HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 048 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, February 21, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, February 21, 2017

● (1530)

[*English*]

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

I notice that while not everyone is at the table, everyone appears to be in the room. We'll get going, because I have a couple of public service announcements before we hear from our witnesses.

Colleagues, I'm sure you're aware of this, but in case you're not, I'll do a friendly reminder. Karen Shepherd, the outgoing Lobbying Commissioner, is having a farewell reception today. If you get an opportunity, it's at the Mill Street Brew Pub on Wellington Street, just down by the bridge, if I remember correctly. It goes from 3:30 until 7 tonight. I'll do my best to make my way over there on behalf of the committee, but if other committee members wish to go, I think that would be more than appropriate.

Colleagues, we have a very distinguished panel of witnesses today, all appearing by video conference. From the Office of the Information and Privacy Commissioner for British Columbia, we have Mr. Drew McArthur, the acting commissioner. We welcome you. Also from that office, we have Michael McEvoy, the deputy commissioner. From the Office of the Information and Privacy Commissioner of Alberta, we have again, Jill Clayton, who has appeared before the committee several times. She has some assistance there, as well. Finally, from the Commission d'accès à l'information du Québec, we have Cynthia Chassigneux, the administrative judge, who is appearing by video conference as well.

We'll have 10 minutes of opening remarks by each group. That will take up about the first 30 minutes. Then we'll proceed to our questioning.

Keep in mind, colleagues, that with PIPEDA, this is about the private sector. If we can focus on that in our questioning, we'll have a great discussion.

Who's going first, Mr. McArthur or Mr. McEvoy?

Mr. Michael McEvoy (Deputy Commissioner, Office of the Information and Privacy Commissioner of British Columbia): Mr. McArthur.

The Chair: There we go. Thank you very much, sir.

Please begin.

Mr. Drew McArthur (Acting Commissioner, Office of the Information and Privacy Commissioner of British Columbia): Thank you very much, Mr. Chair, for inviting us here to review the Personal Information Protection and Electronic Documents Act, or PIPEDA.

British Columbia's private sector privacy law is the Personal Information Protection Act, which I will call the “B.C. act”. As acting commissioner, I oversee how it is applied to over 380,000 private sector organizations, including businesses, charities, associations, trade unions, and political parties. The B.C. act is substantially similar to PIPEDA.

I will address in turn the items raised in the federal Privacy Commissioner's letter to this committee.

First, meaningful consent is a key aspect of PIPEDA and in privacy laws around the world, including the B.C. act. Although these acts were designed to be neutral with respect to technology, we are now seeing challenges to that neutrality with big data. There are concerns that some organizations are somewhat vague in their description of the purposes for which they use personal information.

To provide consumers with a better understanding of how their personal information is being used, organizations need to include clarity of purpose in the use of personal information for data analytics in their notifications to consumers. We believe this can be done within the existing consent-based model. Still, big data analytics represent a potential for both positive and negative outcomes to individuals.

Many of Canada's privacy commissioners and a group of Canadian organizations have been working with the International Accountability Foundation to examine the use of ethical frameworks in addition to existing privacy frameworks in the processing of personal data. These can be very complex and challenging issues. In practice, my office has not seen a situation where consent could not be obtained to enable a valid use of information. Granted, organizations could improve on how they describe their data processing activities in their privacy policies and use cases. Some suggest that organizations should be explicitly authorized to de-identify data so that they may then conduct data analysis without needing to obtain the consent of the individual. This approach would authorize data analytics on information that was already collected but not collected for that purpose.

My concern with this approach is that it is becoming easier and easier to reidentify data, using increasingly sophisticated algorithms. It may be that in a number of years, these reidentification techniques will be so effective that any previously de-identified information will be able to be reidentified.

Some jurisdictions are addressing this problem through legislation that allows processing of de-identified personal information while mitigating against the risk of misuse. Australia is now considering a bill that would make reidentification an offence, with intentional reidentification subject to a criminal offence with up to two years of imprisonment or a fine.

Recent amendments to Japan's Act on the Protection of Personal Information contain requirements for secure processing of de-identified information, including that reidentified information must be processed in a manner such that it cannot be reidentified and it must be handled securely, even though the information is de-identified.

Turning now to privacy and reputation, today personal information that is online or stored in databases has a permanence and availability that did not exist prior to the emergence of digital technologies. The ready availability of this information can, at times, have significant impact on people's lives, for better or for worse.

