HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 052 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, March 21, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, March 21, 2017

● (1605)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Welcome, colleagues. Thank you for your good humour in response to the shenanigans in the House right now.

To our witnesses, thank you very much for your patience. Democracy isn't always neat and tidy. Sometimes it's messy, but it's still the best system we have.

We have a little over an hour. We'll probably have to leave here at around 5:15, unless we have unanimous consent to carry on through the projected bells that will sound at about that time. If we hear from each of our individual witnesses today, it should take us up to about 40 minutes. An additional 30 minutes to get through the first round of questions is probably all we'll get, unless we make a different decision at that point in time.

Without further ado, we are in our 52nd meeting. We're still studying the Personal Information Protection and Electronic Documents Act, or PIPEDA.

Joining us today is Micheal Vonn, a policy director. Micheal, welcome back to the committee. It's good to see you again.

As an individual we have Michael Geist, who is no stranger to this committee. We welcome you back, Michael.

As individuals we have David Fraser, also no stranger to the committee, and Colin Bennett. Thank you very much for joining us.

The order in which I introduced you will be the one in which the presentations will be made, if that's all right.

Yes, Mr. Kelly.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Mr. Chair, I know that we will have a very shortened meeting today, but at this point I'd like to move that the committee invite the President of the Treasury Board, the Honourable Scott Brison, to appear before the committee as soon as possible to discuss the recent decision to postpone his proposed reforms to the Access to Information Act.

I'd like to move that now.

The Chair: Are you moving the motion or are you giving 48 hours' notice of motion?

Mr. Pat Kelly: I'm giving notice of motion.

The Chair: Okay, because any substantive motion, Mr. Kelly, requires 48 hours' notice.

Mr. Pat Kelly: Indeed. So I'm giving notice now.

The Chair: The notice has been given. Thank you very much.

We'll now proceed to—

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Is that debatable?

The Chair: No. In 48 hours we can move the motion.

To get back to our scheduled business, we'll go to Micheal Vonn, please, for up to 10 minutes.

Ms. Micheal Vonn (Policy Director, British Columbia Civil Liberties Association): The BCCLA is a non-partisan society with a mandate to uphold civil liberties and human rights in Canada. Privacy is one of our most important portfolios, and we thank you for the opportunity to appear at this review of PIPEDA.

I'll just note at the outset that we have not been able to review the GDPRs sufficiently to comment upon the upcoming review of adequacy. We are pleased to leave that commentary to others on this panel.

Our association supports and echoes many of the recommendations and concerns that have already been voiced by academics, regulators, and witnesses from civil society. For example, we strongly support meaningful enforcement powers in PIPEDA, specifically, order-making powers, the ability to level financial penalties, and to award compensation to complainants in appropriate circumstances.

We have been calling for these powers for over a decade. In our view, there is no longer any credible argument for retaining the so-called ombudsperson model, as provincial counterparts have long demonstrated that order-making powers can be effectively combined with co-operative investigations, mediation, and education.

Likewise, we join others, including the BC Freedom of Information and Privacy Association, in calling for federal political parties to be covered under PIPEDA, like provincial political parties are covered under our corresponding legislation here in British Columbia.

Our association has heard from many Canadians, and most particularly from those areas that consider themselves ground zero in various robocalls scandals, that the complete failure to regulate the collection, use, and disclosure of their personal information held by federal political parties is entirely unacceptable. For all the obvious reasons, including historical abuses that have facilitated electoral fraud, this is a matter of immense importance and urgency.

I would like to speak briefly to a topic that has been discussed under the title “the right to be forgotten”, or more broadly, online reputation. This is an area of competing rights in which the BCCLA has not yet taken an official position. We are nevertheless very alive to the competing claims and the interests involved, and we would like to clarify a few points.

First, we need to understand the context of this discussion and, in our view, reject the notion that we are talking about a situation that is in any way analogous to ripping index cards out of the library card catalogue, the current go-to metaphor for de-indexing.

In no library that has ever existed has anyone been able to command the service of gathering information about their neighbour who is not a public figure, whose activities were not otherwise within the public interest, or for some other reason notable. Tenants, co-workers, ex-partners of current partners, classmates, and acquaintances—up until recently the vast majority of these members of the public, or ordinary people—have enjoyed the privacy protection of practical obscurity. The Internet and powerful search engines have eroded this protection very significantly, and people are definitely being harmed.

To give you an example of online reputation matters that spring from British Columbia, a small business in Nanaimo had a protracted battle with Google about Google's obligations under its own policy to remove anonymous online reviews. Those included libellous personal attacks on specific company employees. One of those employees, whom I'll call Ms. Jones, was said to be racist and to have the attention span of a wood bug. The company's inability to get the anonymous personal attacks of these employees removed was the subject of a CBC story. In fact, it appears that it was only the negative publicity and the media that finally made Google remove this review.

I needed to recollect the facts of this story for this submission to the committee. It had been reported in the media. I found that article using the following online search: “Google, B.C., online review, personal attack”. Those were my search terms. I found the article, and this is precisely as it should be. The information about Ms. Jones was contained in the article, as it was when it was first published. This too is precisely as it should be.

● (1610)

Then, as an experiment, I searched for “Ms. Jones” just by her name alone, as anyone might do—a nosy neighbour, prospective employer, landlord, or client. The first substantive hit in that search was the article containing the personal attack on her as a cognitively deficient racist.

Is this as it should be?

If this is a problem—and we know it is, because people contact our organization looking for solutions to exactly this kind of problem—how do we fix it without causing harm to other critically important rights, those of access to information and freedom of expression? We say that in order to do that discussion, we have to be very specific about the problem. The problem is not that searching for online reputation stories leads me to Ms. Jones. The problem is that searching for Ms. Jones leads me to the online reputation stories that report the content of libellous statements about her.

Without exploring what options are available to remedy this specific problem, it does seem, at a minimum, premature to announce that a remedy would necessarily be unconstitutional. Certainly the hope would be to find a way to meaningfully secure all the rights at issue.

Finally, I want to address the use of what are called “ethical assessments” or “ethical frameworks” for big data and the Internet of things. As the OPC indicated in their overview of submissions received in their consultation on consent, there is a great deal of enthusiasm within business and industry for ethical frameworks for the use of personal information, either as an added level of accountability or, more likely, as compensation for a system in which consent is being eroded.

The question of if and how consent can be made meaningful is, of course, a very large discussion. My sole point at this juncture is simply to stress that the model for assessment that is being proposed is not ethical. Calling it an ethical framework is deeply problematic.

