HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 062 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, May 30, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 30, 2017

● (1535)

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): Welcome to the 62nd meeting of the Standing Committee on Access to Information, Privacy and Ethics. We have three groups before us today: the Canadian Life and Health Insurance Association, the Insurance Bureau of Canada, and the Interactive Advertising Bureau of Canada.

Welcome, all. We do have a vote at 4:30 and bells are likely to ring at 4 p.m., so excuse the future interruption.

We'll start with the Canadian Life and Health Insurance Association, Mr. Zinatelli and Ms. Duval.

You have 10 minutes to make an opening statement.

Please begin. Thanks very much.

Mr. Frank Zinatelli (Vice-President and General Counsel, Canadian Life and Health Insurance Association): Thank you, Chairman and members of the committee.

I'm Frank Zinatelli, vice-president and general counsel of the Canadian Life and Health Insurance Association. I'm here today with my colleague Anny Duval.

I would like to thank the committee very much for this opportunity to contribute to the review of PIPEDA. With your permission, Chairman, I would like to make a few introductory comments, and then provide the committee with the industry's views pertaining to the PIPEDA review.

By way of background, CLHIA represents life and health insurance companies accounting for 99% of the life and health insurance in force across Canada. The industry protects about 24 million Canadians and some 20 million people internationally. The Canadian life and health insurance industry provides products that include life insurance, disability insurance, supplementary health insurance, annuities, and pensions. For over a hundred years, Canada's life and health insurers have been handling the personal information of Canadians. Protecting personal information has long been recognized by our industry as an absolutely necessary condition for maintaining access to such information.

Over the years, life and health insurers have taken a leadership role in developing standards and practices for the proper stewardship of personal information. For example, back in 1980, we adopted “right to privacy” guidelines, which represented the first privacy code to be adopted by any industry group in Canada. Since then, the life and health insurance industry has participated actively in the development of personal information protection rules across Canada, starting with Quebec's private sector privacy legislation in 1994, the development of PIPEDA, Alberta's and B.C.'s personal information protection acts in the early 2000s, and health information legislation in various provinces.

The life and health insurance industry has had experience with PIPEDA for over a dozen years now, and we find that generally the current model continues to be effective and workable. That being said, your review of PIPEDA will afford the committee the opportunity to consider areas in which some targeted adjustments may be appropriate.

With this in mind, let me turn to a few of those areas.

One key matter that has been much discussed recently is the consent model. CLHIA participated in the Office of the Privacy Commissioner of Canada's consultation on consent and privacy, including stakeholder meetings. In our view, it is still feasible and appropriate to obtain meaningful consent in our industry under the current model, and there is no need to rethink the concept of consent in its entirety. There could be some helpful enhancements made to PIPEDA that would facilitate the obtaining of consent, but we do not believe that a complete overhaul of the model is necessary to achieve this goal. Rather, improvements can be achieved through supporting guidance or clarifying legislative changes that could reduce the burden on both individuals and organizations.

As an example, to address some uncertainty or stress on the consent model that some stakeholders have raised, it might be helpful to expand the list of exceptions to consent to add a new exception that aligns with the concept of legitimate business interests. The new European Union's general data protection regulation will allow businesses to process personal information without consent if they can prove that the data processing is necessary for the purposes of the legitimate interests pursued by such organizations. These interests would have to be balanced against other interests, and so, in the PIPEDA context, could be tied back to what a reasonable person would consider appropriate in the circumstances.

Now my colleague Anny will continue.

● (1540)

[*Translation*]

Ms. Anny Duval (Counsel, Canadian Life and Health Insurance Association): Another aspect which in our opinion needs to be updated is the definition of "publicly available information".

The current definition in the Regulations Specifying Publicly Available Information no longer reflects reality or the expectations of the individuals it is intended to protect. In our opinion, this definition should be expanded to cover situations in which an individual decides to post personal information on a public website.

In such cases, we presume that the individual is waiving any expectation of protection of privacy and that it would therefore not be necessary to obtain their consent in order to collect, use and disclose that information. All the other provisions of the PIPEDA would continue to apply as they do currently for the collection, use and disclosure of publicly available personal information.

The third point we would like to make pertains to the ombudsman model. The life and health insurance industry believes that the current model should continue to be used since it effectively balances individuals' right to privacy and the rights of organizations to use that information legitimately and reasonably in a business context.

This model makes the Office of the Commissioner more accessible, informal and flexible in helping the parties resolve issues. It also makes it possible to work with consumers and organizations to ensure that everyone better understands what should not be done in order to provide reasonable and appropriate protection of privacy.

Another aspect of the ombudsman model is that it focuses the Office of the Privacy Commissioner's attention on responding to individuals' complaints in order to better process them, and on achieving balance between consumers and organizations, rather than devoting time and resources to creating a file in order to deal with a potential breach.

The right approach is to focus on resolving problems first.

[*English*]

Mr. Frank Zinatelli: Finally, Mr. Chairman, we would like to make a very technical suggestion regarding the mandatory five-year review of the act. Based on recent experience, the industry believes that it would be beneficial to all involved if section 29 of PIPEDA was amended to set the start of each review five years from the end of the last review period, as opposed to every five calendar years. This would ensure that the review process is duly finished before the next one is set to begin. It would just clarify things in some ways.

In summary, Mr. Chairman, the life and health insurance industry has had experience with PIPEDA for over a dozen years now, and we find that generally the current model continues to be effective and workable. That being said, your review of PIPEDA will afford the committee the opportunity to consider areas in which some targeted adjustments may be appropriate.

The industry appreciates this opportunity to participate in the committee's review of PIPEDA. We would be pleased to answer any questions you may have.

Thank you very much.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much for that presentation.

For the next 10 minutes, we'll have Mr. Lingard and Mr. Bundus, on behalf of the Insurance Bureau of Canada.

● (1545)

Mr. Randy Bundus (Senior Vice-President, Legal and General Counsel, Insurance Bureau of Canada): Thank you, Mr. Chair.

My name is Randy Bundus, and I am senior vice-president, legal and general counsel with the Insurance Bureau of Canada. I am joined by my colleague Steven Lingard, who is IBC's director, legal services, and chief privacy officer.

We are pleased to represent the Insurance Bureau of Canada and our member companies to contribute to the discussion on the next review of the Personal Information Protection and Electronic Documents Act. We understand that the committee is interested in hearing views on issues that were contained in the federal Privacy Commissioner's 2016 paper that discusses the challenges that traditional notions of consent will face as technology and business models continue to evolve and also potential enhancements to consent under PIPEDA. IBC's comments today are based on the submission we filed in response to the OPC discussion paper.

