HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 054 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, April 4, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, April 4, 2017

● (1610)

[*English*]

The Vice-Chair (Mr. Daniel Blaikie (Elmwood—Transcona, NDP)): We're going to bring the meeting to order.

I want to explain something for the benefit of our witnesses that may seem a little confusing. I'm chairing the meeting today. I'm the second vice-chair, and I'm the only NDP member on this committee, so for the time when an NDP member would normally ask questions of you, I'm going to my seat over there, and we will have another member of the committee sit in the chair. It's going to be a little bit of musical chairs. I want to make sure that everyone understands why that is the case.

Thank you all very much for coming today. We have David Young, the principal at David Young Law; Robert G. Parker, advisory consultant with Risk Masters International Inc.; Ian Kerr, professor and holder of the Canada research chair in ethics, law and technology at the University of Ottawa; and Vincent Gautrais, full professor, director of the Centre de recherche en droit public, Faculty of Law, Université de Montréal.

Thank you all for coming here today. We're starting late, so we'll just jump right in.

Mr. Young, would you like to start with your presentation? We have 10 minutes each for presentations. We'll do all four and then go to questions.

David Young (Principal, David Young Law, As an Individual): Good afternoon, Mr. Chair, and members of the committee.

Thank you for the invitation to appear before you, and to present my views in connection with your study of the Personal Information Protection and Electronic Documents Act, PIPEDA. I have provided a written submission to the committee in which I elaborate on my comments today, and address certain other issues, in particular the right to be forgotten and the European Union's adequacy requirements. I refer you to that submission for my thoughts on those two issues.

By way of introduction, I am principal at David Young Law, a privacy and regulatory counsel firm. As a privacy lawyer, I have been advising organizations in both the public and private sectors, as well as individuals, since before PIPEDA became law. I'm a member of the Canadian Bar's national privacy and access law section, and have worked on the section's responses to both the first review of PIPEDA and the current review; however, I want to make clear that the views I express in my submission and here today are my own.

This review is taking place at a particularly apt time. Issues surrounding privacy are very top of mind in today's digitally oriented world. I propose to address specifically two issues: consent and enforcement.

First, the issue of consent. Consent is the key precept of Canada's private sector privacy laws. It says that individuals have the right to control the collection, use, or disclosure of their personal information, subject to limited exceptions. My basic view is that the current PIPEDA consent rule should not be adjusted or qualified in the statute, with the understanding that its application to evolving contexts will be elaborated through practice, responding to the ever-changing realities of information use.

It would be very difficult in an amendment to PIPEDA to try to articulate the precise going forward needs and mechanics to somehow anticipate the dictates of a fast-changing digital world.

The Office of the Privacy Commissioner's current consultation on consent is a timely undertaking. The results of this consultation should enable the OPC to provide guidance and develop principles to ensure that consent continues to operate effectively as the key rule in PIPEDA. It should also be noted that the courts, including the Supreme Court of Canada, have considered issues of consent, and have made clear that it is inherently subject to important qualifications, including the right of freedom of expression and a reasonable application of the role of implied consent.

Some of the adjustments to the rule that have been suggested would weaken its rigour, and potentially open up the scope for much more extensive collection of personal information than exists today. This, I believe, is what the Privacy Commissioner's consultation is likely to conclude. Also, any such weakening could threaten PIPEDA's adequacy status under the European Union's new privacy rule, the general data protection regulation, GDPR, of which I know you've heard a lot of discussion.

In my view, PIPEDA's current consent rule is flexible enough to respond to the needs of evolving information practices and innovation, and should be maintained. The key objective is to ensure that individuals continue to have the right to control and protect their information.

The second issue I want to address is the enforcement model. There's been much discussion about enhancing the enforcement powers of the Privacy Commissioner. As we know, the commissioner's current role is that of an ombudsperson. PIPEDA's remedial provisions direct him to investigate and deliver reports on complaints made to his office.

These requirements currently do not include any authority to order an organization to take remedial actions. I believe that his authority, as exercised through this mechanism, has been very effective. The commissioner does exercise what, in effect, are order-making powers through his authority to make findings, audit organizations, and make recommendations, and as will be available under the recent amendments to PIPEDA, to enter into and enforce compliance agreements.

● (1615)

Furthermore, the commissioner has the power to publicize privacy transgressions and name offending parties. This is essentially the model that has been used by the provincial privacy regulators, with the exception of a formal order-making power. I believe that in terms of effective enforcement, the model is working well.

All this being said, if it is determined that the current model does not provide sufficient enforcement tools, I believe it would be possible to supplement the commissioner's existing powers with an authority to make binding recommendations, in other words, orders. This authority should not undermine the framework of the commissioner's complaint resolution role, which, in essence, is compliance oriented.

A further proposal mentioned is to provide the commissioner with a power to impose fines. You have heard that this power exists under the provincial privacy jurisdictions and around the world. Firstly, I would note that PIPEDA currently does include provision for fines that, once the current amendments come into force, will include failure to report a breach. Secondly, none of the provincial private sector privacy laws contain a provision permitting the regulator to impose a fine or monetary penalty. What some of them do—and the Alberta law is an example—is provide for an offence punishable by a fine for intentionally breaching the law. Actually, I think Alberta is the only one that has that specific provision in it. Under these provisions, prosecuting an offence is the responsibility of the law enforcement authorities, not the regulator.

The international sphere is different. We are aware that in Europe, for example, the regulators have the power to impose financial penalties, and have done so for privacy breaches in some instances in the millions of dollars.

Canada does have experience with legislation imposing such financial penalties, specifically the Competition Act and Canada's anti-spam legislation. However, I suggest that to date our experience in the privacy area does not equate to the type of transgressions sought to be addressed under those laws.

Providing the Privacy Commissioner with the power to impose financial penalties would be a dramatic departure from his existing authority and would not be consistent with an ombudsperson model. However, if deemed appropriate, it would be possible to supplement the current PIPEDA offence provisions to include financial penalties for matters such as an intentional breach of the law. Such a provision would be consistent with the pending offence for failure to comply with breach reporting requirements.

As a final note, I agree that reference to the new EU privacy rule, the GDPR, should be included in the committee's study. However, as it stands today, significant changes to PIPEDA to respond to the GDPR would be premature. A more precise view may be revealed going forward as we have more experience with the GDPR and its transborder adequacy review process. With the GDPR's added focus on law enforcement and national security agencies, adjustments may be required to enhance protective mechanisms regarding access to databases in our country by such bodies.