In this framework, the people who want to use the data, in order to make money from it, will decide whether it is justified to use that data given the risks to privacy, reputation, etc. Those risks are assumed by other people. The people who stand to benefit are the people who are deciding what the risk level is and whether their purposes outweigh those purported risks. The people who are themselves being subjected to the risk have no say in the process.

It is simply impossible to describe this distribution of benefits and risks as one that is ethical. Assuredly, there are many individuals who would undertake this task with a conscience and with a desire to operate ethically and fairly. That said, individuals aside, the process itself is nakedly one of foxes guarding the henhouse, with merely a promise to be really ethical foxes—although, as you will note by the OPC's reviews, not so ethical that they would like a disinterested third party, say an independent ethics board, to have any part in that guarding function.

In sum, we would like to tell the committee that we have no confidence that the solution of ethical frameworks is either ethical or a solution.

Thank you very much.

● (1615)

The Chair: Thank you very much.

We will now move to Michael Geist, please.

Dr. Michael Geist (Canada Research Chair in Internet and E-commerce Law, Professor of Law, University of Ottawa, As an Individual): Thanks.

Good afternoon. My name is Michael Geist. I'm a law professor at the University of Ottawa where I hold the Canada research chair in Internet and e-commerce law. I appear here today in a personal capacity representing only my own views.

There's a lot that I would like to discuss given more time: stronger enforcement through order-making power; the potential for Canada's anti-spam legislation to serve as a model, at least on the issues of tougher enforcement and consent standards; and the mounting concerns with how copyright rules may undermine privacy. But given my limited time, I'll focus at least for these opening remarks on three issues: privacy reform pressures, consent, and transparency.

First, on the issue of reform, I had the honour of appearing before both the House and Senate committees on Bill S-4, which was ostensibly the effort to update PIPEDA by implementing recommendations that were first made in 2006. At the time it was obvious that further changes were needed. In fact, the ongoing delays in implementing even aspects of that bill, security breach notification, for example, shows how painfully slow the process of updating Canada's privacy laws has been.

I believe there's an increased urgency to address the issue. You've already heard from some and may hear from others about developments in Europe with the GDPR, which could threaten Canada's adequacy standing with European privacy officials.

But there's another international development that I think could have a significant impact on Canadian privacy law that bears attention. That's our trade deals and trade negotiations. The upcoming NAFTA renegotiations seem likely to include U.S. demands that Canada refrain from establishing so-called data localization rules that mandate the retention of personal information on computer servers located in Canada. Data localization has become an increasingly popular policy measure as countries respond to concerns about U.S.-based surveillance and the subordination of privacy protections for non-U.S. citizens and residents under the Trump administration.

Now, in response to those mounting concerns, leading technology companies like Microsoft, Amazon, and Google have established or committed to establish Canadian-based computer server facilities that can offer up localization of information. Those moves follow on the federal government's own 2016 cloud computing strategy that mandated that certain data be stored in Canada.

If we look at the Trans-Pacific Partnership, the TPP, we see that it included restrictions on the ability to implement data localization requirements at the insistence of U.S. negotiators. It seems likely that those same provisions will resurface during the NAFTA talks.

So too, I would argue, will limitations on data transfer restrictions which mandate the free flow of information on networks across borders. Those rules are unquestionably important to preserve online freedoms in countries that have a history of cracking down on Internet speech. But in a Canadian context they could restrict the ability to establish privacy safeguards. In fact, should the European Union mandate data transfer restrictions, as many experts expect, Canada could find itself between the proverbial privacy rock and a hard place, with the European Union requiring restrictions and NAFTA prohibiting them.

Secondly, I want to focus on consent. As you know, privacy laws around the world differ on many issues, but they all share a common principle: collection, use, and disclosure of personal information requires user consent, an issue that has become increasingly challenged in a digital world where data is continuously collected and can be used for a myriad of previously unimaginable ways.

Now, rather than weakening or abandoning consent models, I believe the Canadian law needs to upgrade its approach by making consent more effective in the digital environment. There's little doubt that the current model is still too reliant on opt-out policies in which businesses are entitled to presume that they can use their customers' personal information unless those customers inform them otherwise. Moreover, cryptic privacy policies often leave the public confused about the information that may be collected or disclosed, creating a notion of consent that is largely fiction not fact.

How can we solve some of the problems with the current consent-based model? I'd identify at least four proposals. First, we should implement an opt-in consent approach as the default approach. At the moment, opt-in is only used where strictly required by law or for highly sensitive information, such as health or financial data. That means that the vast majority of information is collected, used, and disclosed without informed consent.

Second, since informed consent depends upon the public understanding how their information will be collected, used, and disclosed, the rules associated with transparency must be improved. The use of confusing negative-option check boxes that leave the public unsure about how to exercise their privacy rights should be rejected as an appropriate form of consent. They never know if they should be clicking or unclicking a box to protect their privacy.

● (1620)

Moreover, given the uncertainty associated with big data and cross-border data transfers, new forms of transparency and privacy policies are needed. For example, algorithmic transparency would require search engines and social media companies to disclose how information is used to determine the content displayed to each user. Data transfer transparency would require companies to disclose where personal information is stored and when it may be transferred outside of the country.

Third, effective consent means giving users the ability to exercise their privacy choices. Most policies are offered on a “take it or leave it” basis, with little room to customize how information is collected, used, and disclosed. Real consent should mean real choice.

Fourth, stronger enforcement powers are needed to address privacy violations. The rush that we saw in Canada to comply with Canada's anti-spam laws was driven by the inclusion of significant penalties for violation of the rules. Canadian privacy law today is still premised largely on moral suasion or fear of public shaming, not tough enforcement backed by penalties. If we want the privacy rules to be taken seriously, there must be serious consequences when companies run afoul of the law.

Finally, I'll say a word on transparency and reporting. As many of you will know, in recent years, the stunning revelations about requests and disclosures of the personal information of Canadians—millions of requests, the majority without court oversight or warrant—point to an enormously troubling weakness in Canada's privacy laws. Simply put, most Canadians have no awareness of these disclosures and are shocked to learn how frequently they occur.

There's been a recent emphasis on private sector transparency reporting. Large Internet companies such as Google and Twitter have released transparency reports. Twitter released their 10th annual report today, and they've been joined by some of Canada's leading communications companies, such as Rogers and Telus.

Despite the availability of a transparency reporting standard that was approved by the government and the Privacy Commissioner, there are still some holdouts. The problem lies with the non-binding approach with respect to transparency disclosures.