There are limited tools available to have personal information removed or corrected in the B.C. act, as in PIPEDA. An individual has a right to withdraw consent, but this is subject to exceptions, such as where withdrawing consent would frustrate a legal obligation. An individual also has a right to request correction of their personal information. However, these are not comprehensive tools if someone wants to eliminate their digital footprint, in whole or in part.

● (1535)

While the B.C. act and PIPEDA can provide some redress where incorrect personal information is being disclosed online, there is also the potential for the disclosure of truthful information to cause harm. This is where the right to be forgotten, the right to erasure that exists in Europe, is useful to individuals who have experienced damaging effects to their reputation owing to information that is online.

While I can see the potential benefit of creating such a right in Canada, as others have observed, it remains to be seen how a right to be forgotten could exist within our legal system alongside the right to freedom of expression. We are seeing many unanticipated consequences of the implementation of the right to be forgotten, so it is a concept that must be approached carefully.

One of these issues is the ability of governments to undertake censorship, and another is that the right to be forgotten is being administered currently by private sector organizations.

On enforcement powers, personal information has become integral to the business model of a number of companies. In this context, order-making power is essential to any privacy commissioner. I believe order-making powers need to be used effectively and judiciously. Allow me to describe how they are used in my office.

Relationships with organizations and public bodies are critical to providing effective oversight over B.C. privacy laws, and order-making powers may, indeed, encourage organizations to work with my office. More than 90% of the complaints to my office are resolved at mediation. My investigators have expert knowledge on B.C.'s privacy laws and work to help parties understand their respective rights and responsibilities. At mediation the parties are aware that, if a resolution is not reached, the matter may go to adjudication, resulting in an order. This encourages the parties to work with us at mediation to find a resolution. Orders from my office require that organizations bring themselves into compliance with B.C.'s private sector privacy law.

The act sets out the kinds of things I may do; for example, to require that a duty be performed under the B.C. act, and I have the authority to specify any terms and conditions for fulfilling that duty.

On the matter of adequacy, now that Europe's general data protection regulation has passed, ensuring that Canada's privacy laws also provide an adequate level of protection will assist businesses that rely upon personal information flows from Europe to Canada. The GDPR says that an adequacy determination can be made where a country or territory offers levels of protection that are essentially equivalent to those within the European Union. Note that an adequacy finding can be made for a territory; so interestingly, a provincial privacy law could be found to be adequate for transfers, even if PIPEDA is not. Essential equivalency is the bar, so there is some work to be done if adequacy is to be maintained.

I've already mentioned the right to erasure. Here are two other areas for consideration.

Parliament has already addressed breach notification under PIPEDA. In B.C., my office recommended mandatory breach notification for both the private and public sectors in the recent legislative review of B.C.'s privacy laws, and the provincial government has committed to doing so.

In Europe, failure to notify can be subject to administrative fines of up to 10 million euros, or 2% of a company's total worldwide annual turnover, whichever is higher. In other areas, fines may be as high as up to 20 million euros, or 4% of annual turnover, whichever is higher. In B.C. and Canada, our fines do not keep up with these standards.

Before I wrap up, I want to comment on one additional area. In response to the Spencer decision by the Supreme Court, law enforcement agencies have indicated that they want warrantless access to online subscriber information. A change like this in PIPEDA would not be consistent with the reasonable expectations of Canadians. Warrants are already available for circumstances that require them, and judicial oversight is critical to public confidence in how personal information is released or disclosed.

Thank you very much, and I'd be happy to respond to questions at the appropriate time.

● (1540)

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

We'll now move to the information and privacy commissioner of Alberta, Jill Clayton, for up to 10 minutes, please.

Welcome back, Jill.

Ms. Jill Clayton (Commissioner, Office of the Information and Privacy Commissioner of Alberta): Thank you very much.

Thank you, Mr. Chair and committee members, for the invitation to speak to you today as you review the Personal Information Protection and Electronic Documents Act. Here in Alberta, we call it "PIPEEDA" as opposed to "PIPEDA", as Drew just referred to it. With me are Sharon Ashmore, who is general counsel with my office, and Kim Kreutzer Work, who is the director of knowledge management.

I thought I would start my comments today by speaking briefly about Alberta's Personal Information Protection Act, or PIPA, and then in a very similar way to Drew's presentation, I will provide some brief comments on the four topics that I understand you're interested in. I'll speak about PIPEDA's adequacy vis-à-vis the European Union enforcement powers, and in particular my ability to order compliance, as well as meaningful consent and privacy and reputation. Then, of course, I would be happy to address any questions you might have.