In the early days of PIPEDA, I heard many criticisms that the law was not well oriented to clear legal guidance since it relied on principles as opposed to prescriptive rules, based as it is on a code intended originally for voluntary compliance. However, the law has clearly stood the test of time, and in my view, its unusual origin provides it with the flexibility to respond to the constantly changing needs of technology and the digital environment of today. This understanding colours very much my view as to what amendments should be considered in this current review.

Thank you again for giving me the opportunity to present my views.

● (1620)

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

Mr. Parker.

Mr. Robert Parker (Advisory Consultant, Risk Masters International Inc., As an Individual): Thank you.

My name is Robert Parker. I'm a retired partner with Deloitte & Touche. I first got involved in privacy in 1995 on an ISO privacy task force. Subsequent to that, in 2000, I joined the initiation of the Canada-U.S. privacy task force that developed generally accepted privacy principles, and most latterly, the privacy or maturity model.

I started a privacy practice at Deloitte, and when I retired in 2005 we had 40 people, 15 full-time and 25 part-time, in our privacy practice.

As mentioned, I'm with Risk Masters International, LLC. We're a group of four retired partners, three in the United States and myself in Canada. We do risk management work, including privacy work. We have a privacy course that we teach in the United States, dealing with United States health care privacy requirements.

I appreciate the opportunity to present some thoughts to the committee and I look forward to the discussion.

I've identified seven areas, and I realize that's a little more than the two that David identified. I would like to focus on just four of them.

I'm going to pass by privacy breach notification. I think we need to do some ramping up of the privacy breach notification requirements and rules, and to specify the obligations and rights of either party if there is a privacy breach. I dealt with this with a U.S. company, which is a global corporation, in terms of how they were dealing with privacy breaches for both electronic and hard copy documents.

Meaningful and effective consent has been discussed in a number of the documents. The issues here seem to be along the lines of front office versus back office. The centre for democracy and information did a study that showed that there's a total disconnect between what you tick on the form or what you click on the website and what happens in the back office. In the back office, they have to change their databases to be able to record that consent. They have to change every application program that looks at that database to test for that consent and then they have to act on it accordingly. That's a huge task, and a lot of organizations have just blown right past that. That's why there is a disconnect between what people consent to and what they are often given.

The last one is the ownership of non-provided personal information and who owns that. There was a court case—and I'm not a lawyer—in Ontario a few years ago. It was a very narrow case so it couldn't be taken as precedent, but it dealt with human tissue. It said that the human tissue taken from a person, once taken from them, belonged to the hospital and not to them. I think some clarification on non-consent issues like that would be helpful.

Of the four I want to talk about, the first one is collection versus retention, use, and disclosure. With the change in society right now, we have a number of individuals, millennials, and so on, who will give all of their information away. They post what they ate for breakfast on Facebook and they go to Twitter. They're very free about their information. They don't see some of the problems that other groups in society and other demographics happen to see. Perhaps the idea or the issue is not so much collection, but retention, use, disclosure, and security over that information.

In 2005, after the London subway bombings, they could go back six months and see who that person met with. They followed it all up and were successful in identifying a number of the perpetrators.

In Ontario, the initial ruling was that the TTC could keep them for 72 hours. If they didn't need them after 72 hours.... I realize that in all the legislation there is the national security clause, which would allow you to keep them longer, but a lot of people are keeping information. They're collecting it and keeping it for a long period of time, and that's even expected to go back years for an email or a piece of correspondence.

● (1625)

If we look at that, maybe collection is not the issue as much as retention, use, and disclosure, as well as how we secure that and nail it down really tightly so that it is not used in an inappropriate manner. That's the first big one: collection, use, and disclosure.

The second one is the Internet of things, and that's where we're using IP protocol to drive “things”. They could be mechanical things. They could be system things. It doesn't matter what it is.

I'll give a couple of examples. Your car, if it's newer, has an engine management module. That engine management module will record a lot of things, including acceleration rates, deceleration rates, how fast you were going, etc. Is that personal information? Could your car tell people? The mechanic can gain access to it, but so can police. In fact, an insurance company in the United States is saying if you will give them access to that, they'll lower your premiums, under the belief that they wouldn't have jackrabbit starts, fast braking, and excessive speed. Is this personal information? That's one example.

Your dashcam would be another example. Is that personal information? Can the police seize it? Do they need a court order, etc.? There's a whole lot coming out in this Internet of things, which I think we should take a look at when we look at the legislation.

The third one out of the four is digital exhaust. “Digital exhaust” can be loosely defined as what's left over after the power is put on. You consummate an Internet transaction and there's all this digital exhaust, like what time the transaction occurred, what happened here, what happened there, who was involved, what the mailing address was—all of that information. That can be resold, and certain people are reselling it in the United States. You might have seen the Federal Communications Commission issue over the weekend that dealt with part of that.

What we have here is this digital exhaust, this secondary information about the transaction. Is that yours? Does that belong to the organization that has collected that information about you? What rights do you have over the use of it, and particularly, over their selling it to other parties who would say, “These are your behavioural patterns,” and issues that you would not, perhaps, want them to deal with?

The fourth one is the adequacy and appropriateness of security. When we look at the first one, about having to nail down all this information if we're going to collect more information, now we have to have security there. The problem is, we're building higher walls, and we're building thicker walls, and we're building deeper and wider moats, and they aren't working. The bad guys still get in. There still are data breaches.

A couple of partners in Pricewaterhouse in the United States suggest a paradigm shift. That is, we let everybody in. You know, "Keep your friends close but your enemies closer." You would build a profile about everybody who visited your website, and you would look at what they did and what an expectation model was. Combine this with big data and you would be able to create a profile on these people. If they went outside that profile, then you could stop it right then and there.

We don't have a fortress mentality. We need a different paradigm shift to look at that, but that means we are collecting information about identifiable individuals, and we're building profiles on each and every one of them. Is that something we want to do, or is that something we want PIPEDA to look at? That's coming down the road, the new paradigm shift in how security is going to happen.

Those are the four key topics. I'm pleased to answer any questions on the three subtopics at the end of this session.

● (1630)

I will mention generally accepted privacy principles. Generally accepted privacy principles were developed by a joint Canada-U.S. task force. Fortunately, because Canada's on it, it's published in both official languages, so it's readily available and I can get copies for the committee. It has 10 principles and 72 criteria, and it's very prescriptive. It deals with breaches. It deals with notification and so forth. It's a very prescriptive document at a very high level. Because it was so prescriptive, we went on to the privacy maturity model. The privacy maturity model takes the CMM, the capability maturity model—Carnegie Mellon and the U.S. Department of Defense—and we put that together into a privacy maturity model which says how an organization should go through....I can send that to you as well.