IBC is the national industry association, representing over 90% by premium volume of the private property and casualty insurance sold in Canada. The private P and C insurance industry in Canada provides insurance protection for homes, motor vehicles, and commercial enterprises throughout the country. There are over 200 private P and C insurers actively competing in Canada.

The P and C insurance industry also works to improve the quality of life in Canadian communities by promoting loss prevention, safer roads, crime prevention, improved building codes, and coordinated preparation for coping with natural disasters.

I'd first like to comment on the insurance industry's layered approach to consent. PIPEDA is a consent-based privacy law that requires that, with limited exceptions, the individual must give consent for the collection, use, or disclosure of that individual's personal information.

While IBC acknowledges the concerns and issues raised in the Privacy Commissioner's discussion paper, we are of the view that the current consent model under PIPEDA is appropriate for Canadian P and C insurers and their customers and does not need to be changed in any significant manner.

PIPEDA was amended in 2015 by the Digital Privacy Act, also known as Bill S-4, to include the concept of "valid consent", which says that consent is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose, and consequences of the collection, use, or disclosure of the personal information to which they are consenting.

It must be noted that the P and C insurance industry is regulated, from a business perspective, at the provincial and federal levels. The provincial and territorial superintendents of insurance have jurisdiction over market conduct and policy wordings, while the federal superintendent of insurance has jurisdiction over corporate governance and solvency. This is in addition to the privacy regulation of insurers by the federal and provincial privacy commissioners.

Canadian P and C insurers have, for many years, used a layered approach for obtaining consent to the collection, use, or disclosure of personal information. For example, when an individual applies for an insurance policy, they are asked to consent to the collection, use, or disclosure of their personal information for a variety of immediate and potential future legitimate insurance purposes, including assessing the risk—what we call "underwriting"—investigating and settling claims, and detecting and preventing fraud. The wording of the consent language in the automobile insurance application forms and claims forms is mandated by the provincial and territorial superintendents of insurance, and insurers and consumers must use these mandated forms. Then, if a claim is made under the insurance policy, the insurer will typically obtain a consent from the claimant to collect, use and disclose their personal information for the purpose of adjusting and settling the claim.

Insurers also employ the use of separate consent agreements obtained when providing insurance quotes and stand-alone products and services. An example would be usage-based insurance. Usage-based insurance, or UBI, is a relatively new product in Canada, although it has been sold for several years in other countries. UBI is an example of a new technology-enabled insurance offering. UBI allows an insurer to customize auto insurance premiums to reflect the actual driving usage by the customer by recording some basic information, such as frequency of use, distance driven, time of day when the vehicle is driven, turning, acceleration, speed, and braking. The information is collected by means of an interface between the individual's vehicle and the insurer.

UBI is a voluntary product, and it is entirely up to the consumer to decide whether they want to accept and use this offering.

● (1550)

Like other auto insurance products, UBI is regulated by the provincial superintendents of insurance. The superintendents of insurance in Ontario and Alberta have set certain standards around how insurers can collect and use this UBI information. It should be noted that the Office of the Information and Privacy Commissioner of Alberta has become involved in the regulation of UBI in that province.

In addition, personal information can be collected about automobile insurance accident benefit claimants through the mandated use of auto insurance claims forms. These forms are mandated by the superintendent of insurance and also contain certain privacy and consent wordings similar to those contained in the auto insurance application. This layered, circumstance-specific approach gives insurers the ability to inform their customers of new uses and disclosures of their personal information, and to obtain their consent as the need arises and the relationship with the individual evolves, including with the offering of new technology-based insurance products.

Next I'd like to speak a bit about updating the consent regime.

Legislative and regulatory regimes need to be periodically updated to keep them current. IBC and its members support the following proposals to enhance PIPEDA's consent regime.

First, with respect to exceptions or alternatives to consent, there are situations in which insurers rely upon certain exceptions to the current model that exist in section 7 of PIPEDA, such as the investigation of fraudulent claims, or obtaining witness statements in order to adjust and settle insurance claims. There is a similar, but different regime in the EU general data protection regulation, or GDPR, that will come into force in 2018. The GDPR includes reference to legitimate business interests, but it is unclear how this would apply in practice and how it is different from the current exceptions in PIPEDA. Legitimate business interest might be useful as a supplement to the PIPEDA exceptions.

The importance of PIPEDA and the provincial privacy laws continuing to be adequate for the purpose of the GDPR is a matter for in-depth consideration by this committee.

Next I'd like to touch on anonymized aggregate data.

The use of anonymized aggregate data, as a form of de-identified data, is currently being used by insurers and should remain a viable alternative to the consent requirement. It can be used in various legitimate ways, and safeguards against misuse of this data by third party service providers are built into contracts between them and the insurers.

With regard to codes of practice, insurers are heavily regulated by a number of regulatory authorities, particularly the federal Office of the Superintendent of Financial Institutions, or OSFI, which regulates solvency and corporate governance; and the provincial and territorial superintendents of insurance, which regulate market conduct, including the wording of certain mandated insurance policies and forms.

Were codes of practice to be considered, our view is that they would be redundant and add little value due to the strict requirements already put into effect by federal and provincial regulators.

With regard to the OPC enforcement model, IBC agrees that independent oversight bodies such as OPC play an essential role in protecting the privacy interests of Canadians. Based on insurers' experience with OPC to date, the industry is of the view that OPC has done an extremely effective job of protecting individuals' privacy with the powers currently afforded to it under its governing legislation. Insurers take their privacy and consent obligations very seriously and understand the importance of strict compliance with the requirements imposed upon them by privacy legislation and insurance regulators. Recognizing the importance of these obligations, insurers have an internal ombudsman's office whose role is to conduct independent and impartial investigations of consumer complaints. The role of the ombudsman's office would likely have to be re-evaluated should the OPC's powers be expanded.

Furthermore, it is noteworthy that the 2015 amendments to PIPEDA found in the Digital Privacy Act included new enforcement powers for OPC, including the ability to compel organizations to enter into compliance agreements. Also, recent developments in privacy jurisprudence, particularly the creation of the new privacy torts commonly referred to as “intrusion upon seclusion” and “public disclosure of private facts”, creates further incentives for organizations to protect against privacy breaches at the risk of increased reputational and monetary damage.

● (1555)

For these reasons, IBC does not believe OPC needs additional powers to be able to continue to function appropriately and fulfill its mandate.

Thank you for your attention. My colleague Steven Lingard and I would be happy to take questions later.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much for that presentation.

