HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 061 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, May 16, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 16, 2017

● (1545)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Welcome, colleagues, to the 61st meeting of the Standing Committee on Access to Information, Privacy and Ethics, for the continued consideration of the study of the Personal Information Protection and Electronic Documents Act, PIPEDA.

I apologize to our witnesses for the committee's tardiness today. We have good reason. We are all just getting here from the House, where House business took us a little longer than anticipated after question period.

We'll get right to it.

We have an hour and forty minutes remaining so we should be able to get through this with no problem.

I am pleased to be joined today by Mr. Robert Watson, president and chief executive officer of the Information Technology Association of Canada. We also have Mr. André Leduc, who is the vice-president of government relations and policy.

From the Consumers Council of Canada, we have Mr. Dennis Hogarth, vice-president.

From the Canadian Chamber of Commerce, we have Scott Smith, who is the director of intellectual property and innovation policy.

Each organization will be given an opportunity to have about 10 minutes for their opening remarks. We'll go in the order in which you were introduced.

From the Information Technology Association of Canada, Mr. Watson.

Mr. Robert Watson (President and Chief Executive Officer, Information Technology Association of Canada): Thank you, Mr. Chair, and honourable members. It's a privilege to be here today to discuss the evolving worlds of technology, data, and privacy on behalf of the Information Technology Association of Canada, ITAC.

ITAC is the national voice of Canada's information and communications technology industry. Canada's ICT industry includes over 37,000 companies generating over 1.1 million jobs directly and indirectly. Beyond this, the ICT industry creates and supplies the goods and services that contribute to a more productive, competitive, and innovative economy and society. In this spirit, we welcome the opportunity to support your research on the evolving privacy environment in Canada.

The Internet has become the most powerful driver of economic growth in human history, outpacing the steam engine and the advent of electricity. Over the past few decades, data has emerged as a valuable commodity with the power to solve complex problems and generate immense benefits and value for organizations, individuals, and society. *The Economist* publication recently noted that the world's most valuable commodity is no longer oil; it is data. Today, ICT companies in Canada are using data to improve traffic flows, decrease accidents at intersections, detect health risks, improve agricultural yields, and improve the quality of life for all Canadians. We hope this discussion will deliver recommendations that enhance Canada's privacy regime in a way that promotes responsible use of personal data while supporting and enabling data-based innovation that will support the continued growth of Canada's ICT sector.

At the outset, I want to make it abundantly clear that a strong privacy regime, one that maintains the trust of Canadians, is firmly in the business interests of Canada's ICT industry. Maintaining customer trust is critical to businesses, and it has vital importance when a customer trusts a company with their personal information. In an era in which data is the world's most precious commodity, this is true today more than ever. Data, including customers' personal information, is also quickly becoming essential to most business activities, be it for fulfilling customer orders, billing, customer relationships, or supply chain management and marketing. Therefore, PIPEDA is not only consumer legislation; it is also economic legislation. I encourage this committee to factor the significant economic stakes involved into its deliberations as it considers recommending any legislative changes.

Several parties have stressed that PIPEDA is being challenged by emerging technologies and new business models. However, PIPEDA's technology-neutral and principles-based approach was designed to enable it to adapt with the times. It already includes a workable framework for managing many of the challenges associated with emerging technology like data analytics. Provided that PIPEDA is not interpreted in an overly restrictive manner, it can remain an appropriate principles-based framework able to address Canadians' privacy concerns.

Over the past year, ITAC has engaged in consultations conducted by the Office of the Privacy Commissioner, and there are three areas in these consultations on which I would like to provide additional remarks. First is protecting online reputation. Second is modernizing approaches to consent. And third is the question of whether additional enforcement powers should be provided to the Privacy Commissioner.

With regard to online reputation or what is also known as the right to be forgotten, the challenge is the permanence and searchability of any online post and the impacts that regrettable choices or malicious postings can have on a Canadian's offline reputation.

To address these challenges, the OPC has raised the idea of new legislative powers or processes to remove an individual's information from the Internet. ITAC questions whether the new rules are necessary at this time. Rather, ITAC would recommend that the government focus its efforts on educating Canadians, especially young Canadians, about how to interact responsibly online and to think before they post.

We also recommend that the government leverage the existing legal framework to improve its own processes for seeking redress from online libel through the court and make these legal avenues more accessible to the ordinary citizen. ITAC recommends against introducing an EU-style right to be forgotten that forces search engine companies to alter search results based on individual complaints.

● (1550)

Internet businesses have shown themselves willing to remove content in compliance with court orders and legal requirements, but no business should be deputized by the government to have to decide whether to strike the balance between an individual's privacy and freedom of expression. These decisions are best left to the courts.

Number two is consent. There have been considerable discussions about how new technologies like data analytics and the Internet of things make it more challenging for individuals to provide meaningful consent. ITAC strongly supports the technology-neutral, principles-based approach of PIPEDA, but our members find that express consent is an overemphasizing of how PIPEDA is interpreted by the Office of the Privacy Commissioner.

In today's fast-paced Internet and mobile-enabled world, slowing the transfer of information to complete transactions to garner express consent is a practice that has significant limitations for both customers and businesses, including individuals' willingness to read or understand what they are consenting to. By a show of hands, how many members of this committee have read every word of their iTunes privacy statement?

Increased technology complicity also means that differing or multiple organizations may be storing, processing, and analyzing the same data, making it hard to focus, to be fully explained to individuals. There are also situations where unanticipated use of data could be of great benefit to users, but where it may be difficult, if not impossible, to obtain renewed expressions of consent.

With these challenges in mind, ITAC has proposed several changes that we believe will address the challenges of consent while allowing businesses to form, continue to innovate, and generate economic value from data.

First, if express consent is not always a realistic option, frameworks should be put in place to expand implied consent in appropriate situations. Specifically, ITAC recommends a new exemption be introduced to allow for processing of personal information based upon legitimate business interests or purposes that are consistent with those in which consent was originally obtained. PIPEDA already has tools to provide boundaries for these forms of implied consent, such as the reasonable person test under section 5.3, and the OPC can provide additional guidance as required.

ITAC also proposes the exemption to consent for publicly available information be updated. The existing exemptions under PIPEDA regulations, essentially phone book details, are outdated and do not reflect the current landscape of personal information shared in public venues. Building on the time-tested model of PIPEDA itself, we recommend a new principles-based, technology-neutral exemption for publicly available information be developed that is better suited to adapt and evolve over time.

Last, ITAC also suggests that additional enforcement powers for the OPC are not required at this time. Enhanced enforcement powers were provided to the OPC as recently as 2015 through the Digital Privacy Act, and time is needed to test their effectiveness. Under the current framework, there is a tremendous amount the OPC can do to enhance and promote privacy, including through its public education function. Order-making powers could hinder the collaborative relationship that currently exists between industry and OPC and potentially make it more challenging for government and industry to collaborate and co-create solutions in this rapidly evolving field.

I want to thank you again for the opportunity to provide these remarks today, and I look forward to answering any of the questions you may have.

● (1555)

The Chair: Thank you, Mr. Watson.

Just for the record, I don't remember anybody raising a hand when you asked the question, and given that this is not televised, I need to make sure that the audio recording reflects that accurately.