Thank you for your time. I know I've used my 10 minutes and a few seconds, but I appreciate the opportunity. As you might feel, I'm passionate about privacy.

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

We're going to proceed now to Professor Kerr.

Professor Ian Kerr (Professor and holder of the Canada Research Chair in Ethics, Law and Technology, University of Ottawa, As an Individual): Mr. Chair, honourable members, thank you and good afternoon. I appreciate the opportunity to appear before you today as part of your PIPEDA review, a statute in desperate need of legal reform.

My name is Ian Kerr. I'm a professor at the University of Ottawa, where I hold a unique four-way position in the Faculty of Law, Faculty of Medicine, school for information studies, and the department of philosophy. For the past 17 years, I have held the Canada research chair in ethics, law, and technology. Canada research chairs are awarded to "outstanding researchers acknowledged by their peers as world leaders in their fields."

I come before you today in my personal capacity.

I'd like to begin by reinforcing some points that have already been made in previous testimony.

First, to put it colloquially, and to disagree with my colleague David Young, the call for stronger enforcement through order-making power, the ability of the OPC to impose meaningful penalties, including fines, is by now a total no-brainer.

As Micheal Vonn of the BCCLA who recently testified before you said, "There is no longer any credible argument for retaining the so-called ombudsperson model". This has already been acknowledged by Commissioner Therrien, former commissioner Stoddart, and assistant commissioner Bernier, and has been fortified by testimony from other Canadian jurisdictions that already have order-making power, which commissioners Clayton and McArthur have testified before you as being advantageous. Strong investigatory and order-making powers are a necessary component of effective privacy enforcement, especially in a global environment. Let's get it done.

Second, I agree with former commissioner Stoddart and with overlapping testimony of Professor Valerie Steeves, both of whom have stated that PIPEDA's language needs to be strengthened in ways that reassert its orientation towards human rights. As Professor Steeves attests, privacy rights are no longer reducible to data protection, which itself is not reducible to a balancing of interests. Enshrining privacy as a human right, as PIPEDA does, reflects a profound and crucial set of underlying democratic values and commitments. Privacy rights are not merely trade-offs for business or governmental convenience. PIPEDA needs stronger human rights language.

Having reinforced these views, the majority of my remarks will focus on two central themes raised by this study, transparency and meaningful consent. I will use this framing language to orient your thinking, but in truth, both of these concepts themselves require expansion in light of dizzying technological process.

When PIPEDA was enacted, the dominant metaphor was George Orwell's *1984*, "Big Brother is Watching You." Strong privacy rights were seen as an antidote to the new possibility of dataveillance, the application of information technology by government and industry to watch, track, and monitor individuals by investigating the data trails they leave behind through their activities. Though perhaps no panacea, PIPEDA's technology-neutral attempt to limit collection, use, and disclosure was thought to be a sufficient corrective.

However, technological developments in the last 17 years since PIPEDA go well beyond watching. Today, I will focus on a single example, the use of artificial intelligence, AI, to perform risk assessment and delegated decision-making. The substitution of machines for humans shifts the metaphor away from the watchful eye of Big Brother towards what Professor Daniel Solove has characterized as:

> ...a more thoughtless process of bureaucratic indifference, arbitrary errors, and dehumanization, a world where people feel powerless and vulnerable, without any meaningful form of participation in the collection and use of their information.

This isn't George Orwell's *1984*; this is Franz Kafka's trial of Joseph K.

Since the enactment of PIPEDA, the world we now occupy permits complex, inscrutable artificial intelligence to make significant decisions that affect our life chances and opportunities. These decisions are often processed with little or no input from the people they affect, and little or no explanation of how these decisions were made. Such decisions may be unnerving, unfair, unsafe, unpredictable, unaccountable, and unconstitutional. They interfere with fundamental rights, including the right to due process and even the presumption of innocence.

It's worth taking a moment to drill down on some real-life examples. IBM Watson is used by H&R Block to make expert decisions about people's taxes. At the same time, governments are using AI to determine who is cheating on their taxes.

● (1635)

Big Law uses ROSS to help its clients avoid legal risk. Meanwhile law enforcement agencies use similar applications to decide which individuals will commit crimes and which prisoners will reoffend. Banks use AI to decide who will default on a loan. Universities use AI to decide which students should be admitted. Employers use AI to decide which people get the jobs, and so on.

But here's the rub. These AIs are designed in ways that raise unique privacy challenges. Many use machine learning to excel at decision-making. This means that AI can go beyond its original programming to make discoveries in the data that human decision-makers would neither see nor understand.

This emergent behaviour is what makes AI so useful. It's also what makes it inscrutable. Machine learning, knowledge discovery in databases, and other AI techniques produce decision-making models differing so radically from the way that human decisions are made that they resist our ability to make sense of them. Ironically, AIs display great accuracy, but those who use them and even their programmers often don't know exactly how or why.

Permitting such decisions without an ability to understand them can have the effect of eliminating challenges that are essential to the rule of law. When an institution uses your personal information and data about you to decide that you don't get a loan, your neighbourhood's going to be the one under more police surveillance, you don't get to go to university, you don't get the job, or you don't get out of jail, and those decisions can't be explained by anyone in a meaningful way, such uses of your data interfere with your privacy rights.

I think this is the sort of reason that a number of experts have come before you to talk about what they called algorithmic transparency, but in my respectful submission, transparency doesn't go far enough. It's not enough for governments or companies to disclose what information's been used or collected when AIs affect our life chances and opportunities. Those who use AIs have a duty to explain those decisions in ways that allow us to challenge the decision-making process itself. That's a basic privacy principle that's enshrined in data protection worldwide.

I would therefore submit that PIPEDA requires a duty to explain decision-making by machines. A duty to explain addresses transparency and consent but goes further in order to ensure fundamental rights to due process and the presumption of innocence. This is the approach that's taken in GDPR. I would go even further, following EU GDPR article 22, and suggest that PIPEDA should also enshrine "a right not to be subject to decisions based solely on automated processing".

PIPEDA was enacted to protect human beings from technological encroachment. Decision-making about people must therefore maintain meaningful human control. PIPEDA should prohibit fully automated decision-making that does not permit human understanding or human intervention, and to be clear, I make this submission not to ensure EU adequacy but because it's necessary to protect human rights.

Mama raised me right. Among other things, she taught me that you don't accept a dinner invitation and then complain to your hosts about what is being served. Mama's gentle wisdom notwithstanding I would like to conclude my remarks with two uncomfortable observations.