Next we have Ms. Carreno, the president of Interactive Advertising Bureau of Canada, and Mr. Kardash, partner with Osler, Hoskin and Harcourt.

Ms. Sonia Carreno (President, Interactive Advertising Bureau of Canada): Good afternoon, Mr. Chair and honourable members.

My name is Sonia Carreno, and I am the president of the Interactive Advertising Bureau of Canada. I am accompanied today by Adam Kardash. Adam is counsel to the IAB and chairs the national privacy and data management practice at the law firm Osler, Hoskin & Harcourt. We both thank you very much for the opportunity to speak with you this afternoon.

By way of background, IAB Canada is a not-for-profit association exclusively dedicated to the development and promotion of the rapidly growing digital marketing and advertising sector in Canada. IAB Canada represents over 250 of Canada's most well-known and respected stakeholders in the digital advertising and marketing sector, including numerous small and medium-sized enterprises.

Companies in the digital advertising and marketing sector offer a wide range of highly innovative products and services, including valuable service offerings to individual Canadians. This sector is intensely competitive, and the long-term success of its members is fundamentally predicated on their ability to continually design, develop, offer, and improve valuable digital products and services. Our members are data companies. The products and services offered by our members inherently require the processing of data, and often this data includes personal information. Our members recognize that their long-term success as commercial enterprises requires the respectful treatment of personal information in their custody and control, which includes complying with PIPEDA and other applicable privacy legislation.

I'm going to turn it over now to Adam Kardash to talk a little bit more about PIPEDA's framework.

Mr. Adam Kardash (Partner, Privacy and Data Management, Osler, Hoskin and Harcourt LLP, Interactive Advertising Bureau of Canada): Thank you.

The central theme of our comments this afternoon is our view that PIPEDA's statutory framework is very well suited for innovation.

While there are certain challenges in applying PIPEDA's fair information principles in today's highly dynamic data environment, it is clear that the overall statute has worked and continues to work as an elegant and effective model for organizations to respectfully treat personal information in the course of developing and offering highly innovative and valuable services, products, and features.

The lasting success of PIPEDA in this regard, and the reason PIPEDA can continue to help foster innovation, is largely grounded within the following key features of the statutory framework. PIPEDA is predicated on balancing the interests of individuals and the legitimate need for organizations to process personal information, a balancing that is critical in today's digital economy. PIPEDA's rules are drafted in a principles-based, technologically neutral fashion. Another feature is PIPEDA's accountability model.

PIPEDA remains particularly effective today because it was drafted in a technologically neutral and sectoral-agnostic fashion, and it is well suited to address the seemingly novel privacy considerations that may be raised by new technological developments. As any amendments to the statute are reviewed and considered, it is critically important that PIPEDA remain drafted in a technologically neutral manner, since any statutory requirement that is drafted to focus on a certain data element, process, or ecosystem risks being obsolete and out of date soon after it comes into force.

It is also important to note that while PIPEDA is often referred to as a consent-based statute, in practice, the most powerful feature of PIPEDA is its accountability model, as it provides rules that govern the entire life cycle of an organization's personal information processing. It is important to frame PIPEDA's consent rule as just one part of an organization's broader obligations under the act.

PIPEDA's accountability model is elegant and effective since it holds organizations responsible for their personal information practices and does so in a non-prescriptive manner. The accountability model needs to remain non-prescriptive in nature as this will afford organizations the flexibility to tailor, adapt, and refine their privacy programs in a practical manner that is suitable to the industry sector, size of the organization, nature of a given organization's personal information practices, and evolving commercial needs.

I'm now going to offer a few comments on the continuing viability of PIPEDA's consent requirement, as you've already heard.

As the committee has heard from previous witnesses—

The Vice-Chair (Mr. Nathaniel Erskine-Smith): If I can jump in just one second, bells have begun ringing, so we have 30 minutes until the vote. We need unanimous consent to continue going. We're obviously very close to the chamber, so I propose that Mr. Kardash conclude and we limit the first round to five minutes each. We'll get a first round in, go vote, and come back and see where we can pick up from there. Does that sound fair?

All right, that's how we'll proceed.

Continue, Mr. Kardash.

● (1600)

Mr. Adam Kardash: Thank you.

As the committee has heard from previous witnesses, there is an increasingly active discourse and growing recognition in the global privacy arena of the legal and practical challenges posed by the statutory consent requirement in an evolving data environment, but despite these challenges, as you have just heard, it's important to highlight that in many contexts PIPEDA's current consent requirement is and continues to be a legally viable and practical means of authority under PIPEDA for organizations to collect, use, and disclose personal information in today's data environment using what the Federal Court of Appeal has referred to as a flexible, pragmatic, common sense approach.

A prime example of the viability of PIPEDA's current consent requirement within a complex data ecosystem is in the context of the collection and use of information for the purposes of online behavioural advertising, or what is now more commonly referred to as interest-based advertising.

Based in large part on guidance issued by the Office of the Privacy Commissioner of Canada relating to OBA, the Digital Advertising Alliance of Canada, a not-for-profit organization and consortium comprising IAB Canada and seven other leading national advertising and marketing trade associations, developed and launched a program called AdChoices, the Canadian self-regulatory program for online behavioural advertising. Dozens of key players in the online and mobile advertising ecosystem have signed up for the DAAC's AdChoices program, all with the view of helping to enhance their respective compliance with PIPEDA and, overall, to enhance the trust of all stakeholders in the Canadian digital advertising arena.

PIPEDA's consent requirement also establishes a helpful framework for the processing of personal information involved in data analytics or what is referred to as big data processing. Data analysis is an inherent part of research development, and the insights derived from big data analytics now being conducted by companies are leading to profound and unprecedented levels of benefits and improvements in efficiency and convenience, and new products and offerings. PIPEDA's consent provisions, specifically principle 4.3.3, helpfully contemplate circumstances in which organizations must process personal information in connection with providing a product or service offering, such as the case in which data analytics is being conducted for research and development.

In a written submission, which we're providing to the committee, we offer several recommendations for amendments to PIPEDA for the committee's consideration, and I'll touch upon them briefly this afternoon.

While PIPEDA's framework remains viable, it's critically important to ensure that PIPEDA in the long term is able to address the challenges of the consent model as these challenges may become more acute with increasingly complex data ecosystems such as the Internet of things. PIPEDA will impede innovation if companies do not have certainty regarding the legal viability of their authority under PIPEDA to process personal information. Certain of these challenges can be addressed by surgically amending PIPEDA to expand the circumstances in which organizations can collect, use, or disclose without consent. We are of the view that the amendments to PIPEDA, if appropriately drafted, could address the range of challenges in a manner that balances the interests of all stakeholders.