I obtained some information under the Access to Information Act, and learned that after an industry-wide meeting organized by the Privacy Commissioner in April 2015, Rogers noted the following:

> It was indicated at this meeting that any guidelines adopted would fall short of regulation, but would be regarded as more substantive than voluntary guidelines.

Yet, if the non-regulatory approach does not work, it falls to either the federal Privacy Commissioner or the government to take action.

The most notable company to refrain from meeting these transparency standards is Bell Canada, Canada's largest telecommunications company. Bell initially claimed that it was waiting for a standard from the Privacy Commissioner, but now, almost a year after that standard has been released, they still have not released the transparency report. Millions of Canadians still don't know when, under what circumstances, and with what frequency Bell discloses their subscriber information. In my view, that's simply unacceptable.

If the current law doesn't mandate such disclosures there is a problem with the law, and reform requiring transparency disclosures with real penalties for failure to do so is needed. I don't need to tell you that scarcely a day goes by without some media coverage of a privacy-related issue. I think it is clear that the public is concerned with their privacy, and it is also clear that the business community has come to recognize the value of personal information. It is time for the law to catch up.

I look forward to your questions.

● (1625)

The Chair: Thank you very much.

Now, we move to Mr. Fraser, please.

Mr. David Fraser (Partner, McInnes Cooper, As an Individual): Good afternoon. Thank you to the committee and to the chair for this opportunity to speak with you today about this very important subject.

If I could just briefly introduce myself, I am a privacy lawyer and partner with McInnes Cooper in Halifax. I’ve been practising law in this area for about 15 years, and I’ve had a strong interest in the intersection or collision between technology and civil rights for quite some time. I'm also a part-time member of the faculty of law at Dalhousie University, where I've taught courses such as Internet and media law, law and technology, and privacy law. I'm a past president of the Canadian IT Law Association and former chair of the national privacy and access law section of the CBA.

I think the perspective that I can offer is as somebody who regularly advises businesses with a view to compliance with Canadian privacy laws, and I have represented a number of companies and clients in connection with investigations with the Office of the Privacy Commissioner of Canada.

I've had the benefit of advising clients on a full range of privacy, access to information, and technology issues in that time. In connection with this, I'm also often exposed to the privacy laws of other jurisdictions. One thing that's been abundantly clear to me over the last 15 years is that the more I learn about other countries' privacy laws, the better the Canadian law looks. It is actually a marvel of technological neutrality and resilience. It was drafted in the 1990s but continues to hold up very well, particularly with the amendments put in through the Digital Privacy Act.

I should emphasize that my comments should not be attributed to my firm, my clients, or any organizations that I'm associated with. These are my own views and my own opinions.

On the specifics, I'd like to address three issues, but I'd be happy to discuss any of the topics that I'm sure will come up in the rounds of questions.

First, I'd like to address the right to be forgotten. Then, I'd like to speak about the powers of the Privacy Commissioner. Finally, I'd like to address the question of consent.

In my previous appearances before this committee, particularly on the Privacy Act inquiry, I was asked about the right to be forgotten and whether it should exist under Canadian privacy law. My view then, as now, is generally no.

In the meantime, we've actually had a decision from the Federal Court of Canada in a case called Globe24h.com, which, as I understand it, related to a Romanian individual who operated a website entirely based in Romania. He would scour court and tribunal decisions from Canadian websites and post them on his own site. The main difference was that these tribunal websites, operated by government entities and organizations like CanLII, put in place measures so that individual names can't be indexed on search engines. If your name appears in a court case and you search your name, it's not going to show up in these databases.

This individual took down or didn't implement that protection. A person could find their name—it was associated with a court case—and it might have been embarrassing since for most people any day in court is not their best day. He then implemented a mechanism by which people could ask to have it removed. If they mailed in a request, it might be processed in six months, or they could pay some cash online and it would be taken down right away. Essentially it's been characterized as an extortion scam.

An individual whose information appeared on Globe24h.com complained to the Privacy Commissioner. The Privacy Commissioner found that the webmaster had violated Canadian privacy law—even though it was entirely based in Romania, I think it was not an unsensible decision on jurisdiction—and then took the next step, which is to go to the Federal Court as is already provided for in PIPEDA. The Federal Court issued an order finding that the purposes, which were ultimately extortive, were not reasonable and were in violation of the legislation. It required that the individual take down all of these decisions—and, as I understand it, the site is now inoperative—and required payment of compensation. Finally, the court ordered the individual, again in Romania, not to do it again, not to take any Canadian court or tribunal decisions and put them online in violation of the legislation.

One thing that I would note is that this decision—or at least the court case—was entirely uncontested, so there wasn't any nuanced understanding or discussion of countervailing interests, like the charter section 2(b) rights related to freedom of expression. The decision actually applied a provision in PIPEDA related to journalism that was found, in a parallel case in Alberta, to be unconstitutional, so I'm not sure we can necessarily take this as clear guidance that all of a sudden a right to be forgotten has been found in our legislation.

I generally urge caution with respect to this case, because the case itself was uncontested, or seeing it as attributing or injecting into our existing privacy law a right to be forgotten. I would also urge caution if the committee and others are looking to inject into our privacy law a right to be forgotten. For example, in many of the cases that we've seen coming out of Europe, the existence of the information on the Internet is entirely lawful, and the indexing of it is seen to be particularly problematic.

● (1630)

In the examples that Ms. Vonn mentioned, if the content underlying it is libellous, then, in fact, you can get an injunction to get that sort of content removed. Is it really the place to go after the indexer in connection with that particular problem?

Also, what needs to be noted and taken into account is that we have the right of freedom of expression in our constitution and guaranteed in our charter, but we don't have a right of privacy vis-à-vis businesses. So, if you attempt to do anything in this area, you're going to want to draft it for the purposes of surviving charter scrutiny, which is going to be difficult to do in the context of the right to be forgotten.

The next thing I'd like to talk about is the powers of the Privacy Commissioner. Based on my experience advising businesses in dealing with the Privacy Commissioner on a regular basis, I personally do not think it's a good idea to expand the power of the commissioner. The commissioner, in fact, has significant powers that are seldom used. If the commissioner were granted order-making powers or the ability to levy fines against organizations, his many roles would need to be closely examined in light of basic principles of procedural fairness and fundamental justice. The commissioner, not surprisingly, is an advocate for privacy rights. One should not lightly give one person or institution the powers of an advocate, an educational authority, an investigator, a prosecutor, and a judge. These functions are generally separated and are separated for a reason. It's an inherent conflict of interest to have the same person identify the bad guys, investigate the bad guys, prosecute the bad guys, determine that they are bad guys, and then punish them for being bad guys. We separate those in just about every instance. What we would end up with is, ultimately, something that looks like the Canadian Human Rights Commission, where you have a commission and a tribunal. I'm not sure you'd get many people advocating for an institutional structure like that for dispensing swift justice.