First, as I appear before you today, I think it's fair to say that my sense of déjà vu is not unwarranted. With the exception of a few new points like my submission in favour of a duty to explain, much of what I have said, indeed much of what everyone who has appeared before you has said, has all been said before.

Although many honourable members of this committee are new to these issues, those who have done their homework will surely know that we've already done this dance in hearings around Bill S-4, Bill C-13, the Privacy Act, the privacy and social media hearings, and of course the PIPEDA review of 2006. Yet we see very little in the way of substantive legislative change.

Although ongoing study is important, I say with respect that you are not Zamboni drivers. The time has come to stop circling around the same ice. The time has come to make some important legislative changes.

Second, as I prepare for the question period, I look around the table and pretty much all I see are men. Inexplicably, your committee itself is composed entirely of men. Yes, I realize that you have called upon a number of women to testify during the course of these proceedings. This, of course, makes sense. After all, a significant majority of privacy professionals are women. Indeed, I think it's fair to say that the global thought leadership in the field of privacy is by majority the results of contributions by women.

● (1640)

I find it astonishing and unjustifiable that you have no women on this committee, a decision to me as incomprehensible as many of those made by algorithms.

I feel compelled to close my remarks by making this observation a part of the public record.

Thank you for your careful attention. I look forward to questions.

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

[*Translation*]

We'll now hear from Dr. Gautrais, full professor and director of the Centre de recherche en droit public at the University of Montreal's faculty of law.

Dr. Vincent Gautrais (Full Professor, Director of the Centre de recherche en droit public, Faculty of Law, University of Montreal, As an Individual): Thank you, committee members.

My name is Vincent Gautrais. I'm a law professor and lawyer, and the director of the Centre de recherche en droit public at the University of Montreal. I have the L. R. Wilson Chair in Information Technologies and E-Commerce Law.

I'm very pleased to be speaking for the second time before this committee regarding issues related to the Personal Information Protection and Electronic Documents Act, and to be participating as a Canadian in this democratic exercise.

Last time, in June 2012, the committee invited us to provide a general response to the legislation. This time, Mr. Therrien's letter dated December 2, 2016, is guiding us through certain points to consider. Therefore, I'll refer to the four topics presented in his document. For my first ten minutes, I'll focus on the first point regarding consent. I've worked a great deal on the electronic contract issue. It was the subject of my doctoral thesis, in another century, about 25 years ago.

I think, and with regard to certain proposals presented before, the current situation is relatively ridiculous. Many people have made this unfortunate observation. There's hardly any debate. We know that nobody reads privacy contracts or has a reasonable possibility of reading them. There's no space limits for contractual content on a screen. The contracts are therefore extremely long. While the Supreme Court is proactive and creative in many cases, it didn't seize the opportunity to fight against this clearly detrimental practice in 2007, during the Dell Computer case. It's too bad.

It's too bad since, over time, consent has lost its initial purpose or initial goal. At first, it was designed to protect individuals by giving them some control over their own data. Instead, consent has become a way to protect the companies that use the data. Companies can now completely free themselves of any contract by burying their obligations and methods in page after page. Information is like oxygen. Yes, it's necessary, but when there's too much, you can't breathe anymore.

In light of this failure, what should we do? On that note, I want to introduce three elements. The first is the format. It's possible that things would be better and that individuals and citizens would be better protected if they had to formally express their intention and if the user had to accept a de facto situation first. That's the debate between opt out and opt in, which has already been presented to you, the committee. I think the debate underscores the classic opposition regarding the matter, since the second term, opt in, provides more protection than the first term.

Unfortunately, although I've liked the idea for years, I think the opt in solution has a few limits. Even a clear contract remains inaccessible to the average person. The contract is inaccessible as a result of its length, the fact that we don't read the same way on a screen, the very complicated legal terms, the hyperlinks that constitute invitations to “get out” of the contract, and so on. The process moves fast, and internet users are expecting that speed. In addition, the functional illiteracy rate often makes it unrealistic for people to read contract clauses. The promotion of the opt in solution first and foremost emphasizes the expression of consent and, to a lesser extent, beforehand, the contract's readability.

Recently, an American researcher showed that clickwrap, which involves clicking an “I accept” button, rather than the frequent browsewrap, which involves having the privacy policy somewhere on the company's website, had practically no impact on whether a document was read. The researcher showed that only 0.36% of people read the contract further, which again, is negligible.

In that sense, the appearance of strips—you've all seen them—at the bottom of websites, which indicate that users accept those infamous cookies, is seen more as an irritation to the reader rather than as a tool to protect the individual.

● (1645)

Second, this wariness regarding consent can also be verified on its merits. I don't think we can consent to everything. In contract law in general, even though there are rules for abusive clauses, for example, this situation is rarely verified when it comes to the protection of personal information. The consent clauses currently available on the Internet are filled with stipulations that clearly go against the interests of individuals. Judges rarely verify these clauses.

What happens when a company asks an internship candidate—this has already happened in a lawyer's office—to consent to providing his Facebook password so that the company can find out what the candidate has written on his profile? An actual study showed that 48% of users would be ready to exchange their password for a chocolate bar. However, we can't consent to everything, and I think we need to have some control over certain parts of the contract.

Third, regarding consent, in some situations, consent can't be provided in practice. This is true for artificial intelligence. I want to challenge a company to properly explain to its users how their personal information is used in the context of big data. That's why, in terms of the deconstruction of this contractual reflex, the cases where consent isn't necessary or required must be increased. For example, sections 67 and 68 of Quebec's Act respecting Access to documents held by public bodies and the Protection of personal information mention cases where so-called "information-sharing agreements" allow for the use of personal information without the consent of the people concerned. Therefore, the two bodies agree on the use of data.

Rather than asking for almost fictional consent, it would be better to present the case to Office of the Commissioner representatives, specialists, and privacy experts. They are best suited to assess the guarantees the company wants to provide to compensate for the use of the data. Your committee proposed this information-sharing agreement solution for the public sector legislation, the Privacy Act, in a recent report dated December 2016, in paragraph 2.2, recommendations 4, 5 and 6.

Through these three areas of examination, namely, the format, the substance, and the release from consent cases, we've tried to make consent less sacred. As noted by a British writer, we need to leave behind "contractual fetishism".

This brings me to my second point, which will be much shorter, given the lack of time. You'll have understood that I tend to think users have limited control. Individuals can't do much. They can do a bit when it comes to the contract, but not much. Also, where should this control be exercised?

