PIPEDA, provides this technological independence?

Prof. Florian Martin-Bariteau: I think that on this point, aside from writing, this is currently the case. There are no rules specific to paper or the Internet.

You are going to propose amendments to the bill and Parliament will pass it. In the time it'll take for the legislation to come into force, technology will have advanced. If we think of artificial intelligence and robotics, for example, we don't know what tomorrow will bring. We only know the situation today. So it's preferable to always keep to this idea of principle. This will allow the law, once it's been properly drafted and not as it is currently worded, to be in force for many years and to adapt to all technological developments that we can't even imagine yet.

Mr. Rémi Massé: Okay. Thank you.

On another point, the comments of all the witnesses obviously caught my attention.

Mr. Martin-Bariteau, in your remarks, you mentioned the right to be forgotten. You find that the proposition dreamed up and demanded by some is dangerous.

Could you tell us more about what led you to make such comments? You said that in a democracy, the archives have never been erased simply because they were disturbing, at least not legally. In your opinion, this is very dangerous ground. I'd like to hear more about that.

Prof. Florian Martin-Bariteau: This comes back to the idea of reputation management. For many people, when they propose a right to be forgotten, they want the right to be able to erase information that concerns them. For example, it can be disturbing press articles that talk about some things they have done in the past. An article might have appeared in the press last year and, later, they went to a job interview. They would like to be able to erase the information that is recorded.

It's true that we are in a world today where it is increasingly difficult to forget. The Internet doesn't forget, nor does it forgive. People have never been allowed to go to *La Presse* or the daily newspaper *Le Devoir* to ask that articles be deleted. A person might say that, since an article is no longer agreeable, we will remove it from the archives and erase it from all the libraries.

I don't see why today, because it's facilitated by technology, we would allow actions like that, which would erase the memory.

However, as someone said earlier, there are a number of other cases of information gathering, which is the case in Globe24h.com. One of my colleagues insisted that this is perhaps the beginning of the right to forgot. When I read the court ruling, which is on pages 70 to 76 of the judgment, I think that the problem is that the collection of information is in violation of the act and is being used for illegal purposes. In this case, it was to extort people by telling them that we would delete data in exchange for money. This is not reputation management. These are just attempts at fraud.

● (1700)

Mr. Rémi Massé: Thank you.

[*English*]

The Chair: Mr. Dubourg, did you want to follow up? No.

Go ahead, Mr. Saini.

Mr. Raj Saini: I have a very quick question for Ms. Scassa.

My good friend Wayne Long asked a question about kids when it comes to privacy. I just wanted to ask your advice on one issue. In the United States a minor is determined to be the age of 13. That regime is undertaken by the FTC. Under the new GDPR regulations that have come out, the age will be 16. In Canada we don't have an age parameter. Apparently the Privacy Act covers all ages.

I'm wondering if you think that's important for two reasons: one, to have a benchmark where websites can have some control in terms of who they're dealing with; and two, when it comes to the right to be forgotten, to make it easier for people under that age as compared to an adult.

Prof. Teresa Scassa: As a parent of teenagers, I'm all in favour of the higher level of 16, simply because I think there's an educational function to be played there as well. It's not simply a question of strictly consent. It's a question of ensuring that kids under that age are given more opportunities to reflect on what they're doing, what they're consenting to, and what they understand about information collection. There really is an educational role to be played there.

Mr. Raj Saini: So it's 16, then?

Prof. Teresa Scassa: As a parent of teenagers, I'd kind of go with 25—

Voices: Oh, oh!

Prof. Teresa Scassa: —but 16 I could live with, yes.

Mr. Raj Saini: Thank you.

The Chair: Mr. Massé, and then we'll have a quick question from Mr. Bratina.

[*Translation*]

Mr. Rémi Massé: Thank you, Mr. Chair.

I forgot to ask you something earlier, Mr. Martin-Bariteau.

In your conclusion, you referred to a short bilingual document containing examples and recommendations, and you didn't have time to finish your remarks. We would be very interested in having you send us this document and your recommendations.

Prof. Florian Martin-Bariteau: I would be pleased to.

[*English*]

The Chair: Thank you very much.

Mr. Bratina.

Mr. Bob Bratina: Thank you.

Mr. Karanicolas, you focus in your work on digital rights and freedom of expression online. With regard to journalism and personal information protection as it relates to journalists and fake news—we hear all about that right now—much of that is just distributed electronically. What responsibility do you think news outlets should have in receiving, publishing, or broadcasting information that is received through, let's say, digital means?

I guess the only way I can focus this on our conversation is to ask whether the public should have a right to access the sources used by the news media to publish or to put their news on air.

Mr. Michael Karanicolas: Journalists' source protection is a very important principle of freedom of expression and needs to be protected. We're moving away from PIPEDA here, but I think the law is not as strong in Canada as it should be. It's a cardinal rule that needs to be safeguarded that journalists don't need to divulge their sources.

On the issue of fake news, as soon as the issue started to come out, I think a lot of freedom of expression people were unhappy because they saw the direction in which this conversation was going to go. There's a strong need for initiatives to promote savvy readership and to promote responsible journalism, but the term “fake news” is very often abused by governments around the world to try to prohibit opinions that they don't agree with. As soon as the door to that conversation started, I think a lot of people were very upset, and I think that's the direction that the conversation globally is unfortunately heading in.