One thing that the Globe24h.com case actually does stand for is the ability of the commissioner, along with the complainant, to go to court. PIPEDA provides for an expedited application process. You appear in front of a Federal Court judge, and you put your case forward. The respondent has an application to respond—although in the Globe24h.com case, the individual declined to do so. The matter is determined by an impartial judge who has the ability to order an organization to change its practices. It has the ability to order compensation and damages. Those damages could, in fact, be punitive, but you'll note that most of it is based on wanting those powers to be remedial. I think that is, ultimately, a good thing.

One thing that I'm also concerned about is that if you were to reformulate the Office of the Privacy Commissioner, the spirit of collaboration and cooperation that I've generally seen would disappear. If the Privacy Commissioner is both the cop and the prosecutor, you would see businesses asserting their right to remain silent and, in fact, not cooperating in the same way that they do. In my experience—there may be other companies out there that aren't as co-operative as my clients—my clients are generally looking for a resolution; they are looking to negotiate something with the commissioner. That involves a fair amount of back and forth, and a fair amount of co-operation. If that role changes dramatically, then you're in a different environment entirely.

Finally, and just briefly, on consent, I would caution that although technology has gotten much more complicated and individuals' relationships with technology and the way that personal information is collected, used, and disclosed has gotten more complicated, any notion of abandoning the consent principle is, I think, problematic.

One aspect of it, for example, is the suggestion that everything should be opt-in, as Professor Geist suggested. I think we need to take a moment and think about how that actually plays out in many circumstances. For example, when Twitter launched, it had two options: your tweets could be public, or your tweets could be private. Many advocates say that the defaults of any new service, when it rolls out, have to be the most privacy protective. This would have meant that on day one when you signed up on Twitter, all of your tweets would have been protected. Those first users would have been yelling in an empty room. In fact, it was designed to be a public platform for people who want that. That was intended to be the default of Twitter, but if you wanted to, you could scale it back.

If there were a law that made it mandatory that your tweets be protected or that you had to implement the most privacy protective option, Twitter would have launched without protected tweets because they would have had to implement that. You ultimately end up with an option that is less privacy protective. We need to be cautious about where some of these decisions are going to take us, particularly in light of the enormous diversity of products and services that are out there.

I also really hesitate to implement any system that takes away an individual's choices. One of the great things, and one of the real core values, related to privacy is related to individual autonomy. There are those who probably don't mind the defaults—to kind of take them away in a particular direction. However, for those who actually take the time to understand or who are given the means to understand exactly what's going on with their information, they should always have the right to do that.

● (1635)

Thank you so much for inviting me to participate in this important discussion. I really look forward to the questions and answers.

The Chair: Thank you very much.

We'll now move to Mr. Bennett, please, for up to 10 minutes. Then we'll immediately proceed to our round of questions.

Professor Colin Bennett (Professor, Department of Political Science, University of Victoria, As an Individual): Thank you, Mr. Chair.

Thank you for the opportunity to appear before you again.

I am a professor of political science at the University of Victoria, and I'm generally known for my comparative work on privacy governance in both the public and the private sectors.

I understand that you would like to know a bit more about the European regulation and its impact on Canada, so that's what I want to principally talk about, and perhaps suggest how it should or should not influence our deliberations here about PIPEDA. Then I will suggest three areas where there are some glaring divergencies between what we do in Canada and what the Europeans are proposing.

When the general data protection regulation comes into force across the entire EU in 2018, it will be the most comprehensive set of data protection requirements in the world, and it will, in large measure, set the standards for the protection of personal data in global electronic commerce and cloud computing. For countries like Canada, it contains important extraterritorial implications that we need to consider very carefully.

Under the former directive, as you know, Canada was awarded an “adequacy status”, meaning that businesses could legally process personal data on European citizens without further contractual mechanisms. The EU did not consider Canada, as a jurisdiction, adequate, just those organizations that were subject to PIPEDA. Nevertheless, the adequacy status provided some significant practical benefits to Canadian companies. More importantly, it sent a symbolic message that Canada was a safe jurisdiction within which personal data could be processed. That issue, of course, assumes a more critical importance in the context of CETA, which will presumably increase trade and therefore the volume of consumer and employee data that flows across the Atlantic to Canada.

To this date, only 11 jurisdictions have been awarded this adequacy status under the European directive, and Canada is by far the biggest economy within that number. For the United States, adequacy is granted only to those companies that have self-certified under the new EU-U.S. privacy shield arrangement. Under the general data protection regulation, the adequacy mechanism will continue and the countries that have been awarded that status will continue to enjoy its benefits for the time being. The EU Commission envisages a mechanism of periodic review at least every four years, so presumably we can expect an evaluation of the Canadian assessment by 2021, but there is no guarantee that the benefits of that status will continue. Furthermore, there are lots of other countries that are likely to want to get in line. The difference between 2001 and now is that now there are something like 100 countries around the world that have data protection legislation sort of on the European model.

In October 2015, there was a decision by the European Court of Justice in the so-called Schrems case, which was about Facebook, that invalidated the former EU-U.S. safe harbor agreement and that has changed the politics of adequacy assessment in a number of ways. There are three points to note.

First, an existing adequacy determination does not absolve a European privacy protection authority from investigating a complaint against a company residing in another jurisdiction. Adequacy is not, and probably never was, a get-out-of-jail-free card. Canadian companies are as vulnerable as others to challenge in the EU.

Second—and more recently since the Snowden revelations—the entire question of access to business data by security and intelligence services is now prominent in any adequacy determination. In 2013, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs called for a review of Canada's privacy regime in light of our participation in the Five Eyes alliance, so this whole question is now part of the assessment process. Those concerns also need to be considered in light of the assurances by the American government in the EU-U.S. privacy shield that access to personal data by U.S. law enforcement and national security agencies will be subject to clear limitations, safeguards, and oversight mechanisms, although that will be reviewed and it is the subject of ongoing litigation in Europe at the moment.

● (1640)

Thirdly, the European court raised the bar for adequacy assessments to have what is called an “essential equivalence”. We do not have any clear signals yet on what that means. It's rather like revising for an exam without knowing what the grading standards are. What aspects of privacy protection are going to be considered essential? There are some new things in the general data protection regulation that did not appear in the directive and are not really prominent in PIPEDA either. Are they going to be part of the test that includes? My colleagues have talked about the right to be forgotten. There's a right to data portability in the regulation, which I could talk about. There is the right to object to decisions made on automated processing. There is privacy by design and privacy by default. Which are essential principles, and which are methods of enforcement and implementation?