Very briefly, these proposed amendments include, as you heard just a few minutes ago, the following:

First, broadening the permissible grounds under PIPEDA to collect, use, or disclose personal information without consent where there are legitimate business interests of the organization.

Second, modifying the wording of PIPEDA's research exception to expressly include analytics.

Third, modernizing the exceptions to consent for collection, use, and disclosure for publicly available information.

And finally, expressly authorizing organizations to de-identify or anonymize personal information without the necessity of consent.

We invite questions from the committee with respect to any of these recommendations.

I have just one final comment. I want to offer views regarding the sufficiency of the OPC's current enforcement powers under PIPEDA.

PIPEDA currently provides the OPC with a suite of powers to enforce compliance with the act, and despite the calls for enhanced enforcement powers that this committee has heard, we feel strongly that there do not appear to be compelling examples illustrating precisely why the existing arsenal of OPC powers is insufficient.

On the contrary, to date the OPC has been remarkably successful in carrying out its statutory mandate under PIPEDA. The OPC has been highly respected in the international privacy arena for years as a direct result of its enforcement activities. In our view, the OPC does not need to enhance or supplement its enforcement mechanism.

Moreover, given PIPEDA's balancing of interests framework, a remarkable shortcoming of the statutory enforcement regime under PIPEDA is that the statute does not include an express right for organizations to challenge OPC's exercise of its current enforcement powers.

For instance, organizations have no express right under the statute to refer a subject matter to the Federal Court.

● (1605)

We therefore recommend that PIPEDA be amended to provide organizations with an express right under the statute to challenge the OPC's exercise of its current enforcement powers.

I thank you again for the opportunity to speak with you this afternoon. We'd be pleased to respond to any questions from the committee.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you to IAB Canada for that presentation.

We'll begin the five-minute round with Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon. Thank you very much for coming here.

Prior to your arrival here, several witnesses have come before this committee.

I want to talk specifically about the GDPR, which, as you know, is going to come into effect in May 2018. So far, there's an adequacy status for PIPEDA with our European friends. Since the GDPR is going to come into place in May 2018, we may have to make some changes, specifically regarding the right to be forgotten. Since you represent the private sector, what sorts of things do you foresee should be changed to make sure that our laws are similarly adequate to their laws?

That's an open question.

Mr. Adam Kardash: I'm happy to begin.

Mr. Raj Saini: Sure.

Mr. Adam Kardash: My first comment would be that the GDPR is an incredibly complex piece of legislation. It is still being actively reviewed, and there is a tremendous effort globally to understand what certain aspects of the legislation even mean. We're just getting policy guidance from regulatory authorities in the EU, who are starting to elaborate on what some of the features mean.

Having said that, having had the opportunity to go through the act specifically with respect to client mandates, and having spent years working with the data, I feel that there are vast aspects of PIPEDA that would be substantially similar. There will be a distinction for sure in the sheer prescriptive nature—the GDPR is much lengthier and more prescriptive—but there are aspects under PIPEDA's accountability regime, which has been held up as a model globally, that I think will remain intact and will stand the test of time.

The upshot is that adequacy is a matter of EU consideration and, at a minimum, I think that very careful consideration and a fair amount of time should be taken to understand several of the elements, which even the Office of the Privacy Commissioner of Canada has cited do not expressly exist. There are elements, including the one you've cited—the right to be forgotten—and there are others that don't exist in the GDPR.

Our view, at least practically with clients, has been that certainly with respect to adequacy, while it's a very helpful basis on which to allow for transborder data flows, there are other mechanisms that allow for transborder data flows and that can be accommodated. That's number one. Number two, it would be very important not to enter into a rash revision to the statutory framework until we really understand what some of these provisions mean, and that might take a fair bit of time. At a minimum, we're going to be getting opinions in due course from EU authorities as to the sufficiency. That process will afford us an opportunity to understand the nuance and distinction of where we see the shortcomings, and since it's an EU consideration, that should serve as a starting point for consideration of where the actual gaps are.

I'll just make one point. I mentioned it before but I cannot overstress it. There are vast swaths of the GDPR that, I feel, could be read into our existing framework. I think that, as Canadians, we should feel very proud of how our statute has stood the test of time in the wake of substantial change globally.

Mr. Randy Bundus: I'd like to build on the “right to be forgotten” concept. We have to deal with that very carefully going into the future so that it does not result in unintended consequences.

I have concerns on two fronts.

Insurance fraud is a big issue in our industry. It's a concern. If someone demands the right to be forgotten as a means to perpetuate an insurance fraud, that would be a tragic outcome. We'll have to address it when we go forward with PIPEDA to make sure we don't have any of those unintended consequences.

In addition, with the right to be forgotten, we want to make sure that if the person seeking the right to be forgotten—I'm talking in the insurance context—perhaps approaches their insurer and says they don't want to have any of their records in their files.... They may have had a liability policy with this particular insurer, which 15 or 20 years later, say, might be called upon and is needed by that particular customer. It would be very tragic for that customer if, in seeking the right to be forgotten by this insurer, they would forgo some rights to claim it against that insurance policy when it's needed most.

● (1610)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): You have 20 seconds left in your time, but given....

Mr. Raj Saini: I can give it to somebody else.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): You're so very generous.

Mr. Kelly, go ahead for five minutes.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): Thank you for keeping it under the five, Raj.

I would like to really quickly simplify something for the record and make sure that I've understood all three witness groups together. All three are in favour of retention of the ombudsman model, and none of our witnesses today favour order-making power for the OPC. Is that correct?

All witnesses: Agreed.

Mr. Pat Kelly: Thanks.

Perhaps then, Mr. Kardash, I'll continue with you just a little bit here. I was trying to note your four recommendations. You went quite quickly, and I want to make sure that I understood them correctly. Perhaps I'll let you expand a little bit. You said you had four recommendations. One was to broaden the consent model to include the ability to act without consent where there's a business interest.

In fact, maybe I'll let you just repeat those four points and make sure that we're clear.

Mr. Adam Kardash: I'd be pleased to do so.

We offered four. All of them relate to the ability to process certain data—to collect, use, and disclose personal information—without consent. One of them, as mentioned by my colleague as well, was to create an exception for legitimate interest. This would allow organizations to collect, use, or disclose personal information without consent where there's deemed to be legitimate interest. This is something that's more under EU law right now. That's number one.

Mr. Pat Kelly: That's one.