Mr. Bob Bratina: Thanks. I just wanted to hear your opinion on that.

The Chair: I'm not terribly sure about the germaneness to the study, but it's important.

Mr. Bob Bratina: I'll get to it, if you give me another hour.

Voices: Oh, oh!

The Chair: Colleagues, if you'll just indulge me for a quick second, I have a question for the witnesses.

Notwithstanding the fact that the data garnered by malware, spyware, bots, and so on is covered under different Canadian legislation, that information can sometimes be melded and merged with information that's legitimately garnered through something like the people who follow PIPEDA. Given the fluidity of data, the World Wide Web, and the fact that it's uncertain exactly where the data is actually stored—we have distributed storage around the world, distributed processing around the world, and so on—how important is the harmonious nature of our legislative and regulatory environment when it comes to the protection of information in order to ensure that we get the right balance between protecting people's personal information and not chasing away tech companies in Canada that might be investing, researching, and doing innovative things with the use of data? How do we make sure we get that balance right?

I'll just leave that out there for whoever wants to go first.

Seeing none, I'll pick Mr. Karanicolas.

● (1705)

Mr. Michael Karanicolas: In terms of harmonizing rules and considering how rules are done in different places, it's tremendously important but also tremendously difficult. Ideas about privacy and the appropriate limits of the private sphere, as well as how your personal information should be handled, vary tremendously from place to place, so it's very difficult to come up with a common standard on issues like privacy or data protection.

I do think, though, that you hit on something that I absolutely agree with, which is that the opacity of these data flows is a huge problem. Rather than focusing on the location where information is specifically being stored, to me it's the identity of the players that is a bigger concern and the fact that you can make an agreement with Google or Facebook and you can read their terms of service—difficult to understand as they are, at least you have it in front of you—and then Google or Facebook can pass your information on to a third party data broker and from there it's just a black box.

There is a huge need for transparency on where this information is going after it's been collected by the person you're contracting it with, and generally more information about how information is being processed behind the scenes.

Prof. Teresa Scassa: I agree with that. Transparency at that level is going to be an enormous issue.

I do think that data protection is becoming interdisciplinary as well. Just to use the example of the data portability right, which is something in the new European directive, we were discussing this earlier today and my view is that it is competition law, not really data protection law. It doesn't really matter, necessarily, in terms of the overall regulation of the environment but I do think we are in a context in which there is a lot of overlap now. I see some big data issues as human rights issues or anti-discrimination issues, and then some of them are consumer protection issues.

We currently have traditionally dealt with different issues under different statutes in different departments of government. There is increasing convergence in terms of the relevance of those provisions to data protection, or perhaps data protection to the relevance of those sorts of issues as well. So I think this is a challenge, too. I definitely would agree with that.

[*Translation*]

Prof. Florian Martin-Bariteau: I agree with what was said.

[*English*]

The Chair: Okay.

Subsequent to that, in previous experiences on this committee and in my previous role as a database administrator, my issues with data are a bit technical, but there is a whole debate around deletion and deactivation, which are different things completely. We haven't had a very good discussion about deletion versus deactivation.

The other thing I think we need to flesh out a little bit more on the committee is the language, the simplicity of the language and the layman's use of the language when it comes to agreements or terms of agreement when we sign on for something, because the currency, as you say, in most cases is actually the data that's provided and the personal information that's provided when we log on and use a free app, for example, or even a paid app.

I know there are a lot of questions. Nobody that I know of, and I'm a computer geek of sorts, reads the end user licence agreements that are 65 pages long and full of legalese. I'm wondering if you have any recommendations for this committee in terms of simplifying that for the consumer.

Prof. Teresa Scassa: Michael, do you want to start?

Mr. Michael Karanicolas: In terms of the rights of the consumer in terms of deletion and understanding, again, transparency plays an important role at the outset. Users should be able to understand what information about them companies are holding, and then requesting that the deletion is of that information, or the removal of that information when they leave the service, or the correction of that information, are important aspects to pursue.

In terms of simplifying terms of service, there is a fundamental challenge, which is that these terms need to be legally binding. They're drafted by lawyers, and they need to be specific and they need to be written in a particular kind of language. The avenue that we support is generally providing simplified terms of service that go alongside the actual legal terms of service in order to explain things. I think that can be done. There are initiatives that have explored ways to explain what's being done in clear English that have had significant success.

There is a role for the OPC in terms of promoting model terms of service, which I think can be done. You can draft a standardized agreement that can be adapted to different contexts and I think that's an issue that should be pursued.

● (1710)

The Chair: Thank you very much.

Thank you to my colleagues. I'm not going to adjourn the meeting right now. I'm going to suspend the meeting and go in camera because we have a small matter we need to discuss.

At this point in time I'll excuse our witnesses. Thank you very much for your assistance as we continue our deliberations on PIPEDA. We know we can count on your expertise again in the future should the committee need it.

Colleagues, we're going to suspend for a few moments and we'll come back in camera.

[*Proceedings continue in camera*]