At the moment, the adequacy requirements in the regulation are quite vague. They have to be applied consistently, and I would suspect that the EU is not going to insist on legal reforms in other countries that either are unrealistic politically or that will obviously pose constitutional problems for some jurisdictions, especially the United States. In light of that, I think we should be reluctant to revise PIPEDA just because the Europeans want us to. In any case, there is unhelpful rhetoric about this regulation being kind of the gold standard for privacy protection around the world. It is a mix of different provisions, some of which have been imported from countries like Canada. We should modernize PIPEDA because it needs modernization, not because it will satisfy a vague and shifting set of standards imposed from Brussels. We should take note of what the Europeans have done and draw lessons. I suspect that serious efforts to update and amend PIPEDA will not go unnoticed on the other side of the Atlantic. On the other hand, I would suspect that leaving the law as it stands will send the wrong message.

With that in mind, in conclusion, I'd just like to draw your attention to three broad areas, in which, I think, there are the most glaring divergencies between what we do in PIPEDA and what the European regulation says.

Firstly—and I'm going to skip over this, because my colleagues have talked about it—are the enforcement powers of the Privacy Commissioner. Under the general data protection regulation, data protection agents are empowered to levy some really significant administrative fines against companies—up to 20 million euros or 4% of annual turnover. I would not suggest that we go that far. Fines do capture the intention like no other sanction does, but in general, having reflected on this, I think at the very least, the Privacy Commissioner should be given powers equivalent to those available to the B.C. Information and Privacy Commissioner under our private sector legislation.

Secondly, we need to ensure that the Privacy Commissioner has all the tools in the privacy toolbox. At the moment, PIPEDA is written in a very reactive way. The statute is written as if the entirety of this work is devoted to complaints investigation and resolution. As David Fraser said, there are provisions in PIPEDA that have not really been actively used over the years. I believe that the most effective functions are more proactive and they involve a variety of other instruments. As personal consent becomes far more difficult to obtain in this era of big data analytics, I think organizations are going to have to rely on these other tools. The general data protection regulation and many other contemporary privacy protection laws recognize the importance of these other policy instruments in effective enforcement implementation and say that organizations must stand ready to demonstrate their compliance by using such mechanisms—things like codes of practice, privacy seals, privacy standards, privacy impact assessments, and so on. The regulation tries to incentivize good privacy practices, and I believe that PIPEDA should try to do the same thing.

So I would like to see a more explicit recognition in section 24 of PIPEDA that the commissioner may encourage these kinds of tools and, in some cases, require the adoption of those accountability mechanisms by Canadian companies and their trade associations. In particular, there is privacy by design and privacy by default.

● (1645)

The general data protection regulation says that organizations, should, as far as possible, ensure that, by default, the only personal data processed are those necessary for each specific purpose of the processing. It goes on; it's complex. What it tries to do, therefore, is to ensure that privacy protection will become an integral part of the technological development and organizational structure of any new product and service, and to the extent that organizations do not do that, they are then subject to heightened sanctions if there are investigations.

The Vice-Chair (Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): Mr. Bennett, I don't want to cut you off, but we're just over the 10-minute mark and will probably have less than a half-hour for questions. If you could wrap it up, it would be appreciated.

Prof. Colin Bennett: I was going to speak about privacy impact assessments, codes of practice, standards, and certification, and also the processing of sensitive data. There's a significant difference between what PIPEDA and the regulation say about sensitive data. In particular, I think there's a divergence, as Micheal Vonn has said, with respect to the processing of data on political opinions and affiliation.

I thank you very much for your attention. I'm sorry that I was slightly overtime. I look forward to your questions.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much to all the witnesses.

We'll begin with Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you all for being here today. Some of your faces I recognize; you've been here before. Welcome back.

Something that you've all spoken about or alluded to today is the right to be forgotten.

I'll start with you, Mr. Fraser, because you've written very clearly on that issue. You've said that it would be unlikely to withstand a charter challenge unless there was a pressing or substantial issue.

I have a question for you. With the advent of social media now and things such as that, there are children who are on social media, minors especially. Do you feel there should be some provision made to protect them or to allow them the right to be forgotten, especially if they're under, let's say, 14 to 16 years of age, an arbitrary age? Going forward, if they've done something in their youth, should they be held liable for that?

I would like to get an opinion from everybody, but I'd like to start with you.

Mr. David Fraser: Sure. I think that to a certain extent some of what we think of as being a right to be forgotten or a right to erasure, as it's more recently being called in Europe, actually exists. You have the ability to revoke consent that you've given previously. The Privacy Commissioner did an investigation of Facebook related to account closures, and all of that does exist.

So when it comes to any commercial organization that collects, uses, or discloses that information, that consent can be revoked, and you can require that information to be deleted.

● (1650)

Mr. Raj Saini: Mr. Geist.

Dr. Michael Geist: You talked about whether or not there ought to be specific protection for minors, and it's worth noting that in the United States there is. They did establish stronger privacy protection laws, specifically for those 13 years and under. There's a reasonable debate as to the effectiveness of those rules, but there was a recognition that they do require stronger protection.

I would argue that some of the recommendations that I made and that the committee has heard from others would go a long way to providing those protections. I've known David for a long time and respect him a lot, but the notion that somehow an opt-in standard takes away choice strikes me as completely the opposite of what it does. An opt-in approach ensures meaningful choice. It means that your choice is more appropriately reflected. So part of the challenge, for minors and for many others, of course, is to ensure they have the necessary tools and education about some of the privacy choices they're making and ensure those are adequately reflected. If there is a problem, in many instances it is that companies take advantage, I would argue, of individuals who are unaware of what will happen to their information. This may be particularly true amongst kids, who oftentimes are facing peer pressure to post information and therefore aren't really seeing their privacy choices adequately reflected.

A stronger consent-based model, I think, would go some way to helping solve some of that.

Mr. Raj Saini: Madam Vonn.

Ms. Micheal Vonn: Yes, thank you.

With regard to the revoking of consent to private companies, you can't really do that once the information is dispersed on the Internet. That goes to the key importance of looking at the potential, in appropriate circumstances—where there are no countervailing rights trumping the right to freedom of expression, etc., and where we're not talking about a public personality, but an ordinary individual—for delinking...once information becomes dispersed online. You don't have the option to go to the service provider, because the information has gone beyond them. You cannot revoke consent.