Mr. Adam Kardash: Number two, there's currently an exception under PIPEDA in paragraph 7(2)(c) for the use of data for statistical and scholarly study and research. It's just for the use of data. The wording, in my view, allows for the conducting, for example, of analytics, which is a form of research, but it would be very helpful to have clarification for companies to do what they've been doing for decades already. Now, there would be even more profound benefits to Canadians to having the clarity that, just for the use of data, an expansion of paragraph 7(2)(c) of PIPEDA would expressly permit data analytics as a type of internal research, like research and development, without consent.

Third, I cited the "publicly available" exception. As the committee is aware, there are exceptions under PIPEDA for the collection, use, or disclosure of certain publicly available information. These are very specific provisions. Just by way of example, one of the publicly available exceptions for which you don't require consent is the name, address, and telephone number of someone in relation to "a subscriber that appears in a telephone directory". That made sense 20 years ago. It just doesn't make sense in the digital economy. So I'm talking about expanding it and making it technologically neutral wording that's more appropriate.

Mr. Pat Kelly: Okay.

Mr. Adam Kardash: Finally I mentioned, consistent with my colleagues, that organizations now engage in a practice referred to as de-identification or anonymization or obfuscation, which is extraordinary helpful to protect the privacy interests of individuals while it's processing, but it protects individuals because the data can be rendered non-identifiable. There's an open question—and this raged in Europe for years—as to whether you need authority to actually just de-identify the information. Our respectful suggestion to the committee is that this discussion be put to rest. Clarity should be required, and organizations should be able to take the step to safeguard the data and should be able to de-identify or anonymize data without consent, rather than having to seek consent to de-identify. This is a helpful safeguarding measure, so that's the basic point.

Mr. Pat Kelly: Thank you.

Do I have a moment left?

The Vice-Chair (Mr. Nathaniel Erskine-Smith): You have one minute.

Mr. Pat Kelly: I will just quickly perhaps ask our other two organizations to comment on the suggestion about amending PIPEDA to allow businesses or regulated industries to challenge the OPC through the Federal Court and the recommendation that was made for an amendment to allow for this.

Could I have the other two organizations comment on that recommendation?

Mr. Frank Zinatelli: I had not considered that, but it seems like a good suggestion that this committee should take a look at.

● (1615)

Mr. Pat Kelly: Thank you.

Mr. Randy Bundus: I share Frank's view of our industry. I hadn't thought of it either, but absolutely it would be an interesting proposition to consider.

Mr. Pat Kelly: Thank you.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you.

Madame Trudel, you have five minutes.

[*Translation*]

Ms. Karine Trudel (Jonquière, NDP): Thank you, Mr. Chair.

I want to thank the witnesses for their presentation.

My question is general.

We have talked a lot about the right to be forgotten at previous meetings, a subject of great interest to me. In many cases, this issue likely involves individuals aged 18 and over, but we must also remember that children have access to technology today and that they leave traces. The ease with which they can use the various applications available on phones and tablets means they are not always aware of the traces they leave in social media.

We touched earlier on the fact that the right to be forgotten could lead to the disappearance of certain information that might otherwise be used 20 or 30 years later. How can we achieve a balance between the need to preserve certain information and the ability to make other information disappear, or the result of certain acts by individuals that could not be considered fraudulent or criminal? How in your opinion could we combine these two aspects, while still allowing the right to be forgotten for certain information that could disappear? I would like to hear your thoughts on that.

[*English*]

Mr. Frank Zinatelli: I'll make an initial comment.

In our industry, the life and health insurance industry, we enter into contracts that sometimes last 30, 40, or 50 years. There is information that we collect as part of the application process that could be relevant 40 or 50 years down the road. There is this type of information we collect, which is legitimate information we need for our assessments, and then there is also information that is legally required to be collected, for example in the context of anti-money laundering, etc.

Definitely, for legal requirements or information that is required for a legitimate purpose, it would be very damaging if suddenly an individual could simply say, “I don't want that information to be out there anymore.” There may be circumstances, as you said, relating to children, etc. that could be looked at. Certainly, if it is legitimate information that one needs, and if a person enters into a contract and provides that information, they simply should not have the choice of then saying “Let's forget about all that.” I'm sure there are other circumstances in which information needs to be retained for valid reasons.

In my view, it would have to meet a really high threshold for anything to be forgotten, as it were.

Mr. Randy Bundus: You've raised a very interesting question, and it is going to be very difficult to come to the right spot for an answer. Legislatively, I'm not sure how you would manage that.

We are dealing with young people—that's one example—and they want the right to be forgotten. Perhaps there is an answer in legitimate business interests: If there is a legitimate business interest that's necessary for the relationship of conducting the commercial business, maybe an exception for that should be made to the right to be forgotten. And there are other areas.

My view is that the concern we have with people who want the right to be forgotten is rarely in areas that would really have a business relationship effect. That's the big question we face going forward, I agree.

Mr. Adam Kardash: I agree with both colleagues.

Striking a balance is difficult. I'm not sure that the answer is necessarily embedding that principle within a statutory framework. There is an existing framework right now that allows for respectful treatment of the life cycle of data, including data retention principles. These are very difficult aspects to enshrine without knowing the unintended consequences of having them embedded.

In the committee's consideration of this, I think we need to be very careful moving forward. In previous testimony, you heard about freedom of expression considerations, which I think are also very ripe for detailed consideration in that type of corporate principle to the legislative scheme.

● (1620)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you very much for that.

We will break now and reconvene after the vote has concluded.

● (1620)

(Pause)

● (1640)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): All right. Let's pick up where we left off.

We will conclude our first round with Mr. Long for five minutes.

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

Thank you to our witnesses. I apologize on behalf of everyone for the votes and the delays. Your presentations were very informative.

To Sonia and Adam, I want to focus on the subject that I've been focusing on for the last while, and that's children's rights under PIPEDA and I guess the lack of clarification around how we're going to protect our children in terms of meaningful consent. I don't have to tell you that there was a recent sweep of websites, 62% of which share information. My kids are older, but I have friends with younger kids who are on their iPads and Notebooks and stuff, and who are on sites.

I just want the two of you to tell me, if you will, how we're going to protect our children. If you look at COPPA in the States, I think it's a lot more defined with respect to protection and meaningful consent by kids under 13 years old. Can you elaborate on what modifications and amendments we can make to PIPEDA to protect our children?

Perhaps you can start, Adam.

● (1645)

Mr. Adam Kardash: I'm happy to answer that.