As mentioned by a number of previous speakers, obviously we must have—it's a no-brainer, as Mr. Kerr said—an Office of the Privacy Commissioner whose powers are much more significant than the Commissioner's current ones. The Office of the Commissioner is able to negotiate changes in attitude with regard to international players, and it did so very well with Google and Facebook. However, the current legislation is known for its incredible inability to allow the Office of the Commissioner to take action, in comparison with the legislation of other organizations.

I think the Office of the Commissioner's powers should be increased. The increase must result in the ability to impose financial penalties, as mentioned by a number of people. These penalties could have a more specific impact on reputation. Surprisingly, unlike the vast majority of legal decisions in Canada, the Office of the Commissioner's decisions are anonymous and the names of the companies never appear and are redacted and hidden.

I won't address the third point regarding online reputation. First, this issue has been widely discussed. Also, when I spoke in 2012, I was able to raise concerns regarding the notion of the right to be forgotten. We should be very wary of how this notion can be applied and of its impact on other fundamental rights and freedoms.

Lastly, I want to say a few words about the adequacy of articles 25 and 26 of the 1995 European directive and now article 44 and the subsequent articles of the 2016 European regulation.

● (1650)

It's certainly important to consider working more closely with our European partners. The perception of privacy in that region is interesting. However, I think we shouldn't be too dazzled by how privacy is viewed in Europe. Privacy is a cultural issue, and this view differs from our own. We can look at what's going on in Europe, but we must maintain our Canadian identity.

In short, we need to further integrate the new technology, make consent less sacred, maintain our Canadian identity and ensure the legislation is somewhat less "decorative" in terms of penalties.

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

[*English*]

Mr. Bratina.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): Thanks, gentlemen.

My mind is just spinning because I don't how we're going to come out with a simple, agreed upon set of facts that we can move forward on. We already have a difference of opinion, as expressed by Mr. Kerr.

Mr. Young, I'd like to hear you defend your position against what Mr. Kerr said.

Mr. David Young: Thank you. I was actually thinking about that as Ian made his case.

There are a couple of things. I don't think we disagree in the essence of the ethic we're looking for, which is control. I use that word. That's what our law is right now, it's control of your personal information. It may be honoured in some ways in the breach today. In fact, you could probably make a case that it's honoured a lot in the breach with big data. In my comments in my submission I give some examples of that and, really, a lot of what Ian is talking about with AI and other research that he's done resolves down to big data. So what's the practicality?

I will say...and I think in essence much of what our colleague at the Université de Montréal is saying is, I don't disagree with it. We have to protect that. I do disagree with the professor. I know you asked me to respond to Ian, but notice is not the solution. Notice is the public sector rule. That's what the professor has alluded to. You just have to give notice, and then you can do whatever you want.

That's what we've got today with the so-called opt-out rule. You give notice, and if you don't like it, you opt out. If the notice isn't adequate, you may not have enough information to opt out or you may not have the opportunity to opt out.

Coming back to your question, I think the consent rule we've got is very strong. It really should be applied. I made the point, I'm not saying we couldn't build into PIPEDA some actual mechanisms to enhance either that rule or address some of the machine learning issues that Ian has raised, but I think the realistic way to do that is through Privacy Commissioner guidance. The commissioner has done a wonderful job. In fact, we're guided in Canada. I'm not trying to minimize our authority at all, but the FTC in the United States, the Federal Trade Commission, which has no privacy law, no general privacy law, has done a phenomenal job, and we listen to it and we are guided by it. The commissioner is guided by it.

Developing mechanisms that can address the issues is frankly the way I would respond to Ian's issue. I don't disagree that you shouldn't have unpredictable results occurring because somehow your data has been amassed with everybody else's, and boom, they're determining something about you that you didn't expect. I totally am on speed with that. The bottom line is, I don't think that's something we could put into PIPEDA as a statutory rule.

● (1655)

Mr. Ian Kerr: Mr. Bratina, if I understood your question correctly, you were asking to speak to the difference on the enforcement issue—

Mr. Bob Bratina: Yes.

Mr. Ian Kerr: —on the powers issue, so I'll speak briefly to that.

Mr. Bob Bratina: That's fine.

Mr. Ian Kerr: I think I'll speak also to the consent issue as raised.

Mr. Young notes, I think quite correctly, that the FTC has done a phenomenal job, despite having to be very sector-specific, not having omnibus legislation in the way that we do. One of the main reasons the FTC has done such a spectacular job is that they have big sticks—they have order-making power and enforcement ability, including the ability to impose fines.

I'd like to give an example that speaks to that. I think it also goes to the consent issue, because my understanding of what Professor Gautrais was trying to say had to do with dismantling some of the fictions around consent and the problems with privacy as a contractual consent model.

In 2009, the students from my university's technology law clinic brought a complaint to the Privacy Commissioner of Canada. The complaint was regarding Facebook in particular, and its privacy practices. As a result, the commissioner made a full investigation, came to a decision, and made some recommendations. Of course, not having order-making power or the ability to impose fines, she could only make recommendations.

What was interesting, as the world watched Facebook's response to that, was that Facebook decided as a result, or at least in coincidence, to put forward privacy settings for the first time. This was back in 2010. The world was shocked that in response to some of these complaints about privacy, Facebook listened and put in privacy settings, which allowed people to adjust their settings as they wished. This could perhaps be seen as giving people the power to control their privacy.

Interestingly, what actually happened was that Facebook, which had many psychologists in its employment, recognized that 88% to 92% of the people who use Facebook would never change their privacy settings. As a result, the way those privacy settings were put forward was the single biggest data grab in history, and I don't think there's been anything like it since. It was all based on consent and control.

I think what we see in situations like that is the fact that the Canadian Privacy Commissioner, or the commissioners around the world, didn't coordinate with this order-making power and the ability to impose fines as we start to see them do today. It's precisely why Facebook could get away with that.

It's important to note that Mark Zuckerberg does not adhere to the same settings that he set for the rest of the world. He's changed his privacy settings, knowing that he would be among the roughly 18% of people who would change their privacy settings. I think the story is telling, both from the perspective of order-making power and from the perspective of the illusion of control and consent that we have in privacy law.

● (1700)

Mr. Bob Bratina: I was going to ask about the notion of principle versus proscription, and whether or not we just need a Ten Commandments kind of law, as opposed to the details we can never seem to agree on.

Mr. David Young: That is what PIPEDA is. It has 10 principles. It has a useful supplementary explanation, which actually becomes guidance.

The Vice-Chair (Mr. Daniel Blaikie): Mr. Jeneroux.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, Mr. Chair, and my thanks to all of you for being here, including Mr. Gautrais, who is with us virtually.