From the Consumers Council of Canada, Mr. Hogarth, the floor is yours.

Mr. Dennis Hogarth (Vice-President, Consumers Council of Canada): Thank you, Mr. Chairman.

I am Dennis Hogarth, the volunteer vice-president of the Consumers Council of Canada. I'd like to say that the council is pleased to contribute to this study.

The Consumers Council is a national not-for-profit organization that supports the protection and strengthening of consumer rights and the awareness of consumer responsibilities. It works with consumers, government, and business for a better marketplace. Consumers have a clear stake in privacy, the implementation of PIPEDA, and any improvements that might be made through this review.

Important issues have been raised during this study. They reflect the need for more clarity in definitions and interpretations in Canadian privacy legislation.

In terms of the emerging electronic environment, by 2020 more than 50 billion Internet devices will be used globally, all developed to collect, analyze, and share data, mainly from consumers. A massive, growing number of data points are collected, often referred to as “big data”.

Consumer data is collected both actively and covertly through search, social media, credit card transactions, and such sites as Amazon, Expedia, and many others. Information is also now collected more passively through seemingly benign devices that report on location, living habits, and personal preferences. Every Internet connection records information about a user. Although data can be disassociated from personal information to prevent a privacy risk, when data is combined into a big data environment and analyzed with sophisticated software, we now know that the identity or profile of specific individuals can be unmasked.

In terms of the personal information risk, privacy laws lag the sophisticated uses of personal information. The accumulation of personal data creates a risk both for organizations holding it and for consumers whose information is stored.

A 2016 study by PricewaterhouseCoopers reported that many organizations still don't fully understand the risks of cybercrime and how to effectively respond to and manage these types of incidents. Issues range from low board-level appreciation of risks to weak controls used by third-party outsource vendors. Whereas consumers once knew what information we provided to organizations and why we provided it, we are now unlikely to know what information is stored about us, where it is stored, and how it is used.

This brings us to the issue of consent. Data analysis techniques grow ever more sophisticated and are now capable of accessing massive data stores. Personal information is collected, matched, and used in so many ways that it seems inconceivable that the current consent models will remain feasible or meaningful. Organizational privacy policies are often complex and one-sided and often lack transparency.

For meaningful consent, consumers need to understand how their data will be used. It is doubtful that consumers will even be able to read and fully understand the policies; yet they must overlook this to participate in an unavoidable electronic world.

A sliding scale for consent has been discussed as a possible solution. Sensitive personal information would require explicit consent, as always, but use of less sensitive information might be subject to implicit consent. To enable such a solution, the definition of sensitive information would need expansion.

Increasingly, privacy protection may turn less on who obtains personal information and more on how it is stored and kept from detrimental use. To mitigate risk, greater controls must be established around organizations that make sophisticated uses of personal information. These organizations need particular oversight to ensure that they use information appropriately.

On the issue of children and privacy, the council agrees that information collected from children under the age of 16 should be prohibited, unless authorized by a legal guardian. However, age is not authenticated easily, and children can fool systems. Without some form of reliable registry system to verify age, controls will be hard to implement without generating new privacy concerns. Regardless, protections for children included in the general data protection regulation, GDPR, should be considered for inclusion in any revisions planned for PIPEDA.

● (1600)

As to the right to be forgotten, where possible and practical, PIPEDA should restrict organizations from retaining personal information that is no longer reasonably required for processing, or where it is outdated or unable to be confirmed as accurate. Reasonable limits should be placed on the retention of certain types of personal information by controller organizations or outside processors.

Big data will create greater difficulty in identifying personal data when consumers make personal information requests of organizations. Equally, it may be difficult to identify what information needs to be deleted. Technical solutions such as meta tagging of data may assist this process, but such systems could be prohibitively costly for smaller organizations to implement.

On the issue of enforcement, organizational focus on privacy has drifted. Therefore, PIPEDA compliance by organizations remains problematic, largely because non-compliance carries minimal risk. The Office of the Privacy Commissioner must have strong, effective enforcement measures and penalties, including punitive fines and other measures for compliance failures.

We believe that a more appropriate model would include an OPC function to review published organizational privacy policies and practices, especially where these organizations are known to make extensive use of personal information. These organizations should be required to register with the OPC, providing a description of how they collect, use, and control personal information.

Periodic compliance reviews should be made against published policies and controls over data. Review results could be posted online so that consumers can know how their information is used. Oversight could be enhanced through a regulatory model that uses independent third parties.

With regard to compliance with EU standards, the GDPR represents the current gold standard for the world and will likely form the basis for future revisions to many national privacy laws and practices. Aligning PIPEDA with GDPR might involve more effort by Canadian organizations, but compliance would provide greater protection for consumers while making Canada more competitive than non-compliant countries such as the United States. In a rapidly evolving electronic world, Canadian companies will benefit over the long run. We therefore recommend that the committee carefully consider steps to ensure that Canadian privacy legislation continues to be accepted by the EU as adequate.

Finally, on consumer privacy rights, consumer privacy rights in Canada are applied inconsistently. The OPC's website refers to the various federal, provincial, and other bodies involved. Legal gaps and overlaps exist that create confusion and will grow as a concern for consumers, who want consistent rules for organizations using their information.

In February 2012, the U.S. White House issued a report that included a consumer privacy bill of rights governing consumer data privacy. While not legally binding on organizations, the report provided appropriate guidance about privacy expectations. The council believes that the clear statement of privacy rights and responsibilities set out in the White House report should be considered for implementation in Canada.

I thank you for the opportunity to make this presentation on behalf of the Consumers Council.

● (1605)

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

Our last witness of the day is Mr. Scott Smith, from the Canadian Chamber of Commerce.

The floor is yours, sir.

Mr. Scott Smith (Director, Intellectual Property and Innovation Policy, Canadian Chamber of Commerce): Thank you very much, Mr. Chair and members of the committee, for allowing me to come to address you today.

As was said, I represent the Canadian Chamber of Commerce. We are a not-for-profit trade association and are the vital connection between business and government. We have a network of over 450 chambers of commerce across the country. You are probably familiar with one from your own communities. They're all members of the Canadian Chamber of Commerce, which is the umbrella organization. By extension, we represent close to 200,000 businesses across the country, of all sizes and in every single community.

My role at the chamber is intellectual property and innovation policy from the innovation perspective. That's what you're going to hear about from me today with my remarks. You're also going to hear some similar themes to what I think you heard from the other witnesses, so I hope I don't bore you.

We hear a lot about the pervasiveness of big data and about how both governments and companies are collecting information on us. Much of what we hear comes across as negative and invasive. That's unfortunate. Personal data is the core to creating an innovative product line and user experience.

In a 2016 Accenture survey of more than 500 businesses globally, more than three-quarters of the survey respondents said big data provides better and more personalized customer service, and over half of those respondents said it enhances customer loyalty. Others indicated that the information helps them break into new markets, improve target advertising, and build better products. In a nutshell, data enables innovation.

With your indulgence, I'd like to highlight a few examples of why data is so important to innovation and competitiveness.

First, it's about understanding customers. Big data is used to better understand customers, their behaviours, and their preferences. To maintain a competitive edge, companies are moving beyond traditional datasets and using social media and browser logs as well as text analytics and sensor data to get a more complete picture of their customers.