In the context of numerous client engagements, we've had to address that exact issue. The best place to start, actually, is with your reference to COPPA. Under PIPEDA, as we've heard throughout the afternoon, there's a consent-based requirement. Individuals under the age of 13 would not have the capacity to provide consent. Similar to COPPA, but without any wording, if you are 10 or 11 or 12.... Let's take an eight-year-old by way of example. You would need the consent of a guardian or a parent in order to provide the authority for that particular processing.

In common law, consent of minors generally is one of decision-making capacity, so it will be highly contextual when you get to roughly the COPPA-related age of maybe 12 or 13, all the way up to the age of majority, which varies. Legally you'll have to consider whether there's ability to even obtain context in the circumstance. Regardless, PIPEDA contains a whole suite of rules that are, as I mentioned, sectorally and otherwise agnostic.

So these rules would protect sensitive data the way they would protect any other type of sensitive data—

Mr. Wayne Long: Just let me jump in here. With respect to meaningful consent and children, we talk about eight-year-olds and 12-year-olds. Should there be different levels and layers—i.e., where children eight to 10 have certain parental consent? Can 12- to 15-year-olds give meaningful consent, in your opinion?

Mr. Adam Kardash: I have two comments.

With respect to your first question, I think there are times when it seems as though it would be helpful to have different age gates for different types of scenarios, but given the explosion of the array of different types of services and offerings and context, it's incredibly difficult to operationalize those. PIPEDA has been excellent because it's been agnostic and not prescriptive.

That being said, can a 12- or 13-year-old give consent? It could be in a decision-making capacity, but certainly those under 12, the same way they wouldn't otherwise have capacity if incapacitated by other means, wouldn't be able to provide a valid consent.

Mr. Wayne Long: Okay.

Do you have anything to add to that?

Ms. Sonia Carreno: I don't have any further comments. I do know that our counsel and our committees are talking at length about the subject of children in general. I think there's a lot of policy being written right now, just in the private sector in general, to protect children. They're doing the best they can, and they are sharing ideas with one another.

Mr. Wayne Long: Thank you.

I'll switch to the insurance side of the table here. We've obviously had some insurance brokers up here on the Hill in the last couple of days. Correct me if I'm wrong, but I think it's safe to say that the insurance industry is an older industry. Would you say that? Is the average age for a lot of the independent insurance brokers older, at around 50 or 50 plus?

Mr. Randy Bundus: We represent the actual manufacturers, the insurers themselves, but I would have to suggest that it seems to be the case that brokers are an older group, yes.

Mr. Wayne Long: Is there concern that insurers aren't being proactive enough in changing their ways or technologies?

Again, I think that industries and companies need to be proactive with respect to what's coming with the GDPR and different things, not to let it come to them but to be proactive. Do you think the industry is being...?

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We're at the end of the five minutes, so perhaps you could make your answer as brief as possible.

Mr. Randy Bundus: I'll let my colleague Mr. Lingard answer that question.

Mr. Steven Lingard (Director, Legal Services, and Chief Privacy Officer, Insurance Bureau of Canada): Thank you very much for the question.

I think our industry is actually being proactive and innovative. An example is usage-based insurance, which is something that has been sold in a number of other countries.

Now, we are finding that just as P and C insurers are regulated at the provincial level for market conduct, some of the regulators are not quite as forward-thinking as we would like them to be. We're finding that there are hurdles being raised against insurers innovating and providing new products.

● (1650)

Mr. Wayne Long: What kind of hurdles?

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We'll come back to you, Mr. Long. I think we'll probably have time at the end.

Mr. Kelly, go ahead, please, for five minutes.

Mr. Pat Kelly: Thank you.

If I may, I'll start with the Insurance Bureau of Canada.

Is the membership in your organization voluntary or compulsory for industry members?

Mr. Randy Bundus: The membership is voluntary.

Mr. Pat Kelly: Broadly, what percentage of the industry do you represent? Is it all or most...?

Mr. Randy Bundus: Ninety per cent of the property and casualty premiums written in Canada by private insurers are written by members of IBC.

Mr. Pat Kelly: Excellent.

I noted in your opening remarks that you made reference to the fact that your industry is highly regulated, and certainly by no means just by PIPEDA. You are regulated by the insurance acts of various provinces as well as by OSFI, which has significant powers.

You mentioned your internal ombudsman process as well. Do you have a lot of privacy complaints directed to your internal ombudsman?

Mr. Steven Lingard: The ombudsmen we were referring to are those at individual companies. We don't have records for those complaints. I'm sorry that we can't provide any information about that.

Mr. Pat Kelly: Okay, so each individual member has its own ombudsman—

Mr. Steven Lingard: That's correct.

Mr. Pat Kelly: —and it's part of your own best practices to have an ombudsman, or it's a requirement of your....

Mr. Steven Lingard: Actually, it's required under the provincial insurance acts. Not in all provinces, but I know that in Ontario there is a requirement for companies to have an ombudsman, with responsibility for handling customer or consumer complaints. We don't have any knowledge of the number of complaints or the types of complaints that come in.

Mr. Pat Kelly: If these various ombudsmen were failing to provide adequate recourse to their members, would you hear about it as a larger industry group? Do you know whether privacy complaints are an issue?

Mr. Steven Lingard: I believe that we would hear about it, because we do have a good working relationship with the provincial superintendents.

At the end of the day, if there is a complaint that cannot be resolved or is not resolved with the insurer, the consumer will go to the superintendent's office.

Mr. Pat Kelly: Right.

Mr. Steven Lingard: In Ontario, that is FSCO. We would hear back that something was not being handled properly and that FSCO was going to do something about it.

Mr. Pat Kelly: To your knowledge, does the OPC receive a lot of privacy complaints from your industry?

Mr. Steven Lingard: We haven't had a meeting with the OPC in a year or so. We used to have annual meetings with them, and we got updates.

My understanding is that there are not very many complaints made to the OPC, or to the Alberta or B.C. privacy commissioners. I think we have a pretty good track record in that regard.

Mr. Pat Kelly: Good.

Do you attribute the fact that you have gotten out of the annual meetings to there being an absence of concern or issue? Is it a matter of them not getting to you because they're too busy with other things, or do you think that things are pretty good and that your industry, perhaps, is not a problem?

Mr. Steven Lingard: We attribute it to the fact that, I think, our industry does a very good job, as was mentioned earlier, I believe, by Mr. Zinatelli of CLHIA.

Insurers have long known the importance of protecting the privacy and personal information of their customers. In the meetings we had with OPC, with Jennifer Stoddart when she was there, with Elizabeth Denham when she was in B.C., and with Frank Work and Jill Clayton in Alberta, the number of privacy complaints that we were told about was minimal. There were a handful at best over the course of a year. Those were in the first couple of years of PIPEDA or the PIPAs coming into force. The numbers dropped after that.