Mr. Gautrais, I'm going to start with you, if you don't mind. I'm also going to press you a little bit on some of the comments you made just towards the end of your comments. You appeared at this committee in 2012, and you spoke of:

> establishing a strictly minimalist approach in legislation, without developing, in my opinion, any new concepts. We have seen such concepts in Europe—including the "right to forget", which was developed in a number of European pieces of legislation and seems to me overly difficult to apply.

Now, some time has passed since 2012. Particularly, we have the European Union's general data protection regulation coming into force in 2018. Have your opinions changed on that? You touched on it a little bit, but I was hoping you'd get into a bit more detail.

[*Translation*]

Dr. Vincent Gautrais: I can see you're well prepared, because you made comparisons. Thank you for mentioning this. Honestly, I don't think there's any change in position. In terms of privacy, but also the other areas affected by digital technology, each change in legislation has resulted in a very serious problem. This has already been mentioned, specifically by Mr. Young.

I think the principled approach in the legislation is quite good. That said, regarding the strengthening of the sanctioning powers of a monitoring body, such as the Office of the Privacy Commissioner, I didn't mention this possibility five years ago. The Office of the Commissioner did a very good job of changing things, as in the case of Facebook in 2009. In 2009, the Canadian Office of the Commissioner changed practices around the world. This is incredible, given that the legislation isn't very strict and contains very few constraints. I think we could still make things easier, because privacy has become more significant and the risks are more significant. The major change would involve the need to strengthen an organization's powers. I think that's the only important major change. However, the principled approach, apart from the consent matter, still seems applicable. This is apparent in particular in the text of the Privacy Commissioner, Mr. Therrien, who thinks this approach should be maintained.

[*English*]

Mr. Matt Jeneroux: Great.

In light of a lot of that, in particular, with what's coming before us in 2018 with the European data protection regulation, is there anything you feel we should take more urgent steps on now to align ourselves with what's happening in the European Union?

You've kind of touched on it already, Mr. Gautrais, but I also would like to get Mr. Parker in on some of my questioning. If you have anything else to add first, Mr. Gautrais...and then I'll move on to Mr. Parker.

[*Translation*]

Dr. Vincent Gautrais: Regarding Europe, I really don't think there's any rush. It's important to be connected, but the European approach seems useful culturally. I know it fairly well. I've been in Canada for 25 years, but I'm from Europe. I started in law in Europe. There's a very strong cultural difference when it comes to privacy. The view of privacy isn't the same, and as I said, we shouldn't be dazzled by the European approach. We need to maintain our Canadian identity, which is very North American.

I don't think there's any rush. We shouldn't be blinded by fear either. I think it's completely possible not to receive a notice of compliance, like the one we received in 2001. I think it's possible that we won't receive it, because the European regulation contains new principles. I also think that the Article 29 Working Party in Europe, which verifies the compliance of foreign countries, has become much stricter. I'll give you an example. In 2014, the Quebec privacy law was recognized as non-compliant. Clarifications were requested, and the Canadian legislation is probably stricter than the 2001 legislation. I think there will be differences of opinion, but the Canadian identity in the current legislation must be maintained.

● (1705)

[*English*]

Mr. Matt Jeneroux: Mr. Parker, is there any urgency with the data protection regulation coming forward in 2018 in Europe? I'm curious about your comments, particularly on the "right to be forgotten" piece.

Mr. Robert Parker: I perhaps differ from some other people, but I think the right to be forgotten would be useful. I think people would like the opportunity to extract their information. I don't know how technologically possible that is.

If I can use an example, if people are backing up on DVDs—not many people do it anymore—you can't extract one name from it. You'd have to rewrite the entire DVD, so it's impractical to remove one person's information from it.

The other thing is on where that information may reside in the organization. It may have been collected in one location and may be disseminated throughout the organization. It may be very difficult to identify all of the instances of that information and to be fully in compliance with the right to be forgotten.

In principle, it's a good idea, but there are some technological issues there.

The Acting Chair (Mr. Pat Kelly (Calgary Rocky Ridge, CPC)): We're down to 10 seconds, so I'm going to move over to Mr. Blaikie.

Mr. Daniel Blaikie: Thank you very much.

I want to start by returning to something that Mr. Young had said about tying the fines and penalties for breaking the law on the privacy of information to a proof of intention. I just wonder if that's exactly what you meant, or if that—

Mr. David Young: Sorry, just repeat the—

Mr. Daniel Blaikie: Having to prove the intention of breaking the law in order to to be able to assign penalties, and I'm wondering if that's—

Mr. David Young: How do you ascertain intention? Is that the issue?

Mr. Daniel Blaikie: I'm wondering if it becomes too high a threshold, really, or what you have in mind.

Mr. David Young: No, not really. In fact, I've had colleagues who have suggested it may be too weak a threshold.

To give you an example of that theory, organizations intentionally take steps to comply with privacy law. They develop privacy policies, procedures, a whole infrastructure. If ultimately the commissioner concludes that it's not compliant, is that intentional breach, they've intended to do that?

It's very easy to say...and quite frankly I think there has to be an intentional element if you're talking about a fine. You don't fine somebody for negligence unless it's gross negligence.

Mr. Daniel Blaikie: What I'm trying to understand is when you talk about having, for instance, law enforcement be in charge of the investigation and then law enforcement is trying to prove intent. I appreciate that for a company that in good faith honestly tries to observe people's privacy and they develop a system and in the end it's found not to be adequate, slapping them with the maximum fine may not be fair treatment.

● (1710)

Mr. David Young: Right.

Mr. Daniel Blaikie: But wouldn't it be important at that point to try to divorce the charge of having an inadequate system from the penalty? Wouldn't it make more sense to—

Mr. David Young: Charge them—

Mr. Daniel Blaikie: —consider intention with respect to how to assess the fine and not whether or not there has been a breach or whether or not they have an appropriate regimen?

Mr. David Young: I pulled out the Alberta act, and that's what the Alberta act says now. It says, intentionally breach the provisions of this act. I'm not sure about the Quebec act, but other than that it's the only law we have in Canada that actually imposes fines for breach of the legislation.

Mr. Daniel Blaikie: Right. For instance, I know that in other areas, like rail safety for instance, there is legislation on the books. Part of the issue and why the legislation is rarely used, or why there are not many successful cases prosecuted under that act—whatever safety violations are potentially out there—is because trying to prove that the company had the intent of causing harm is just simply too high a threshold to meet.

Mr. David Young: Right.