The big objective in many cases is to create predictive models, tailored not to the individual. The information they're collecting, yes, is about individuals, but they don't really care about the individual information. It's about the collective; it's about the large balance of information that they're collecting to identify patterns of behaviour.

A good example of this might be the use of data by ski resorts. Radio frequency identification device, RFID, tags are inserted into lift tickets. They can cut back on fraud and wait times at the lifts as well as help ski resorts understand traffic patterns, which lifts and runs are most popular, at which times of day, and even help track the movements of an individual skier, if he or she were to become lost. All of this benefits the customer by making the experience more seamless. I know I'd be happy if I got a text telling me there was two feet of fresh powder on my favourite run, even though my employer might not be so pleased that I disappeared for the day.

The second theme is optimizing business processes.

Big data is also increasingly used to optimize business processes. Retailers are able to optimize their stock based on predictions generated from social media data, from web search trends, and from weather forecasts. Employers are able to optimize work flow by monitoring patterns of behaviour and adjusting processes wherever those behaviour patterns demonstrate high productivity.

Next is personal quantification.

We can now benefit from the data generated from wearables. How many of you have a Fitbit? I see one hand, just for the record.

It collects data on our calorie consumption, activity levels, and sleep patterns. While it gives individuals rich insight, the real value is in analyzing the collective data. Analyzing the decades-worth of sleep data in a single night that's collected will bring entirely new insights that can feed back to individual users.

The same is true in life sciences. Clinical trials of the future won't be limited to by sample sizes but can potentially include everyone.

While big data is used to enable law enforcement, it is also used by our financial institutions. Credit card companies monitor behaviour patterns. When those patterns deviate from predicted norms, customers are notified, which helps prevent fraud and identity theft.

PIPEDA predates social media, it predates video streaming, and it predates the notion of ransomware, which we all heard about this past week; yet it has done a pretty good job of remaining relevant as technology has evolved.

● (1610)

As principled legislation, the need for government action to react to technological change hasn't been necessary. Judicial oversight has proven time and again to be an adequate recourse where an organization has stepped outside the boundary of reasonable use of data.

Notwithstanding, significant changes were made to PIPEDA in 2015. Legislative change on something as ubiquitous as privacy legislation will always have a profound impact on business that results from the uncertainty these changes introduce to the economy. Some of those changes introduced in 2015 are not even yet in effect. We're still waiting for the details on how companies will be expected to comply with the breach notification requirements and the keeping of records indefinitely on all of those breaches. We don't really understand right now what that's going to mean. While the clarification to the definition of consent did little more than recognize a common best practice by making that change, it did cause some consternation in the business community as to what the change was attempting to accomplish at the time.

Although we need to monitor what happens in other jurisdictions to ensure our laws are compatible with our trading partners, to ensure the free flow of data and the ability to innovate, doing so preemptively could have unintended consequences. For instance, changes to the general data protection regulation in Europe are imminent, and equivalency in Canada might be put to the test. However, we must understand that the GDPR is much broader than just privacy. It's as much about the public sector and security as it is about privacy.

For instance, a comment was made about the U.S. and the U.S. surveillance. That is a factor when we're dealing with the GDPR. It's a lot more than just our privacy legislation.

Tightening controls on the collection, use, and disclosure of personal information will not likely have a positive impact on privacy protection. The manner in which information is collected and the business model that information collection is built on makes tighter controls untenable, and we're talking about basic behaviour. Trying to create a consent model around behaviour is next to impossible.

Sharing personal information requires trust. Maintaining that trust requires digital responsibility best practices, and to name a few of those: ensure personal data management meets consumer expectations; show transparency in how personal information is sourced; give people more control over their data; explain the benefits consumers earn from sharing information; and use data for social improvement.

The companies that embrace these best practices will be the ones to prosper as new technology such as blockchain evolves that will put control of personal information back in the hands of the individual.

While this past weekend's WannaCry ransomware attack may not have been focused on personal information, it is certainly a global wake-up call regarding the vulnerability of the digital economy. That means we also need a more robust response to cybersecurity concerns.

I'll give you a couple of recent statistics. In the third quarter of 2016 alone, 18 million new malware samples were captured. More than 4,000 ransomware attacks have occurred every day since the beginning of 2016. The amount of phishing emails containing a form of ransomware grew to 97.25% during the third quarter of 2016, which was up from 92% in the first quarter of 2016. Although 78% of people claim to be aware of the risks of unknown links in emails, they click anyway.

The data that's collected, stored, and used by organizations is extremely valuable. Some of that value is yet to be conceived, but governments and organizations alike are vulnerable to attack and I would argue that resources would be better used in international collaboration to target the criminal enterprises attacking databases rather than monitoring the organizations that are innovating and serving customers.

With that I will conclude my remarks. Thank you for your attention.

● (1615)

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

We're going to have a round of seven-minute questions.

Mr. Ehsassi, the floor is yours for seven minutes.

Mr. Ali Ehsassi (Willowdale, Lib.): Thank you ever so much, gentlemen, for your testimony. It was very helpful.

I'll start off with Mr. Watson. I had the pleasure of listening to your remarks. I did notice that you had quite a bit to say about meaningful consent, about the need to maintain reputations and enforcement powers. I didn't hear anything about adequacy and how important that would be as we actually consider the possibility of revising PIPEDA. Is that important? In your opinion, is the European model the gold standard?

Mr. Robert Watson: I'll answer, and then André will jump in.

We think the European model is very burdensome. It in fact puts the responsibility onto the organizations to decide who stays on and who comes off. In our view generally, people who are putting information out there are generally doing it through the proliferation of smart devices whereby they're putting information out. All through that process with smart devices there are checks and balances, even on the device.

You can have a check and balance in whether you want to have an application on your device and whether you want that application to follow you; you can decide whether you want any emails from that organization at all, and although you don't read them all, you do have to agree to the terms and conditions of anything you buy on the site.

You are thus making a conscious decision every time you progress on the device, and the organizations have put that in place because frankly, for any organization these days, the reputational risk of doing something for an individual and having it go out into hyper space—of doing something wrong—is just not worth it. They are taking care of it and are quite willing to work with the Privacy Commissioner to keep up with modern organizations.

André, do you have anything to add?

Mr. André Leduc (Vice-President, Government Relations and Policy, Information Technology Association of Canada): Adequacy remains highly important, especially pursuant to the EU trade deal and the free flow of data between Europe and Canada. I wouldn't go so far as to say the GDPR is the gold standard. One would have to measure the privacy levels in Europe against those in Canada.

Maintaining adequacy is important, and we believe that PIPEDA in its current form will allow us to maintain that adequacy and to continue with the free flow of information between Canada and Europe, which again is going to be even more important once we are able to implement the EU-Canada trade deal.

Mr. Ali Ehsassi: Would you say that the European model is burdensome as well, or...?

Mr. André Leduc: There's little question. An example coming out of the EU is the cookies example. Every website that you have in Europe has a warning that pops up first.

I'm not sure anybody is more or less protected by this policy. It's burdensome for companies and it's burdensome for the consumers who, I would venture to guess, 99.99% of the time when visiting a website will click through and allow cookies to come through on the website so that they can get the information they're looking for.