Mr. Raj Saini: Thank you for that.

Mr. Bennett, I don't want you to feel left out. I'll ask you an international question, since you brought up the GDPR.

Now that we've signed the CETA deal, internally we now have the issue of the trade barriers between provinces. Three provinces do not subscribe to PIPEDA, which is considered substantially similar to the existing legislation in B.C., Quebec, and Alberta. We have a problem internally where there's no consistency, but now we've signed CETA, and I'm sure that in the future we will sign other free trade deals—and you mentioned the EU and the U.S. privacy shield. To me there seem to be two or three different standards out there, whether it's GDPR, the EU privacy shield, or our involvement in the Five Eyes alliance.

Is there some way we can normalize or standardize what our privacy regime should be and what it should look like, not only internally but also internationally, so that our international trade partners will understand it and so that domestically we will have one regime rather than two or three?

● (1655)

Prof. Colin Bennett: I wish.

On the point about the provincial laws, I think there was an assumption initially that if PIPA in B.C. and Alberta, and the law in Quebec were considered substantially similar to PIPEDA, they would, by default, be considered adequate under the European Union standards. The European Union, however, has rejected an independent application by Quebec to have its law considered adequate, so that assumption is not absolutely correct. That's something that's going to have to be figured out in the context of the upcoming review of Canadian adequacy under the EU's GDPR.

At the moment, the adequacy standards of the European Union are stipulated, but they're quite vague. They have to do with respect for the rule of your law. They have to do with the essential principles of data protection. They have to do with the existence of redress mechanisms. They're trying to walk a very fine line between protecting the rights of European citizens when their data is processed overseas and interfering with the internal politics and constitutional requirements of other countries. That's where the tension has existed with the United States.

On the EU-U.S. privacy shield issue, I think that the continuation of that arrangement is up in the air at the moment, for a number of reasons. First, the standard to which that was negotiated was the old European directive and not the new one. Second, there's litigation in Europe at the moment, specifically in Ireland, about the mechanisms by which Facebook is transferring data to the United States. On either side of the Atlantic, there could be a pulling of the plug on that agreement.

On whether or not we should take account of that, I couldn't really advise, because we don't know what the future holds.

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

We'll now move to Mr. Kelly, who I believe is sharing his time with Mr. Jeneroux, if there is any.

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

Mr. Pat Kelly: We'll see how it goes.

If I may, I would like to start by asking Professor Geist about data localization.

You spoke about that in some detail, but I was intrigued by some of the things you said and would like to have you expand.

You spoke of localization being important for Canadians, if I understood you correctly. You named some large data collectors and spoke of the necessity or desirability of localized data in Canada, while recognizing the undesirability of data localization in countries —you named China—where restrictions on the transmission of data are problematic and controlled by the state.

Would not some of our other international partners perhaps have a problem with Canada appointing itself the arbiter of where localization is good and where it is bad? How do you think this would work in the eyes of the international community?

Dr. Michael Geist: Thanks for the question. Let me unpack it a little bit. You've talked, in a sense, both about data transfer and data localization, and they're different things.

The issue of data localization is with regard to a country requiring businesses to store or retain personal information locally, ensuring that that information enjoys the protections that their national laws provide. In fact, it is also what our national government has done as part of a process that was started by the Conservatives, and continued by the Liberals in terms of a cloud-computing strategy, recognizing that there might be some information held by government that we would not want stored on servers elsewhere.

What I think we are likely to see in NAFTA and what we saw in the TPP, largely at the behest of the United States since they represent some of the companies that tend to store large amounts of data and tend to store it in the United States, are attempts to preclude countries from adopting mandates to require that data be stored locally. We're certainly seeing some commercial impetus for doing so.

That's why those big companies have set up those servers in Canada. They're responding, in a sense, to market demand for better protection, but I would argue that Canada should certainly be free to say that for certain kinds of information, we want to ensure that it is retained in Canada so that Canadians know that it is adequately protected and subject to Canadian rules. I am expressing concern that as part of the trade negotiations, we may find attempts to override that.

That, I should note quickly, is different from restrictions on transferring data across borders. We've also seen the United States focus on stopping restrictions doing that, but as Professor Bennett just explained, the European Union has tried to do exactly that. They have tried to create restrictions on the ability to transfer data across certain borders.

Mr. Pat Kelly: Ease of transfer, though, begets differences in localization or where the data is stored. If it's easy to transfer data across a border, it can be stored elsewhere. Do they not...?

Dr. Michael Geist: There are two things. First of all, data always moves easily. If we take it as nothing more than ease in moving the data, then the concern will be that the data will move and be transferred to the lowest-level jurisdiction for protection. I don't know that many Canadians would be comfortable if they were told that many of the protections they think they enjoy are lost because their data is being stored in a jurisdiction with no privacy protections at all, and it would be very difficult for a privacy commissioner to assert jurisdiction.

Even in the context of data transfer, what we often find takes place in Canada is that you might send me an email, and if you're on a provider like Bell and I'm on a provider like Rogers, that data may actually transfer across borders and boomerang back into Canada. So the issue of even allowing data to go across borders—I grant you that it is easy to do—has been raised as a potential concern by some jurisdictions.

I wanted primarily to flag this issue of localization because we've seen a strong commercial impetus for it. We've also heard the Government of Canada talk about it, and we've started to see it enter into the lexicon of trade negotiations. Given what we've heard from the Trump administration, it seems quite likely that we'll see that resurface as part of the NAFTA renegotiation.

● (1700)

Mr. Pat Kelly: Thank you.

Mr. Fraser in his remarks about the Romanian extortion case made me think about this business of localization and the ease of transfer and the connection between the two. I'll ask anyone who would care to jump in and talk about the level of understanding, adoption, and adherence to PIPEDA as it stands now. Many of you have spoken of the desirability of strong penalties to encourage compliance. Owing to my having had a career in small business, I know there's a lot of awareness among business holders that there is a Privacy Act, that there is a desirability to comply, and that there is a fear of consequences for failure to comply. Apart from that, however, there is very little understanding of what any of this means.

I'll open that up to whoever would like to comment.

Mr. David Fraser: As somebody who practises privacy law on a daily basis and advises businesses, I think one thing that's notable—certainly it's been my experience and I've heard it anecdotally from others—is that the large banks, the large telcos, and the large Internet companies have squads of lawyers on staff. They have compliance people. They have international compliance people. In fact, their level of compliance is pretty high, although their risk threshold might be slightly different from that of a small or medium-sized business.