To begin, Alberta's Personal Information Protection Act, or PIPA, came into force on January 1, 2004. The act balances the privacy interest of Albertans with the need of organizations to collect, use, and disclose personal information of their customers, clients, employees, and volunteers for reasonable purposes. PIPA has been declared substantially similar to PIPEDA, which means that in Alberta it is PIPA, and not PIPEDA, that generally covers provincially regulated private sector organizations and businesses.

My role is to provide oversight for the act. I have a number of powers and responsibilities under the legislation to ensure that its purposes are achieved. So far, PIPA has undergone two reviews by all-party committees of the Alberta legislature. This in fact is built into the legislation and is a statutory requirement.

The first review took place in 2006-07 and led to several amendments, most notably, mandatory breach reporting and notification requirements, which came into effect in May of 2010. Alberta became the first private sector jurisdiction in Canada to have mandatory breach reporting and notification, and we have since become the model for many other jurisdictions that are contemplating similar amendments.

I think I'll mention that since 2010 we have seen close to 750 breach reports under PIPA and have issued close to 600 notification decisions. So far, we've found that in approximately 56% of those cases there was a real risk of significant harm, in which case I required the organization to notify affected individuals.

The second review of PIPA was more recent and concluded at the end of 2016. During one of my appearances before that review committee, I spoke about the importance of global considerations when considering amendments to Alberta's legislation. I believe those comments are relevant here again in regard to PIPEDA's adequacy status vis-à-vis the European Union.

When it comes into force, the European Union's general data protection regulation, or GDPR, will make privacy law across Europe stricter and will enhance the protection for Europeans' personal information in such areas as consent, accountability, privacy management frameworks, breach notification, and privacy impact assessments. In a global economy where Canadian and Alberta businesses are participants, and where private sector privacy law needs to be adequate and substantially similar, the effect of the GDPR must be considered in any discussion about amendments to our legislation governing the collection, use, and disclosure of personal information.

I'm not necessarily suggesting that PIPEDA or, by extension, PIPA will be deemed to be inadequate, but I am suggesting that there's a need to be mindful of global and national considerations when we're contemplating amendments, to ensure that they don't weaken the legislation and that they are not out of step with global and national considerations. I think it's important to remember that although legislative requirements and regulations may sometimes seem to be burdensome, they also help to provide the public and businesses and their service partners with stability and reassurance, both of which are necessary to win customers and to facilitate business and information sharing.

Going on to enforcement powers, I'm able to issue orders under all three of the acts for which I provide oversight: our public sector's Freedom of Information and Protection of Privacy Act and our health sector's Health Information Act, as well as PIPA.

Order-making power does not preclude my office from resolving cases by an informal mediation process rather than going through the formal inquiry process. In fact, in most cases when we receive a request for review or a complaint, we investigate and attempt to mediate and resolve that matter informally. It's only when findings and recommendations are not accepted that the matter may proceed to inquiry. In 2015-16, approximately 80% of our cases under PIPA were resolved through that mediation process as opposed to inquiry, and since 2004 we have issued 134 PIPA orders.

● (1545)

In most cases organizations comply with orders. In the very odd case where an organization does not, I can file the order in the Court of Queen's Bench, at which time it becomes enforceable as a judgment of that court. I have had occasion to file orders twice in the last year. In one of those cases it was under the Health Information Act and not PIPA, and in the other case, it had to do with ensuring compliance with a breach notification decision I had issued under PIPA. In both cases, after filing with the court, the matters were resolved before the court heard the cases. In those examples, order-making power was extremely valuable in obtaining compliance.

Moving on to meaningful consent, I will first note that in Alberta, we talk about PIPA as being consent-based legislation, and generally, I think it works well. Requiring organizations to obtain the consent of an individual before collecting personal information and to provide notice of the purpose for collection helps to ensure that individuals are able to make informed decisions and exert some measure of control over their personal information.

However, I am aware of ongoing discussions in certain forums that suggest that a consent-based framework is not always adequate. I seldom hear that consent and notice should be done away with entirely, but there does seem to be concern that in this age of big data, predictive analytics, and complex information systems, consent and notice may not be adequate in all cases and may stifle innovation as well as initiatives that are in the public interest.