Is this type of regulation really doing anything, then? We talked about whether anybody has ever spent the time to read through the privacy policies that you see posted on a website, or do you just click through very quickly so that you can get to what you need to get done? Consumers in this day and age are always just clicking through.

There's also a system of checks and balances built into privacy legislation. It is not in the best interest of a private sector company to abuse the personal information of their own customers or clients. You can talk to T.J. Maxx, you can talk to Home Depot, you can talk to Target about the implications of having a significant data breach. Those companies were the victims of a data breach, of hackers getting into their system and accessing the personal information of their customers. They're being victimized, and they're doubly victimized by it by having a number of consumers.... For the larger businesses, that's great; they'll survive. For a Canadian SME.... You'll lose half your customers. That's usually an end-of-life incident.

It is, then, in the best interests of the businesses when they're collecting the information.... You can see how valuable it is now. As we point out, it is the new oil. There's a very high level of value for it, and protecting and storing that information and being able to analyze it is in the best interest of these private sector entities.

● (1620)

Mr. Ali Ehsassi: Thank you.

Mr. Hogarth, I take it that you come from a very different perspective, because you said that the European model is the gold standard. Why do you think it would not be too burdensome for Canadian companies to comply?

Mr. Dennis Hogarth: I'm not saying it wouldn't be burdensome. I'm saying we should make a comparison of the key points in the GDPR versus PIPEDA to make sure that we maintain compliance to the extent possible. I'm not saying that we wholesale implement the GDPR for Canada.

I think some of the main points, about four of them, have been identified as things that need to be looked at, such as children's privacy, which is a key one. As an example, when I checked out of a Staples store, my daughter was 14 and they tried to sign her up with her email address. It was a clerk who was probably 17 or 18 years of age.

There are things that need to be tightened up in terms of our infrastructure. I don't think people are properly trained in organizations, just as they probably aren't as aware as they should be in the general public.

Certainly we should do whatever we can to try to maintain that compliance with GDPR, at least to the extent that we remain adequate. Believe me, I've dealt with situations where we tried to transfer information to the U.S. and it's really very difficult if you have to go on a company-by-company basis.

Mr. Ali Ehsassi: During your testimony, you were talking about how big data and information-gathering could pose a risk for companies. I believe the only reference you made was to cybercrime. Are there other concerns that companies should have?

Mr. Dennis Hogarth: Certainly as you get into an environment where more and more stuff gets pumped into these databases, they're not going to stay within a single organization. They are going to cross organizational boundaries and you'll lose track of the information. That's why I'm basically saying that we should come up with a standard.

Meaningful consent is very impractical now. We really need an environment where organizations are tested, where somebody else basically reviews privacy policies because we can't all do it, as has been raised. Nobody here has probably reviewed more than one or two of the privacy policies that govern their lives, and there might be 20, 30, or 40 of them out there. There should be a third-party review and a standard against which these privacy policies are tested.

The Chair: Thank you very much.

We'll now move to Mr. Jeneroux, please.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you to the witnesses for being here today.

I just want to start and get everybody on record here.

Mr. Watson, you said no to the order-making powers.

Mr. Hogarth, you're for the order-making powers, correct? Yes.

Mr. Smith, I didn't get your position on order-making powers. Could you quickly comment?

Mr. Scott Smith: The order-making powers are unnecessary, so my comments refer back to the judicial system and the fact that it has been very competent in dealing with any issues where companies have crossed boundaries.

Mr. Matt Jeneroux: Okay.

On that line, the last time there was a statutory review of this act was in 2007. At the time, in the opinion of Mr. Watson and Mr. Smith, no order-making powers were necessary. However, since that time, this committee has reviewed the Access to Information Act and the Privacy Act, and we have suggested that both of those include the order-making powers. Do you think under that information perhaps it would be necessary, then, to have all acts similar in terms of granting order-making powers, or does that not change your opinion whatsoever?

Maybe I'll start with Mr. Hogarth.

● (1625)

Mr. Dennis Hogarth: When you refer to all acts, which acts do you mean?

Mr. Matt Jeneroux: Sorry. In our committee's review of the Access to Information Act and the Privacy Act, we recommended the order-making powers with that for the commissioner. With those two acts moving in that direction, would you be of the same opinion?

Mr. Dennis Hogarth: Order-making powers are going to be essential to achieve compliance. As I said in my testimony, the problem is that organizations aren't stepping up, because they see minimal risk in non-compliance. If they have to spend $50,000 to comply versus taking the risk of non-compliance and there's essentially little risk of being fined or penalized, they're going to take the easy route.

Mr. Matt Jeneroux: Okay.

Mr. Smith?

Mr. Dennis Hogarth: I have actually seen that in practice.

Mr. Scott Smith: My concern about order-making powers goes back to the experience some businesses have had with the Canadian anti-spam legislation, as an example, under which the order-making power and the compliance organization and the organization that is there to give guidance are all the same people. That creates a difficult situation for businesses. It would change the relationship between the OPC and businesses right now, which is an amicable relationship. I would be concerned that this amicable relationship would dissolve.

Mr. Matt Jeneroux: Okay.

Mr. Robert Watson: We're saying that order-making powers at this time are not necessary; that there is a good working relationship between OPC and the industry.

I somewhat disagree with Mr. Hogarth, in that there is significant cost to a company if it doesn't comply, and companies are aware of that.

Also, just to be certain, what we're talking about today is not going to stop cybercrime at all; it's going to happen. That's a different topic altogether. If somebody's coming to steal your information, really you need to put in place other applications to stop that, not more and more regulations.

Mr. Matt Jeneroux: I'll go back, then, to you, Mr. Watson, on another line of questioning, on the right to be forgotten and the right to erasure. You made comments about education being needed, not necessarily legislation, for that.

We have struggled at the committee level trying to determine what type of incident is necessary to enable that right to be forgotten and the right to erasure. Essentially, what I feel should be forgotten by everybody else might not necessarily be the opinion of my colleagues on the other side of the table.

With those different opinions in mind, how do you formulate this education to be relevant and successful?

Mr. Robert Watson: Again, I'll start, and André can jump in here.

On the right to be forgotten, first of all, before we are forgotten we ought to remember the different types of people—and I mean age groups—using the Internet. The young kids really don't care what they give over; it's of no concern to them. They may mature into a different attitude, but right now they don't care and they give information freely.

If you're doing business with somebody, the Privacy Commissioner and the privacy laws allow the right to have your information private. That's agreed. But the right to be forgotten.... I understand the concept. I just think that trying to put in regulations to deal with it is exactly what you said: there are so many different applications and so many different situations that it will be very burdensome for anybody to try to comply with, or even keep up with.

Mr. Matt Jeneroux: Yes.

Mr. Robert Watson: That is the problem.

Mr. André Leduc: You won't see a lack of compliance from the industry in responding to a judicial order. We have judicial procedures in place, if a judge decides that the content on a website needs to be taken down. You won't have any issue—the company or the website host will take it down. This is the problem: the issue you'll run into is what happens when that website is hosted in Brazil.

Adding regulation is not necessarily, then, the best practice. We already have laws on the books that will deal with this issue, and you already have compliance with judicial orders for the content to be taken down. The fear would be in deputizing the ISP industry to respond to these. If a consumer says that he or she wants that information about him or her taken down, how many times are they going to get these types of requests?