The level of awareness of the mechanics of how to actually comply with Canadian privacy law—how to get people's consent, how to manage all that, and how to protect information—is actually quite low in the very large portion of our economy. Here I refer to the SMEs across the board.

One thing I think is worth discussing—and I don't have a ready solution for it—is that although the Privacy Commissioner has done a lot of work with big banks, telcos, and Internet companies, how do you educate and reach those SMEs and incentivize them to protect Canadians' personal information better? I don't have an out-of-the-box solution for that.

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

We now move to Mr. Blaikie.

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

I'm interested in picking up on the conversation about our international partners and how much of Canadian privacy law ends up getting dictated in a trade agreement or by our desire to have easy transfer of information, as is the case with Europe. Presumably CETA was an opportunity to try to get some further protection—having Canadian privacy practices more formally recognized and having them less in doubt. It seems, though, to have been an opportunity missed.

To what extent, as things go forward with technology and trade agreements, do you anticipate these questions being decided by international trade partners instead of Canadian legislators? What's the interplay between Canadian law and the trade agreements?

Dr. Michael Geist: I'll give it a try. I don't doubt Michael and Colin may have responses, and David, too.

I'll quickly say that it is readily apparent that these issues have entered into the realm of trade negotiations. We saw it unquestionably within the Trans-Pacific Partnership, within the TPP. The Secretary of Commerce in the United States, Wilbur Ross, has talked about the need to address the digital economy as part of renegotiating NAFTA.

If you look at the e-commerce chapter in the TPP, you see there's a blueprint for the kinds of issues that we are likely to see come up within NAFTA. They include things like data localization and data transfer. I should note that they also included in the TPP a provision on countries being required to have a privacy law, but it was a very watered down version in light of the fact that the United States, while it has strong enforcement, doesn't have broad-based privacy rules.

I don't think there's any question that we're going to continue to face those pressures. In some instances that might be a good thing. David talked about what it would look like if the Privacy Commissioner were given order-making power. He suggested it would look like the Human Rights Commission. I would argue that it would look like just about everybody's privacy framework. It would look like the other privacy commissioners across the provinces. It would look more like what we see in the EU. It would even look like the Federal Trade Commission in the United States, where we do see order-making power and the ability to enforce the common approach in many other places. The outlier in this case, actually, is the federal Privacy Commissioner, who hasn't had those powers.

● (1705)

Mr. Daniel Blaikie: Does anybody else want to jump in?

Prof. Colin Bennett: I agree with that.

I'd just add one other dimension. It's something that I mentioned very briefly. In the politics of adequacy assessment, it is a political judgment, not just a legal judgment. I have a couple of points on this. One is that the Europeans really do want this system to work; they're not going to want the process of adequacy assessment to collapse. Therefore I think there would be a cost if, as I say, a country like Canada, a trade partner, were to lose its adequacy status.

Secondly, I would just reiterate that the whole issue about access by intelligence services and national security services, etc., to business-related data is also part of the equation. If you look at the EU-U.S. privacy shield, you see there's as much in that about that issue as there is about commercial transfers.

Mr. Daniel Blaikie: One of the things we've heard about PIPEDA is that it has a broad statement of principles. Would you think that it makes sense...? It seems to me that it wouldn't be right to constantly have Canadians' privacy rights on the table every time we get into a trade negotiation. You can end up trading Canadians' privacy rights for something that has nothing at all to do with those rights, but with the price of rice, or whatever. Do you know what I mean?

There are some things that seem not worth hawking because they're totally separate things. Forgive me for not having the legal background. When we talk about putting principles in legislation, if international trade is going to continue to be an important aspect for determining Canadians' privacy rights, would it make sense to have something like a statement in PIPEDA about government's seeking to defend the privacy rights of Canadians in trade negotiations, or to try to incorporate the principles of PIPEDA into trade agreements? Would this make sense rather than just leaving it an open question on whether this one department of government, when it goes off to negotiate trade agreements, cares about the mandate of other government departments mandated to protect the privacy of Canadians' personal information?

Dr. Michael Geist: I think the general principles do serve us quite well. But what we've experienced, especially as new technologies have emerged in recent years, is specific privacy legislation or regulation trying to address new concerns, whether identity theft, or spam, or some of the national security issues that have arisen. We're now likely to see some of these other new issues come up. We've even seen data localization at a provincial level pop up in a number of instances as well.

I think part of it is a matter of being live to the issue. If we look at the experience with the TPP, we see that the Australians were aware of exactly what I have been talking about. They obtained a side letter from the United States specifically addressing the potential for them to be be subject to EU demands on the one hand and U.S.-led demands in regard to the TPP on the other hand. Canadian negotiators, with all respect, seemed to be asleep at the switch and didn't raise the same kind of issue and didn't obtain the same sort of thing. Had the TPP, which now seems like it's dead, come to fruition, Australia would have protected itself in terms of data transfer issues and privacy protection; Canada would not have.

Mr. Daniel Blaikie: We don't typically expect—though, granted trade negotiation teams are large and have a lot of expertise—the negotiating team to be able to foresee everything when we burrow down into an issue either as a committee or in various government departments.

If trade agreements are going to be determinative of a particular kind of issue, does it make sense to build somewhere into the principles of a statute governing those protections for Canadians that it's a goal of the Canadian government to try to enshrine those same protections in international agreements? It's not something binding, obviously. It's not to say you can't sign a deal. There's always going to be give and take, but it's to try to build that into the framework so that it's something that Canadian trade negotiating teams are more likely to take note of. It raises a flag for them that these are questions you have to ask when you go to the negotiating table.

Does that make sense as a tool, to try to put that on the radar?

Dr. Michael Geist: What I would say makes sense for Canada is to open up the trade negotiations. If there was were a fundamental problem with the way the Conservative government, with all respect, negotiated CETA and the TPP, it was that it was done with an enormous amount of secrecy and then presented on a take-it or leave-it basis.

The TPP is dead. ACTA , which it negotiated, is dead, and CETA had to largely be renegotiated by the Liberals on key issues because of that secrecy. If we want to ensure that does not happen again when we talk about the NAFTA renegotiation, open these things up. The solution isn't to ensure that every negotiator knows the nuances of every single issue; the solution is to bring in many experts into the process through the negotiating process so that these issues get flagged as we're negotiating—not after the fact when it's too late to do anything about it.

● (1710)

The Chair: Thank you very much.

Mr. Erskine-Smith, please, for our last seven minutes.

Colleagues, this will take us past the point where bells will start to ring. I'll assume that we'll give Mr. Erskine-Smith his full seven minutes.