Mr. Daniel Blaikie: Would we not be at risk of repeating something similar if that were the way that we—

Mr. David Young: If you don't use intent, what are you going to use?

We have already, imminently, that it is going to be an offence for failure to report a breach, and that's just failure to report the breach.

In part, the response to what you've described is the very substantial scope for due diligence. In criminal law and in any regulatory law, it's actually part of the law. It doesn't have to be written in, but it is written into.... Look at the anti-spam legislation, for example.

To answer the example you gave, I think that would be the best way you'd respond to that.

I hope the committee has understood that I think the system works well...and notwithstanding Ian's example of the Facebook, because Facebook responded. He didn't like how they responded, so how would an order-making power deal with that? They just kept doing what they were doing but they put a privacy notice up, and blah, blah, blah.

The system has worked well, in my view. However, I understand there is pressure to consider more higher enforcement powers. I'm saying the commissioner could very easily, under its existing model, convert its recommendation power or add an order-making power to that. He basically does that now. He really does that and much more so than in 2007.

Mr. Daniel Blaikie: I wonder now, just because I only have so much time, if we could hear from Professor Kerr on that point and then we'll come to Mr. Parker as well.

Mr. Ian Kerr: Sure, and I'll try to keep my remarks on this brief.

In terms of your question about intention as being too high a standard, I tend to agree with that. If we hold the standard of proof so high—and those kinds of things are difficult to make out—if we take it almost to a level of a criminal standard, and we know criminal standards to be higher.... Mr. Young, I think rhetorically, asked the question, if it's not an intentional standard, what would it be? I would suggest that in the same way that the general approach to the reasonable expectation of privacy is an objective standard based on notions of reasonableness, and we have a whole area of private law that regulates harms to people on the basis of reasonable foreseeability and other aspects of an objective standard, we could certainly come to find some level of fault-finding that isn't at the level of intent in the way that you're suggesting.

Mr. Daniel Blaikie: Thank you.

Mr. Parker.

Mr. Robert Parker: With regard to intent versus event, we can look at some of the FTC rulings, particularly on CVS Pharmacy. One store didn't train their employees properly, didn't give patients access to their own medical information in that drugstore, and there was a $4.5-million fine for 53 events that occurred.

So the event, not the intent, was the threshold they appeared to apply in that case.

Mr. Daniel Blaikie: Okay.

For my last question, I want to follow up on that question of digital exhaust, which, if I've understood correctly, is that if I give my information to one company under a certain umbrella, and then they own that information, what can they do with that information? Can they sell it to another organization?

Mr. Robert Parker: Yes.

Mr. Daniel Blaikie: Maybe I've misunderstood the concept, but—

Mr. Robert Parker: Digital exhaust is what's left over. You executed the transaction and bought the goods, but you left a time-stamp on there as to when you did it. You left your credit card information on there or on PayPal or however you paid for it. You have all of these other pieces of information, which they can sell.

● (1715)

Mr. Daniel Blaikie: If we're dealing with that on the contractual model, does that really mean just a longer consent form and document? Or is there a way to do it that doesn't involve making the consent form more cumbersome?

The Acting Chair (Mr. Pat Kelly): You have time for just a very brief response.

Mr. Robert Parker: I think the consent model would be difficult to do. Just making it longer, with more and more consent—

Mr. David Young: Could I have 15 seconds to respond?

The Acting Chair (Mr. Pat Kelly): We're over time. I'm sorry. We may get back to that with another question.

It's now time to go to Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you very much, all of you, for being here today.

I just want to pick up on the right to be forgotten. There's been a lot of discussion on that, even going back to previous meetings. Some people have said that it couldn't stand a charter challenge.

If we leave the main premise alone, what is your opinion on the right to be forgotten for children? Do you think there should be some provision up to a certain age, if children have posted things online? What's your opinion on that? Should we have some provision for that?

That question is to all of you.

Mr. Ian Kerr: First of all, one of the points that hasn't been mentioned today, but I think has come up in previous testimony, is that even if we put aside the grandiose right to be forgotten in the European sense, PIPEDA and privacy legislation across Canada, the principles that we've referred to so many times, already include a principle about data accuracy. In situations where there's data that's untruthful or that is misleading about people, we already think that the privacy law suggests there should be a form of redress.

As I think Professor Florian Martin-Bariteau and Professor Teresa Scassa talked about, the idea of a right to erasure of wrongful information that's online could be fortified. My view is that it's already covered under the existing principles, but it may be the case that in the context of social media and young people, we ought to use that as an anchor in, to talk about something much less grandiose and vague than a right to be forgotten and something much more specific that protects children. I think we should do that.

Mr. David Young: I would certainly agree with an enhanced or a conceivable statutory right to be forgotten for children. As you'll see in my brief, I think we have a right to be forgotten. We don't know the scope of it, because there are two cases going to the Supreme Court that will articulate that in the next year. That's where I think we have to treat very carefully the general right, because I think we have it, frankly. Ian mentions accuracy. You can withdraw consent. Consent is the right to tell somebody that they can no longer use your information and can no longer keep it: delete it.

The simple answer to your question is “yes”. We've had constitutional issues with legislating children's rights for a number of reasons, but I don't think it's an insurmountable issue.

Mr. Robert Parker: I believe in withdrawing consent and I believe in the right to be forgotten. With respect to children, I haven't gone into the details, but in the United States, COPPA, the child online protection act, does provide some protection, for children 13 and under, from the information that they are likely to provide or do provide to an Internet service provider.

As I said before, it's difficult to get all the instances of that data removed from throughout the organization, particularly if that data has been sold to other organizations. I think it's a good idea to be able to withdraw consent and also to have the right to be forgotten. I see technical challenges.

[*Translation*]

Dr. Vincent Gautrais: I'm not sure that I'm in favour of a specific right for children, such as the right granted recently by the Europeans. The law already allows us to remove certain data when the damage is greater. It's true that the situation of children is more sensitive. The data can already be removed in certain cases.

I would also say that solutions exist. Facebook, for example, is very responsive and is already very good at removing problem images and videos. The company is extremely effective because it controls, in spite of what it says, the social media. It can limit the damage by removing the data and images of children. It's not a problem situation.

● (1720)

[*English*]

Mr. Raj Saini: I have another question that I wanted to get your opinion on.

Currently, the websites we use are indexed automatically and are unindexed only upon request. Do you think there might be some provision, or that it would be a good idea, to do it opposite to that, so that you would have an opt-in system to secure privacy rather than an opt-out system? Would that be ideal?

Mr. Ian Kerr: I think that is one of the issues on which one might have a principled view and the technical implementation of it would undermine any idealism that one might have, so I'll be a bit deferential in my response.