Mr. Pat Kelly: Right.

You make a good point that you're a provincially regulated industry. Many of your members also have provincial privacy regulation that they have to comply with, a separate regulation as well as the various ombudsmen or enforcement mechanisms that would exist.

So, do you think you have a fairly good culture in your industry regarding the protection of privacy and the knowledge of the importance of it?

● (1655)

Mr. Steven Lingard: Yes, I do. I think we have a very good culture. I think we have strong practices in place. I've said before, and I'll say it again: insurers appreciate and understand the need for protecting the information of their customers. I think we have a very good track record in that regard.

Mr. Pat Kelly: Okay.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you.

That concludes your five minutes, Mr. Kelly.

We'll go to Mr. Saini and Mr. Long, who will be splitting the five-minute time.

Mr. Raj Saini: There's just one follow-up question I didn't get a chance to ask.

With your testimony and with testimony that we've heard before, there seems to be some hesitation in giving the commissioner more enforcement powers. I just want to understand why you feel there should be that hesitation. Why should we not give the commissioner more and more powers to enforce breaches of privacy especially when it's not going to be detrimental to those companies that are following best practices?

I'm just confused about why there's hesitation especially when we know in Europe, especially with the GDPR, the maximum penalty is 4% of general turnover, or up to 20 million euros. Why is there hesitation here in Canada to have a robust enforcement policy?

Ms. Anny Duval: I would probably go back to the words of Jennifer Stoddart, who, as you know, is the ex-Privacy Commissioner of Canada. She was on a panel recently at a national privacy conference that I attended. It was pointed out to her that there are no examples of bad situations. She said there is one. It's

[*Translation*]

Quebec's access to information commission, the CAIQ or Commission d'accès à l'information du Québec,

[*English*]

which has turned into an administrative tribunal. She said that when she looks at the commission in Quebec, she sees that it represents the dangers that the companies are afraid of. She even mentioned.... I'll say this part in French because she was speaking French. She said that

[*Translation*]

the CAIQ decision-makers sign their decisions as administrative judges.

[*English*]

I'm happy to repeat that.

Mr. Wayne Long: Could you repeat that more slowly?

Ms. Anny Duval: No worries.

[*Translation*]

She said that the CAIQ decision-makers sign their decisions as administrative judges. She said in particular that this title is not even in the enabling statute.

[*English*]

So to her, it's a slippery slope of what you could be looking at and be afraid of in the future.

Mr. Adam Kardash: I would just reiterate that in dealing personally with scores of investigations, I have found that there is a benefit to having an ombudsman model that can be unleashed to have even greater benefits, to allow for what I would call a conversation. Unlike other types of statutes in which there are prescriptive requirements, etc., the implementation of a privacy program in a manner that respectfully treats data is a nuanced conversation. It requires a dialogue and it requires that dialogue to be with multiple stakeholders.

An ombudsman model facilitates that. If you're going to change to a scenario in which you start providing the former ombudsman with more enforcement powers, that will change the context of that discussion. It just will. Whether it would come to the extreme, as was just cited, remains to be seen. But it would change.

Going back to the comments that we made, we have had tremendous success with the OPC. It has been tremendously successful in enforcing the act. It's respected all over the world because of this. What we haven't seen, and what I think is really important to consider, is the specific circumstances in which the existing suite of powers has been insufficient. I'm not saying that those don't exist. It's just that those haven't been discussed. There's a very wide range and they work quite well.

The mere fact that there might be another regime that has powers in and of itself didn't strike our committee, at least, as something that's compelling, especially with the benefits that could be afforded by the ombudsman model. I think Canada could lead globally. I think the ombudsman model is a way to do so. We've felt that way for years.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): There are still 45 seconds left.

Mr. Wayne Long: Mr. Lingard, I just want to continue. You mentioned the industry, insurers, face hurdles at times with respect to being prepared and getting ready.

What, as an industry, are you doing to make sure that insurers are ready for the rapidly changing rules and regulations?

● (1700)

Mr. Steven Lingard: We're working with our members to ensure that they are current. An example of something we're working on is electronic proof of auto insurance. You'd think it would be fairly simple. Rather than having to show your pink card to law enforcement—

Mr. Wayne Long: It drives me crazy.

Mr. Steven Lingard: —you could perhaps show your cellphone, like a boarding pass when you go to the airport. That has prompted considerable discussion with some of the provincial governments and some of the provincial privacy commissioners. The federal commissioner has not become involved yet.

It looks as though the process could take months, if not years, to come up with a resolution. That is not in anyone's best interest. We appreciate the need for thoughtful consideration of the privacy issues, but the process is moving very slowly. It's one that we would like to move more quickly. The technology is from 10 years ago, but why can't we use it now?

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much. That concludes that five-minute round.

We're with Mr. Jeneroux for five minutes.

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

Thank you for being here today.

I have one question, and maybe I'll start with Mr. Bundus and Mr. Lingard, and then anybody else who wants to weigh in as well.

I want to talk about the challenges when it comes to preventing privacy breaches, and perhaps any recommendations or observations that you might have from your side of it to make sure we have that information so we can feed it back to our report.

Mr. Randy Bundus: It is a very important issue for members of our industry. As insurers who insure against privacy breaches through cyber liability insurance, they're extremely interested in not only preventing privacy breaches by their own operations but also providing advice to customers to avoid privacy breaches on their front. It's a very new product coming out and a lot of work has to be done to educate users of the systems to make sure the insurance can be sold. As time goes on, new skills, ideas, and perhaps checklists will be developed by insurers to make that product more insurable. That's where we're at.

Mr. Matt Jeneroux: Do you have any recommendations that you'd like to see now, or are you going to wait and see?

Mr. Randy Bundus: Unfortunately, we're in a wait-and-see situation.

Mr. Matt Jeneroux: All right. Does anybody else have a comment?

Mr. Adam Kardash: I want to clarify if the question is whether there are recommendations for helping organizations respond to incidents that would be incorporated into the statutory regime or it is a more general question.

Mr. Matt Jeneroux: It's both. You've opened it up, so let's do that.

Mr. Adam Kardash: As the committee is aware, we've had these discussions, and PIPEDA has a pending statutory security breach notification requirement, which will come into effect once the regulations are put out for comment and then ultimately implemented.