I'll need the unanimous consent of the committee to carry on past that if the bells start to ring. If we were to seek it, would we have unanimous consent? The votes won't start until 5:45. Or, would you rather just let Mr. Erskine-Smith wrap it up and be done with it?

Mr. Daniel Blaikie: Are you seeking unanimous consent to let him finish the seven minutes or to continue indefinitely past the bells?

The Chair: I'm going to let him finish his seven minutes. I'm seeking time beyond that.

Mr. Daniel Blaikie: I think we should wrap it up with—

The Chair: Okay, Mr. Erskine-Smith for our last set of questions, please.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thank you to all the witnesses.

I want to start with you, Mr. Fraser. You cast some doubt or expressed some caution with respect to our recommending the granting of new powers to the commissioner. Also, you mentioned procedural fairness, so I want to get your thoughts on this.

As far as I understand, some organizations already have the power to impose administrative monetary penalties, for example, FINTRAC; the CRTC with respect to the anti-spam legislation; the Ethics Commissioner; and in 2013, the U.K. Information Commissioner issued a $250,000 fine against Sony for a breach with respect to PlayStation. Are all of these models contrary to procedural fairness? Would they not face the same hurdles you've expressed?

Mr. David Fraser: I think all of them face the same issues and the same scrutiny, and I think many of them have addressed them in varying ways in order to incorporate that. Many of them build within their organizations particular firewalls to prevent the investigations from being tainted by the advocacy activities of the organization.

What I'm suggesting is that if you were to build a significant or real firewall, it would end up looking like the Canada Human Rights Commission or other sorts of models.

Mr. Nathaniel Erskine-Smith: To push back a bit, though, is that what the position of the U.K. Information Commissioner looks like? Maybe it does; I'm less familiar with that. But if that commissioner has have a capacity to level a $250,000 fine, that strikes me as more effective than the current powers our current commissioner has.

If you take a differing view, what is the problem with the U.K. commissioner's powers in terms of their model? But maybe you're not familiar with it.

Mr. David Fraser: No, I'm not familiar enough with the structure of the U.K. office.

Mr. Nathaniel Erskine-Smith: Okay.

You mentioned court damages in sections 14 and 16 of PIPEDA in relation to one another. Do you think court damages are sufficient deterrents? Here I would just note that the last case I really remember as a law student was Ward and the $5,000 in damages awarded for an illegal strip search. That struck me as a pittance for a severe privacy breach, so are court damages sufficient do you think?

Mr. David Fraser: Maybe one of the things to address is whether or not it's adequate that only one individual can go to court in connection with any particular complaint. But it's modelled on being compensatory, so a judge, an independent person, with all of the evidence in front of him determined, in that case, that $5,000 was adequate.

The Ontario Court of Appeal has said that the general damages available for harm to feelings in connection with a privacy breach range from a nominal amount to $20,000. Those are the damages that have been assessed by our legal system, which I don't have a whole lot of reason to question.

Mr. Nathaniel Erskine-Smith: One rationale for remedies is compensation and another is deterrence, so when we look at our recommendations with respect to empowering the Privacy Commissioner, it strikes me that greater deterrence is perhaps warranted.

You had some concerns with respect to the opt-in model that Mr. Geist had raised. When we had the Privacy Commissioner before us, he spoke of meaningful consent. If we do not go for an opt-in model, how do we improve the existing model to ensure meaningful consent?

Mr. David Fraser: There may, in fact, be a little bit of confusion. When you talk about privacy by default, where automatically, without the person doing anything else, they're going to follow the most privacy-protected thing, that is going to work on a whole lot of services, but it might not work on all.

In our legislation, as it's currently drafted and if properly implemented, the second principle says that you have to identify the purposes for processing, collection, use, and disclosure of personal information.

The next principle says you have to get consent, and we now have a clear articulation that consent has to be meaningful. There is some flexibility in that the form of the consent has to be based on the sensitivity of the information, and that doesn't necessarily mean you only get opt-in consent for the most sensitive stuff. It's a continuum. There are certain things that are inherent in the use of a service that are just kind of part and parcel—do you need an affirmative check box? If I go to Chapters-Indigo and order a book, do I have to opt in for them to use my address that I've just given them to ship me the book? It's completely obvious in that transaction, and you should be able to imply that consent, but secondary use, for example, using my name and address for marketing purposes for some other purpose, seems to be a sensible opt-in.

One of the great things about the legislation is the fact that it's based on principles and that it's relatively fluid, and it's going to work in the Chapters model, in a bank model, and in a telecom model.

● (1715)

Mr. Nathaniel Erskine-Smith: This will be my last question. You mentioned the importance of choice and not deviating from the consent model for that reason. It strikes me, as terms of use get more complicated and we're opting into so many different services, that there is an existing model already in Ontario that has lasted for decades. In the Sale of Goods Act we talk about implied warranties, and there are standard terms the consumers cannot opt out of; businesses cannot allow consumers to opt out of them, for consumer protection. Do you think the same principles could apply with respect to privacy?

Mr. David Fraser: I'm not sure you'd find it a complete analogue, and I would hesitate to bake something into concrete when the technology is going to move and consumer expectations are going to move. But I do think it does make some sense to have some "if these are your default practices", so "this is your standard terms of use", or "this is kind of a standard privacy policy", which is an expectation that you don't need to do anything additional to get additional consent. But if you deviate from that, then perhaps it does make some sense to bring that to the individual's attention. Among the defects that are identified, I don't think a lot of companies are fulfilling their obligations under PIPEDA well enough with regard to identifying purposes. We could all do a better job. There is discussion of short-form privacy notices, like the nutritional labels, just-in-time notification, which is something I advise my clients about—nobody is going to read your privacy policy. You can't rely on that to be the foundation for your identifying purposes and consent. When you have a form and you're asking for information, you have to make it clear to your consumers at that time what you are going to do with that information. Otherwise privacy policies are just a legal fiction.

The Chair: All right, colleagues, the bells haven't started yet, but I'm looking at the screen and the Speaker is reading the terms of the motion right now, so the bells will start momentarily. We will operate on that assumption.

First of all, I would like to apologize to our witnesses. These things happen from time to time, but thank you very much for your consideration and patience as we deliberated today.

If there is anything else you think we should know, or some answers you wish in hindsight that you had given us, please submit that information to the committee, and please follow our progress on the study of PIPEDA. If anything else comes across your mind that you think would be to the benefit of all Canadians, please let us know.

Thank you very much.

The meeting is adjourned.