There is a judicial procedure for this.

The issue Robert brought up is that the Privacy Commissioner might be better suited for education, as an ombudsperson better situated to educate and work with the provinces through the school systems to educate young people about the danger that anything you post online may stay there for the rest of your life. These don't come down instantly, and when you see young girls posting nude pictures or whatever it might be, once they're on a website they're cut and pasted onto another and another and another.

There's no better way to control it than educating the youth about the dangers inherent with that. Trying to regulate having all of these websites take down this content is an endless game of whack-a-mole, and you'll never be able to catch up.

● (1630)

The Chair: All right. Thank you very much.

[*Translation*]

Mr. Choquette, you have the floor for seven minutes.

Mr. François Choquette (Drummond, NDP): Thank you very much, Mr. Chair.

I want to go back to the right to be forgotten. It's an important issue that everyone may face some day. The privacy commissioner's report entitled "Online reputation: What are they saying about me?" mentioned some online information about a Spanish man with a debt that had not been repaid. The information was easy to find; it just needed a search engine like Google.

That case was eventually heard and the information was removed, not just from the page where it was to be found, but also from the online search mechanism. That is one issue, but there is also the other issue you mentioned, vulnerable people.

More and more, children are being asked for personal information, especially their email addresses. Similarly, we cannot go shopping without being asked for them either. Then we get all kinds of advertising messages.

I have a daughter who will be 15 soon. She is bombarded from all sides and often asks me for my credit card so that she can shop online. These are important matters.

What are your recommendations on the right to be forgotten?

[*English*]

The Chair: Go ahead, Mr. Smith.

Mr. Scott Smith: Some of the comments earlier were in regard to the right to be forgotten. The ability of the Government of Canada, for instance—or any government around the world—to remove the digital footprint of a particular posting is next to impossible from a regulatory standpoint. You can't do it globally.

As a matter of fact, there was a case in B.C. recently where an individual had been stealing intellectual property and selling it on the web, and there was an attempt to have that reference removed globally. There was push-back from the company involved, saying, "You're out of your jurisdiction. How can you possibly say globally, from a B.C. court?" That's a real challenge.

The issue should be more around how companies address this. Companies that are reputable and value their reputation are, I think, complying with these kinds of requests, particularly where children are involved. In trying to regulate that, and in trying to say, "This fits but that doesn't fit," you're asking for trouble in terms of either missing something or going too far. It's next to impossible to get a perfect balance.

[*Translation*]

Mr. François Choquette: What do you think about it, Mr. Hogarth?

● (1635)

[*English*]

Mr. Dennis Hogarth: I agree that it's very difficult in this day and age to track down information once it's put in.

I think we're placing too much emphasis here on kids who abuse the Internet. There's more at stake than that: things such as personal health information, things that are put into databases as a result of credit card purchases, and data that companies have a lot of control over but store long beyond the time they should, especially in the case of young people. If they're identified as people under the age of 16, they should have the opportunity to have that information erased by the time they get older.

There are different categories of information. I agree that it's difficult to recover something once it's out on the web, but there's a lot of other information that we lose track of when we always focus on Internet-based information. Really, there's a lot of other information in databases that becomes stale-dated and no longer relevant, and should in fact be purged.

[*Translation*]

Mr. François Choquette: You talked about modernizing the approach to consent. I do not remember any more who asked whether we had read the entire consent page, with its tiny font, to see what we were consenting to. Personally, I confess that I do like everyone does; I accept the conditions and move on. We can't decline the conditions because otherwise we can't get access to the services we want.

How can we modernize the approach to consent?

[*English*]

Mr. Robert Watson: Concerning the principle behind the right to be forgotten and the right to make sure you know what you're signing, there are laws in Canada. If somebody's information is on a web page, there are laws already available to them to have it taken off the web page. They're there; you don't need anything else to do it. To reach out somewhere else to have your information taken off a web page because you've decided to do something different.... We can't do that anyway, so we can't add regulation.

As to the right for consent, those documents are long. They are that long because there has been a lot of interaction between governments and the lawyers of governments and the lawyers of the organizations to put those together. Believe me, an organization would rather have those documents be as short as possible. They make those documents that long not only to ensure that they're protecting themselves but also to protect the consumer, because if they were ever taken to court, they would have to make sure that the stuff in there gave proper rights to the consumer in purchasing that product. It's in there; they have to make sure it is, because you can't, as an organization anywhere in the world, especially Canada, dupe a consumer: you would never survive the courts.

It's in there, then. To try to put together regulations to say “make sure you know what you're signing” is just not necessary. It's something that's already....

[*Translation*]

Mr. François Choquette: I would like to hear what Mr. Hogarth has to say about this.

[*English*]

The Chair: Pardon me, Mr. Choquette, we're at seven minutes, but we'll get back to you in a few minutes.

Mr. Saini, please.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon, gentlemen. Thank you very much for your presentation.

I want to talk about something that hasn't really been explored, something regarding consent.

Mr. Hogarth, you sent a brief to the committee, and in it you talked about a sliding scale of consent: whether it should be explicit or whether it should be implicit. I know that last year in August, ITAC proposed, in response to the OPC's call for some consultation, as the brief mentioned, a new exception to consent for legitimate business interests.

Now that we're at the point that we're reviewing PIPEDA, and also in light of the fact that in a year the GDPR is going to come online, where do you think we should go with consent? What are your opinions on this?

Mr. Smith, I don't have any readings on you, so you might want to contribute your thoughts on this matter also.

Mr. Scott Smith: If you'd like me to start, that would be great.

There were some changes to consent less than two years ago that were intended as a clarification. I think the comments around a meaningful consent are a little bit misguided, in that what companies are collecting by way of information is not identifiable. For the most part they're collecting behavioural data; they're collecting something that they can then create predictive models out of. The idea that they're going to take the time and expense to merge data files in order to identify a specific individual.... They're not going to do that. There's no benefit to them; there's no incentive for them to do it. The real value is in that aggregated data and the predictive models it creates.

The idea that we're going to create a new model of consent whereby the information that's coming out of your Fitbit to accompany it, which in turn is sold to drug manufacturers, as an example.... There's no personal data being sold; it's the aggregated data and the value of that aggregated data that's being sold.

● (1640)

Mr. Robert Watson: It's an interesting concept, the degree of consent. There's absolute consent, saying that the person has to absolutely consent to every single interaction that is going to happen, and that's very impractical, all the way to the fact that....

I don't know whether you saw that in Toronto a council person suggested that all cellphones' FM frequency ability should be turned on so that in case there's any emergency, they can get to every single cellphone with a broadcast. You can argue that this is a socially responsible consent. Sure it is, because no matter where you are in the area and where they need to find you, it doesn't matter; it's for the benefit of the social good, because there might be an emergency such that you need to be found—that type of consent.

Also, there's consent whereby you simply contract with a cellular service provider to use their service, and because of that—they have to know your whereabouts, obviously—they're able to build a better network.

It's the degree of consent, then, that's the issue.

Mr. André Leduc: I'd add to that. In his opening remarks, Robert pointed out the reasonable person test. Whether consent is the right vehicle is a question that you guys are measuring now. The question is, is it informed consent? Are people just clicking through that button and never reading anything? Is that happening almost 100% of the time? I would venture a guess that, yes, that's what's going on.