One of the comments that industry has made about those regulations is that it's incredibly important to keep them not prescriptive but to give some flexibility. But the statutory safeguarding requirement in PIPEDA is simple. In essence, it's a couple of lines. You need to have reasonable security safeguards. There is jurisprudence already that this means it doesn't have to be perfect, but what is reasonable? Reasonable is informed by its standards. There's a wealth of information security governance standards out there that especially entities in the financial services sector, insurance and financial services, will follow. Within those, it's a basic concept of information security governance.

Now, especially in the wake of the global ransomware attack, which was another wake-up call globally about this, it's a matter of vigilance with respect to the establishment of a continuous information security governance program. Within that, you not only have policies and procedures that you continually review, monitor, and independently test, you also have incident response and readiness plans that you implemented. If you treat it like a piece of paper and file it, it's not worth the paper it's written on. It's a living, breathing type of framework to address proactively information security concerns that not only threaten individual companies but are a systemic threat to the entire country.

Mr. Frank Zinatelli: We've recognized for many years that safeguarding is really an essential principle. In fact, it has to be one of the top two of the 10 principles that make up privacy legislation, so it's always been abided by.

Now, in recent years, we've seen, of course, cyber issues associated with that, and certainly within our industry there's been more work done on the cyber side during the last three to four years. Indeed, we have committees made up of member company folks to be up to date on the most recent developments. We work with our financial services regulators so that they're apprised of what safeguards companies have in place, but it's an ongoing battle.

● (1705)

Mr. Matt Jeneroux: Okay.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): If it's okay with the committee, I have two or three questions.

Is that all right?

Some hon. members: Yes.

The Chair: My first question is to Mr. Kardash. You suggested keeping the status quo with respect to the Privacy Commissioner's powers, and you mentioned that it's a dialogue, and that strikes me as a fair point. Now, if the commissioner has entered into a compliance agreement with a third party, and that third party ignores the compliance agreement, at that point shouldn't there be fines or new powers for the commissioner?

Mr. Adam Kardash: Yes, those compliance agreements are voluntary for organizations to enter into. There are certain reasons it would make sense for organizations to enter into them with the OPC, like a binding agreement, just as you would have in the private sector, so that would make sense in its current format.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): We had a lawyer from a different firm appear before us who suggested that the right of erasure might be fair for those 16 and under. Do you think that would be a fair compromise for this committee?

Mr. Adam Kardash: We've had to work on several dozen client mandates in which we were dealing with concepts in the EU, with global companies, and importing them. These are very tricky, and what seemed to be the case in every single context is that that was unnecessary for the protection of privacy.

We have an existing framework that works fine, and it didn't seem necessary at all in the circumstances.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thank you very much.

Australia has a law proposal—I don't think it's enacted yet—that would make it an offence to de-identify government datasets. You mentioned that de-identification and anonymization are important. Do you think we should not only be looking at rules that would expressly authorize de-identification but also looking at whether to make it an offence or otherwise prohibit re-identification?

Mr. Adam Kardash: Yes. We recommend having something similar to what exists in provincial privacy statutes: an express deemed authorization for organizations to be able to de-identify. I would suggest that the frameworks already exist. If an individual or a corporation were to be re-identifying some dataset, they would have no authority under PIPEDA or provincial legislation to do so. They would be barred from just outwardly in a vacuum re-identifying, so they would have an existing framework to deal with that, and there would be remedies under the federal or provincial statutes to address that.

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Lastly, you mentioned a new exception, legitimate business interest. I understand PIPEDA, but you know far more with respect to implied consent, so perhaps you could explain to this committee the difference between how the law currently operates in relation to implied consent and how this exception of legitimate business interest would add to our notion of implied consent.

Mr. Adam Kardash: Yes, thank you.

It's a critically important question. There are elements to a valid consent, whether expressed or implied. One of the elements required is that the consent be revocable. For instance, if you provide your consent for secondary marketing, there is the obligation to honour your withdrawal or your “unsubscribe” for that.

There are a myriad of circumstances right now in which providing a revocability for a consent process is very difficult in practice. We have a stunningly complex data ecosystem in which the ability to even contemplate how you would give effect to the withdrawal of consent is going to be very difficult. The Internet of things is one of those examples. If it were carefully constructed—and we were very careful, and you will see this in our written submissions—with a balancing of interests similar to that in the EU, this would allow organizations the ability to process data for legitimate purposes and, at the same time, respect privacy interests.

● (1710)

The Vice-Chair (Mr. Nathaniel Erskine-Smith): Thanks very much.

I'm out of time.

Madam Trudel, you have three minutes should you wish to use them.

[*Translation*]

Ms. Karine Trudel: Thank you.

I would like to return to you, Mr. Kardash, for a clarification.

You referred earlier to the right to challenge the commissioner. I would like further explanation as to whether you are referring to organizations that want to challenge the commissioner—perhaps it is a translation issue. I simply want to understand what you mean by the “right to challenge”.

[*English*]

Mr. Adam Kardash: Sure. Right now, when an organization is the subject of a complaint, the Office of the Privacy Commissioner will commence and carry out an investigation. At the conclusion of that investigation, it will issue a report of findings. These are non-binding findings, and there are express rights in the statute right now for the complainant, the individual who launched the complaint, or the Privacy Commissioner to take that to Federal Court. There is no right for organizations to do the same. It doesn't exist.

There would be rights under administrative law to do so, but organizations don't have the express right to do so. It just doesn't exist in there. So in essence, the remedies at the Federal Court level for both the complainant and a privacy regulatory authority are what are set out in the act.

[*Translation*]

Ms. Karine Trudel: So you recommend that the organization should have the right to challenge. Is that correct?

[*English*]

Mr. Adam Kardash: I think it's fair for due process to have rights for organizations balanced. The whole statute is predicated on a balancing. Privacy under PIPEDA is not an absolute right. There's a balance in the preamble of the act and in section 5.3 of the act for the protection of privacy interests to be balanced with the collection, use, and disclosure of personal information for reasonable purposes. Consistent with the balancing of interests, it gives organizations the right to challenge a decision.

One could see in circumstances right now how once the security breach notification rules come into effect, organizations could be fined $100,000 for failure to notify in circumstances where there's a real risk of significant harm. Where are the rights for organizations to challenge something that could have mammoth implications for those that are the subject of such a fine? If organizations could be fined, the only thing I'm suggesting is the express right, within the statute, for organizations to challenge that.

[*Translation*]

Ms. Karine Trudel: Thank you.

[*English*]

The Vice-Chair (Mr. Nathaniel Erskine-Smith): I want to thank all of our witnesses today. That will conclude our public meeting. We will suspend for a few minutes and return in camera.

[*Proceedings continue in camera*]