I am generally of the view that all default settings should default towards privacy. That's the problem that happened when Facebook put in its privacy settings, which I complained about previously. I think that's especially true in the context of an Internet that always remembers everything. The first book by an academic to be written on this subject was *Delete* and was about this idea of the importance of finding proxies for forgetting in an information age.

The suggestion you make would go a long way towards that, but I think it would also make for a fairly unusable environment online. I don't know how to actuate that through prescription. That would be an example of where the law could really undermine the other kind of code, software code, by making that sort of prescription.

That said, I think that as you work through these issues with your committee it's absolutely essential that you think carefully about how we make the defaults always towards privacy. That would be one way to try to do that.

The Vice-Chair (Mr. Daniel Blaikie): We have about 30 seconds if someone else wants to jump in.

Mr. David Young: In terms of what Ian is talking about, I think, an idiom in the U.S. that has been talked about for a number years is called “do not track”, which is a default setting. It basically says that for all this data collection that you.... Any time somebody goes to a website, data is being collected, whether you actively or passively provide it. Now the rule is basically an opt-out rule: you can opt out of it if you're given notice that it's happening. The converse is “do not track”, and really, that's the most protective rule—

The Vice-Chair (Mr. Daniel Blaikie): I'm afraid that's Mr. Saini's time.

We want to make sure that Mr. Kelly has his full five minutes to ask his questions before the end of the meeting.

Mr. Pat Kelly: Thank you, Mr. Blaikie.

I'd like to return to some of the more provocative statements that you made in your testimony, Professor Kerr, and perhaps ask the other witnesses to comment.

You spent quite a bit of your presentation talking about the perhaps frightening aspects of AI decision-making. You invoked Orwell, which some do when talking about the power to know and follow people's activities. There's an important distinction, though, which certainly wasn't lost on Orwell, when information is collected, tracked, or used for a nefarious purpose by a government, rather than by private actors who presumably act with consent. We've heard about all the different challenges the consent model has, in particular with regard to children.

You talked about “a duty to explain”. It occurred to me that a lot of the problems that maybe some would have around the challenges you've mentioned are dealt with through.... When we're talking about private businesses and private actors, as long as there's choice, does that not allay some of the fears that one would have?

I'd ask some of the others to comment on that, as to the distinction between a government collecting information and then being careless about people's privacy versus businesses with which one could choose not to deal.

● (1725)

Mr. Ian Kerr: Will I also get to comment on that?

Mr. Pat Kelly: Sure.

I'll let the others go first and we'll try to make sure we have time.

Mr. Robert Parker: I think if you look at the choice model, yes, you can choose certain things, and that should allow you to “opt out” of having information processed in a certain way or kept on your behalf. I think that's a relatively good model, but it doesn't work in all cases.

Another example, just to go back a bit, is the fact that if you want to be forgotten, you can't on the Internet. I use Facebook very minimally. I don't put any pictures on Facebook. However, my picture is up there and it's tagged, because someone else put it up there and tagged it. It's so omnipresent now. You can take certain items off there, but no matter what you select as your choice, it's out there.

Mr. David Young: I think the biggest problem with pure choice is that it resolves to an opt-out idiom. The choice is usually given—here are the options, maybe it's given clearly—and if you don't choose one of them, you're in.

I can tell you that in the private sector world that's the reality. It's an opt-out reality, not an opt in. If sufficient notice, transparency, Ian's thesis—I don't disagree with him—is made clearly, then the choice should be totally possible. I agree with it.

However, I think as a reality, it's not done effectively. That's what they talk about with meaningful consent. You've heard this a myriad of times, I know. It's a big challenge, but it's not insurmountable. It will never be perfect, but it's not insurmountable.

[*Translation*]

The Vice-Chair (Mr. Daniel Blaikie): Mr. Gautrais, you're welcome to participate in the discussion.

Dr. Vincent Gautrais: Regarding the consent model, I'll simply repeat that I don't think it's necessarily a matter of choosing between opt in and opt out, although that may work in some cases. The issue has merit, but the fact remains that we rely too often on a model based on consent when the consent is fictional. Other solutions exist, such as an examination by an organization such as the Office of the Commissioner.

[*English*]

Mr. Pat Kelly: Mr. Kerr wanted a moment.

The Vice-Chair (Mr. Daniel Blaikie): I know, but we already gave a little extra time.

We're going to go to Mr. Long for the rest of the meeting, which is only about two minutes.

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

I want to drill down a bit on meaningful consent. Again, I stick to this line every time I question, but with respect to children and meaningful consent, I've read in some places that potentially under the age of 13 you have to have parental consent, with 13 to 15 maybe there's a blend, and 15 and up.

Mr. Young, can you comment on what you deem is acceptable for meaningful consent?

Mr. David Young: I would deem meaningful consent...well, understanding, period. In fact, you can look at the recent amendment to PIPEDA in 2015. There's so-called enhanced consent, so read that. I have it chapter and verse in front of me. That's a pretty good description of meaningful consent. It's understanding what you're consenting to.

I'd just make a point about children. Even though there's a very useful rule such as COPPA, and there's a voluntary rule, essentially the same rule, in Canada articulated by the Canadian Marketing Association, those are useful, but, in my view, a minor can't consent.

You can treat it as consent, but they have the right to basically withdraw whatever consent they've given at the time they get to age 18 or 19. It's not exercised, but I think that is the legal rule, so they have an opportunity to re-evaluate it. I think that would work for this "right to be forgotten" for children, for example. They should get to re-evaluate it at age 18.

● (1730)

Mr. Wayne Long: Mr. Parker, do you have anything on—

The Vice-Chair (Mr. Daniel Blaikie): We just have about 20 seconds.

Mr. Robert Parker: Consent is what the individual gives, so you give consent for them to use, and it's like, look at the front office, that's where the forms, etc. go. What happens in the back office is you need sufficient granularity so if you chose A, B, and D, but not C or E, then those three would be taken, and that's not happening. The organizations that collect it, in most cases, do not change the habit of the back office system that will allow that level of granularity, so regardless of what you do on consent, you'll either get everything or nothing.

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

That's all the time we have for today.

Thank you very much to our witnesses, first of all for coming, and second for being patient with the votes that took place in the House.

I do want to mention, in case you're not aware, that if you have any additional comments you want to submit to the committee in writing that you didn't get to make today, or if anything came up to which you feel you want to provide a more fulsome response, you are welcome to be in touch with the clerk and submit those thoughts to him.

Thanks again, everyone.

The meeting is adjourned.