If you want to ensure that businesses, including the public sector, are using personal information responsibly, I would suggest that you add that reasonable person test. Would a reasonable Canadian think that this is an appropriate use of their personal information, or not? The courts have 100 years of experience dealing with the reasonable person test. It seems that in today's fast-paced world, taking the time to actually understand and read about what you're consenting to, the company is trying to be transparent. That's why these privacy policies and the end-usage legal agreements are so long. It's because we've added legal liability to the scenario, and so on. Their lawyers are saying, “We have to indemnify ourselves of legal responsibilities through these things”, but nobody reads them.

Is it informed consent? I would venture a guess to say, likely not, in 99.9% of cases. You'd be better off looking at what is a reasonable, responsible use of Canadians' personal information when it is collected.

Mr. Raj Saini: Mr. Hogarth.

Mr. Dennis Hogarth: I agree that nobody is reading these privacy policies. They've gotten too complex, too legalistic. That's why I think there should be a third-party assessment of some sort made of organizational privacy policies so that consumers can be warned if there are terms and conditions and certain privacy policies that they should be aware of. Somebody could maintain a website that basically reports on the major issues and features of these different privacy policies.

On the issue of consent, we totally agree that there is no way you can have fully informed consent in today's world. That's why we say that probably you need to expand the definition of sensitive information for those things where you need to get explicit consent and implied consent for the rest. The consumer and the public need a reference point for these policies to determine whether they're good, bad, or indifferent.

● (1645)

Mr. Raj Saini: I'll continue with you, Mr. Hogarth.

In your submission, you also wrote that organizations should retain information no longer than is reasonably required. That fits into part of what my colleagues have mentioned in regard to right to erasure in article 17 of the GDPR.

Can you give us some examples of how we can deal with this, especially in this era of big data?

Mr. Dennis Hogarth: In the day of big data, and even before big data, the issue is basically that organizations should set a time limit on what is a reasonable retention period for information. Even in a big data environment, there are tools that can be implemented to tag data and set a time limit or some other criteria on it. We are going to have to move into that world as we move into big data. We can't get into a big data world that is totally uncontrolled in any way, shape, or form. There are technology tools that allow the use of big data and allow the assembly of big data databases. There are also tools that basically allow control of the big data, and those need to be implemented.

The Chair: Thank you.

We'll now move to a five-minute round, beginning with Mr. Kelly.

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

I'll begin with you, Mr. Hogarth.

You talked about the different types of consent and the need to differentiate between that which is particularly sensitive and that which is maybe less so.

Are there currently specific failings of PIPEDA as it is now that need to be addressed? In the concerns you've raised, what are the current failures that are preventing the types of better treatment of information and different types of consent?

Mr. Dennis Hogarth: I don't think it's a case of better treatment. PIPEDA is very explicit when it comes to issues of sensitive information. Quite frankly, I'd have to think about what other things and areas might need to be added.

Certainly, there are some people who consider their address a piece of sensitive information, as is their cellphone number and, increasingly, this information that can identify them, such as your identifier on your cellphone. The way that your cellphone can actually be tracked could be considered sensitive information.

Mr. Pat Kelly: Okay. Is there something specific that you would want to see? What's your one change that you would want to see under PIPEDA, then?

Mr. Dennis Hogarth: I'd like to take that away and think about it, but I'd pleased to do that.

Mr. Pat Kelly: Okay. Well, maybe if I get the next five, I'll try again, but if you could think about it....

Mr. Robert Watson: Excuse me, can I just...?

Mr. Pat Kelly: Sure.

Mr. Robert Watson: Just as a practical situation with regard to your last question about cellphone number numbers and email addresses, people are wanting to keep these for life. You now can take your cellphone number anywhere in Canada and keep it. It'll go with any other carrier for the rest of your life if you want. Your information has to stay at the original carrier and at your new carrier. That's how it works. Your email address and that information you want to keep as your email address has to stay at the original email provider and your new email provider, however it goes. There's a practical application to this consent idea.

Mr. Pat Kelly: Okay. We're studying PIPEDA, and hopefully we'll get to a report that will recommend changes. Is there an existing impediment? Or are there changes that you need, and that you think need to be made to the law as it exists now, in order to facilitate these expectations that perhaps customers have and in order for the mechanics on the side of business to be able to comply?

● (1650)

Mr. André Leduc: When it was drafted in 1999 and introduced in the House, and then through enactment in 2001, I think that at that time we were clicking through websites and we weren't using these devices quite as much. I would venture to say that the pace of life was just a little slower.

I think the biggest thing is what you are studying: is consent the appropriate vehicle? If there's one thing that is worth reviewing in PIPEDA, it's what the value is of somebody actually clicking through consent when they don't know what they're consenting to. Should we be looking at another model of forgoing that step in the process to go more with a “reasonable use and reasonable person” test to evaluate what you should and shouldn't be collecting, or what you're able to collect, and how you're going to use and disclose that data after the fact?

Mr. Pat Kelly: Okay.

Maybe I'll shift gears completely with the time I have left and ask you, Mr. Watson, to talk about what you mentioned earlier, which was the importance of making the distinction between criminal activity and the use of information by businesses. You said that no matter what regulation you might put in place to protect businesses, which have their own interest in avoiding reputational damage and all of this in complying, as an activity distinct from that of actual hackers and those who don't care about any of the foregoing.... I'll let you expand on some of that, because it seemed important to me.... PIPEDA is not the Criminal Code. This perhaps isn't where we address some of these activities that impact privacy.

The Chair: Mr. Kelly has used all of his time for his question, so please give a very succinct answer, Mr. Watson.

Mr. Robert Watson: It's simple. There are two ways for cybersecurity or cybercrime to happen. One way is with existing information sitting somewhere, but more and more lately, it's actually when you're doing the transaction that they get you. It's not historical data.

The Chair: Okay.

Mr. Long, please, if you can keep it short.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you to our presenters this afternoon. Again, it has been very interesting testimony. The more we hear, the more we learn, and the more questions we have, I think.

I think my first experience with the right to be forgotten was—and I promise this won't be my bedbug story with the Saint John Sea Dogs—in 2005-06, when we did have a player who made a statement that actually caused national news. It was on *Hockey Night in Canada*, and I had to do certain things to try to mitigate the damage. I wasn't playing on my phone just now, I promise, but when you were talking, just for fun I googled his name, and the first thing that came up—we're talking about 11 years ago—was that instance.

I'll throw this out right across the panel. Maybe we'll start with you, Mr. Leduc and Mr. Watson. Can we forget about the right to be forgotten?

Mr. André Leduc: I wouldn't suggest that you forget about it. You also need to look back into the pre-Internet world. If something ends up in a newspaper, it goes on microfiche and is still accessible. It's just different in the way that we access it now. We're using a search engine and going to the Internet, so it's more readily available than it was then.

From a legal standpoint, the rule book shouldn't change because we have the Internet. The person made those statements, and whether a judge would afford them the right to be forgotten in those circumstances is what's interesting. That's why we always kind of refer back to.... When we talk about third-party reviewing, we allow it to be our judiciary who does that review. They can make the decision on whether this person will or will not have the right. It's not a simple request that I'd like to have that information taken down from the website—

Mr. Wayne Long: Right.

Mr. André Leduc: The recourse is already there. It was there before the Internet came about, and it maintains its applicability today.

Mr. Wayne Long: Mr. Watson.

Mr. Robert Watson: The beauty of the Internet, which is that it enables everybody anywhere in the world to get information the same as anybody else—if you have the right connection, of course—is also the problem with the Internet. Everybody makes mistakes, and now your mistake is there.... You won't stop people from making mistakes in the future—

Mr. Wayne Long: Right. Just to jump in, this is now a 27-year-old man who's interviewing for jobs and having people check him out. Again, the first thing that comes up is this incident.

Mr. Robert Watson: Yes, immediately. Again, it's the beauty of the Internet. It's instant. In the old days, you would have had to wait. The guy probably would have been employed for a couple of months, somebody would have found it, and then he would have been done.

It's a timing issue. People will always make mistakes or have things they regret saying, or whatever. We can't keep putting in regulations to try to protect people from doing silly things.

● (1655)

Mr. Wayne Long: Mr. Smith.

Mr. Scott Smith: I'd be inclined to agree with that. What you're talking about is essentially a historical record. If it makes the news and it's true, then it exists in one form or another. Just because you've taken it off the Internet.... As André pointed out, it's still going to exist in another form somewhere. Even if it's not online, it's probably still going to be available somewhere. Somebody is going to be able to look it up. You're never truly forgotten.

Mr. Wayne Long: Mr. Hogarth, do you have anything to add to that?

Mr. Dennis Hogarth: I think of somebody who is charged with a crime, for example, but basically is found innocent. Ten years later, the news reports are still out there, and they show up when a search is made. That is the sort of information that probably needs to be forgotten in some way, shape, or form. If somebody is found innocent but the charge is still out there, or the press is still out there, it's going to have an impact on their career and future life.

Mr. Wayne Long: Okay. Thank you.

We do have Fitbits. Our family has Fitbits. We went out and bought Fitbits a few months ago. A few of my friends who have younger children came. I signed up my Fitbit, did all my things, went on my iPhone, synced it, and pressed approve, approve, approve.... Yesterday, I did 15,168 steps, my resting heart rate was 59, I travelled five miles, and I slept for four and three-quarter hours.

That's okay for me. I pushed all the notifications and buttons. But what do we do to protect children? For example, I believe the stat is that 70% of 14-year-old kids have phones now. What do we do explicitly to protect those children from that same thing? The 14-year-old child with his Fitbit basically went through the same thing I did in pressing “yes” for everything. How do we protect children under PIPEDA? What do we do with meaningful consent?

Mr. Leduc.

Mr. André Leduc: There were updates in the Digital Privacy Act in order to focus on the protection of minors—not the guys with hats who live in caves, but the children who we have to deal with—and it has to be a balanced approach.

Robert pointed out that we need better education. This is the advent of the Internet. It's a really big thing. Whether it's the school systems, the parents, or the community groups, we need to be educating kids about the potential dangers.

When you're dealing with something like Fitbit, where it's tracking your heart rate and everything, there isn't a lot of danger there. What we're talking about on the big data side—it's really exciting—is that maybe they'll be able to notify you by a text message half an hour before you have your heart attack. That's where we're heading. That's where big data analytics is going.

In terms of protecting minors, it's very difficult to put the onus on the company that is collecting that information, other than asking you if you are under the age of 18, under the age of 19, or under the age of 21, and saying that if you are, you have to get the consent of your parents in order to fill in that information.

Beyond that, there isn't a lot there. How many 14-year-olds would go to their parents to get the okay to fill in the information on the Fitbit? How many parents would go, "Would you just leave me alone?"

Again, I know that I keep reiterating the same point, but when you look at the reasonable use, the reasonable connection, and a reasonable person test for evaluating what is okay and what isn't, you see that it's a lot easier than trying to regulate a consent regime that maybe doesn't really have any value to it. You're not really getting informed or educated consent, and you can't really tell the age of the person you're collecting from, because I would venture to say that most 14-year-olds would ignore that fact and say, "Oh, it won't let me if I'm 14, so I'll just click on 18, and then I'll get through."

The Chair: Thank you very much, Mr. Long. I appreciate that.

I'll take the round for the Conservatives for the next five minutes, if that's okay with my colleagues.

As a former IT professional, I understand completely what you're saying when you say that data is the most valuable corporate asset. That's been the way of the information age for quite some time, and now, as you've said, data is becoming more valuable than oil, which is interesting.

Mr. Smith, I'm going to you, because I'm going to follow up on what Mr. Long's question was. Data is becoming very, very useful. Actually, it's information that is more useful. Data is raw facts, whereas information is actually coalesced information that's of value and is of use.

Here's my question for you, Mr. Smith. You have been very clear that it's the data, the de-identified data that predicts trends and so on, that a particular user or group of users in a certain age group—or a certain whatever—might be interested in, so that we can have predictive modelling for the purposes of sales and business. I don't think most people have a problem with that.

I actually like the fact that my iPad from time to time knows what I'm thinking more than I do. That's okay, but for a Fitbit, what about the fact that if a Fitbit and its information about sleep patterns, a resting heart rate, and any other health information gleaned from that Fitbit were to get into the hands of a prospective employer prior to an interview? What if it wasn't de-identified, we actually knew who that individual was, and it became an issue, much like the genetic discrimination bill that we just passed in Parliament? What if it became an issue that was keeping somebody from getting a prospective job? Perhaps that Fitbit is measuring their weight and other habits they have that might predispose somebody to prejudice when that person is applying for a job.

I would be interested to see what the point of view might be from Mr. Hogarth and Mr. Smith on this.

● (1700)

Mr. Scott Smith: I think I referred to this in my remarks, but I don't remember. My response to that is, what would be the reputational damage to a company like Fitbit if it came out that they were selling that information to employers, insurance companies, or what have you? They would be out of business very quickly.

Yes, there is a value to that information, and there is possibly even a temptation to sell that information to prospective employers, for instance, but the likelihood of it happening for a company that wants to remain in business—

The Chair: What if the employer is Fitbit?

Mr. Scott Smith: Again, I think that goes back to the privacy policies that are already built in and the fact that they are not collecting identifiable personal information at all. They're not doing it.

Could it happen? Sure. Is it likely to happen? No.

The Chair: Okay. I believe you.

Mr. Hogarth.

Mr. Dennis Hogarth: I have a simple question. Is Fitbit information health information? It's covered under the sensitive categories that require explicit consent. It's as simple as that. For that information to be used by another party would require explicit consent. If it pertained to a minor, it would require the parents' consent.

The Chair: Fair enough, I appreciate that.

I have a question for Mr. Watson or Mr. Leduc.

When it comes to the threshold for compliance, monetary penalties, we talked about how it's different.

Mr. Leduc, or maybe it was Mr. Watson...I think you said it would be okay for Target, that they'd survive. Target is going to survive because they're a large enough company, but a small or medium-sized enterprise might not survive if their data is breached and there were monetary penalties associated with it through any changes that this committee might recommend in the legislation.

Should there be a threshold? I'm not much for arbitrary lines in the sand when it comes to legislation, but should there be a threshold, so that companies that are small and don't necessarily have a privacy person appointed...?

I mean, I had my own IT company before I did this. I was a one-man shop. I was my own privacy consultant in my company. What do we do for those smaller companies? Should we have an exemption so that those companies would be not affected in the same way as a larger corporation, or is there an inequity and unfairness inherent in that?

Mr. André Leduc: I didn't mention this in the opening, but I did my MBA thesis on small and medium-sized enterprise, the compliance with PIPEDA and CASL, and the impacts on those small firms. I went so far as to do a survey of small businesses, and did some focus-group testing with them as well.

The issue that you'll run into is one that you mentioned. A larger corporation would be able to survive. If you hit them with $100,000 penalty, they can pay it and continue on with the business they were doing. When it comes to a smaller enterprise, $100,000 would definitely be the difference between that business continuing and ceasing operations and filing for bankruptcy.

In the case of a data breach, the business is being victimized by a hacker who has infiltrated their system and removed information in order to either damage that enterprise or collect personal information about their customers. With regard to having rules and regulations in place that require companies to understand that they need to keep the information they collect secure, that understanding is already there.

Penalizing a small enterprise for being the victim of a data breach is probably not the best course of action. Bringing them in and having the OPC sensitize them to an understanding of what happened in the hack, doing the investigation—they'll understand the engineering behind it—is probably a better course.

That's the system now. They bring in the small and medium-sized enterprise and explain what the issues were, and ensure that they're compliant going forward.

● (1705)

Mr. Robert Watson: Can I add to that?

The Chair: Very quickly, please.

Mr. Robert Watson: A quick point is that large companies would be impacted even more than small companies, again because of their reputation.

I can assure you that every board now looks at any incident dealing with social media at all very seriously. Just look at the mortgage company in Toronto that didn't pay attention to a couple of misstatements three or four years ago. It's not as if they were insolvent, but all their investors pulled their money.

The Chair: Well, Mr. Watson, nobody around this table understands that something we said four years ago might come back to haunt us.

Monsieur Dubourg, for five minutes, please.

[*Translation*]

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

I would like to welcome the witnesses who have joined us this afternoon.

Thank you for your presentations and the briefs you submitted.

My first question goes to Mr. Watson.

The point you make in your brief is that there is no reason to change the legislation and that it remains current. Despite the technological advances, you feel that there should be no amendments to the legislation.

Is that what you are saying, in fact?

[*English*]

Mr. Robert Watson: We think there's an evolution coming, for sure. The Internet is evolving and evolving fast. There's no question about it.

We believe that the act in place now is good. What should happen is that the OPC should be more like an ombudsman, putting out guidance, working with the industry, suggesting changes. Industry will go with it. There's no question about it. There's no lack of wanting to go along with it. They're just very concerned that if you start layering regulation on regulation, it will never stop. It will get complicated, that's all.

Mr. Emmanuel Dubourg: I agree.

[*Translation*]

You are still on the same wavelength. The other aspect deals with penalties. You said that the commissioner should not be given more powers because the collaborative approach is working well. Is that correct?

[*English*]

Mr. Robert Watson: I agree. They can come out and say that this company is not co-operating and they need it. If they come out with any sort of statement at all, whether it's soft or hard, it will not be taken lightly by the company, and I don't know any company that would take it lightly.

[*Translation*]

Mr. Emmanuel Dubourg: Okay.

Let me now turn to you, Mr. Hogarth.

Your report contains a number of cautions with regard to metadata. You say that, in 2020, there will be more than 50 billion devices connected to the Internet and that a lot of information will be obtained covertly, if I can put it that way.

You are a Fellow of the Order of Chartered Professional Accountants.

First, are there any control measures similar to the ones you suggest we could look at in order to improve this bill?

Second, can you comment on what Mr. Leduc said? When he answered a question, he said that it would be difficult to implement control measures for children from 14 to 16. What can we do to make sure that the data collected are appropriate?

[*English*]

Mr. Dennis Hogarth: First of all, one thing that I pointed out in my brief was that it's authentication that's the issue, and that's going to become an increasing issue, not only for people who are underage, but for all of us. How do you authenticate that you are the actual person who's providing consent or giving access to your data? That's something that needs to be looked at in detail. That's going to involve technology, however you look at it. That's going to be, I think, the major issue.

Your first point was?

● (1710)

Mr. Emmanuel Dubourg: It was regarding control.

[*Translation*]

Can we implement more control measures to make sure that the data collected are appropriate?

[*English*]

Mr. Dennis Hogarth: Control over big data.... For a lot of this stuff, when I say it's being collected covertly, it's a situation like your thermostat at home collecting a lot of different data points of information about how you run your household. They're now talking about the fact that refrigerators are actually gathering information about everything, including what's in the fridge.

You have automobiles that are providing information that could be very valuable to insurers. I don't believe that you give consent to your car to say that you can or can't provide all of that information.

Increasingly, we're going to have to look at ways of looking at those industries, not necessarily from a consent model, but from a standpoint of doing a review or an audit of how they're using information and then asking, is it in fact reasonable? Does it pass the reasonableness test?

Mr. Emmanuel Dubourg: Thank you.

The Chair: Thank you very much, Monsieur Dubourg.

We have our last questioner, Mr. Choquette, for about three minutes. Then I'll ask the witnesses to please clear the room as we have to move in camera for committee business.

I want to take this opportunity to thank you for your testimony today.

Mr. Choquette.

[*Translation*]

Mr. François Choquette: Thank you, Mr. Chair.

I would like to go back to the dispute resolution mechanism. When the Office of the Privacy Commissioner of Canada investigates, it can use a dispute resolution mechanism but it cannot impose a fine or an order. However, the Alberta and British Columbia legislation on protecting personal information in the private sector allows the information commissioner to issue orders.

Do you know of any specific cases when orders were issued by the privacy commissioner in Alberta or British Columbia? Were the results positive or negative? How would you assess them?

[*English*]

Mr. Scott Smith: I don't have direct experience with the order-making powers in Alberta. It's all basically hearsay. I will reiterate what was said earlier, that it creates a gap between the businesses that are involved in those processes and the commissioner. What I will say about PIPEDA is that I don't think anyone could point to an example where the commissioner has done an investigation and the judiciary has pronounced on it, and there hasn't been a resulting compliance.

Is it necessary for the commissioner to have order-making powers? I would suggest no. The system is working quite well right now, and changing it would change the dynamics.

Mr. Dennis Hogarth: I pointed out in my brief that there is a danger in the inconsistency between federal laws and provincial laws that a lot of national companies would certainly get caught up in.

If you are going to look at the success or failure of order-making capabilities, I think you'd probably look to some countries that have actually implemented those programs, such as the U.K. and France. They may seem a little extreme, but they have been very effective in achieving compliance.

Mr. Robert Watson: We don't have any experience with order-making powers.

[*Translation*]

Mr. François Choquette: Okay.

[*English*]

The Chair: Okay.

We're at about three minutes. Thank you very much to our witnesses, again, for taking the time and sharing their expertise with us.

I'll suspend the meeting briefly, and we'll move in camera. We have a bit of committee business to discuss.

Thank you very much.

[*Proceedings continue in camera*]