I've certainly participated in a number of these conversations where we've tried to define the problem, if there is a problem, and to identify and consider some proposed solutions. In those discussions, I often make reference to Alberta's Health Information Act, for example, which is not consent-based but based on a circle-of-care idea, the concept of legislated acceptable uses. We also make reference to the personal information code under Alberta's PIPA, which again recognizes that consent in an employer-employee relationship might not work, and so consent is not required for collecting certain information. We also look to the Health Information Act for the framework around research and research ethics boards. As Drew mentioned earlier, there are commissioners in the country who are interested in some of the projects, notably the Information Accountability Foundation, and a project on developing an ethical assessment framework for certain big data initiatives.

In any event, I believe any solution to the problem, if there is a problem in this area, would involve a mix of legislative, regulatory, and voluntary options, and I certainly support discussion of these issues, including consultations such as the exercise the federal Privacy Commissioner recently undertook.

Finally, I have a few words to say on privacy and reputation. This topic has seen a lot of attention in recent times, particularly around the idea of a right to be forgotten, and whether such a thing exists in Canada or not, and if it does, how it might be enforced in today's global world.

I mentioned this in the trends and issues section of my 2014-15 annual report and said that this was a topic we should be watching over the next couple of years. In particular, we've seen cases like the May 2014 case in the Court of Justice of the European Union; the recent case involving Globe24h at Canada's Federal Court involving information posted on a Romanian website; and a pending decision from the Supreme Court of Canada in Google v. Equustek Solutions. I think that brings home the fact that these are live issues.

Of note, these cases highlight questions of jurisdiction and legal boundaries and the ability to compel compliance; privacy versus freedom of expression; transparency for public figures such as politicians; and the technical challenges and costs for global companies. These are all complicated issues, but they have found their way to my office, as we have seen a recent uptick in the number of right-to-be-forgotten-type cases in the office. We had previously seen about half a dozen of them over the first seven or eight years of the legislation, but I think we have half a dozen in the office right now. They tend to be focused on such issues as websites publishing personal information collected from some source other than the individual whom the information is about. There are also sometimes complaints around decision-making bodies, including personal information, in their published decisions.

● (1550)

As there are a number of live matters in my office at the moment, I'm not going to get into too many specifics. We will be issuing decisions in some of these cases. It is worth noting that these discussions have made their way from other countries, contexts, and the courts to real complaints made by real individuals that are currently in my office.

On that note, I will leave my comments there. I'd be happy to respond to any questions.

Thank you.

● (1555)

The Chair: Thank you, Ms. Clayton.

We now go to Ms. Chassigneux.

[*Translation*]

You have 10 minutes.

Ms. Cynthia Chassigneux (Administrative Judge, Surveillance, Commission d'accès à l'information du Québec): Mr. Chair and members of the committee, thank you for inviting the Commission d'accès à l'information du Québec to participate in the study on the Personal Information Protection and Electronic Documents Act.

This invitation gives me the opportunity to briefly describe the legislation applicable to Quebec in terms of personal information protection in the private sector, as well as the role of the commission and its latest five-year report.

Before examining the Act respecting the protection of personal information in the private sector, which came into force on January 1, 1994, I should point out that, by adopting this act, Quebec became the first Canadian province and the first government in North America to regulate personal information protection in both the private and public sectors. The public sector is subject to the Act respecting Access to documents held by public bodies and the Protection of personal information.

With that clarification, I should mention that the Act respecting the protection of personal information in the private sector applies to all the businesses that, in Quebec, carry on an economic activity of a commercial nature. It regulates the collection, use, disclosure within and outside the province, and the security of the personal information a company has. To that end, it sets out a number of principles in relation to consent, prior information of the individuals in question or even the reason why the personal information is collected, used or disclosed.

It also governs the right of a person to have access to or to correct their personal information held by a company. If rejected, the person in question may submit a request for the disagreement to be reviewed by the commission's adjudicative division. The Act respecting the protection of personal information in the private sector also sets out the duties and powers of the commission in audits and investigations carried out by its oversight division.

Before I describe the commission's role, I should say that the Act respecting the protection of personal information in the private sector, just like the Act respecting Access to documents held by public bodies and the Protection of personal information, overrides any other piece of legislation applicable in Quebec.

This demonstrates the legislator's intent to highlight the paramount importance of the rights given to the individuals in question and the obligations provided for both public bodies and private companies in terms of the protection of personal information.

I will now say a few words about the commission, which was established in 1982.

The commission has two divisions: an adjudicative division and an oversight division, of which I am a member.

The commission's adjudicative division acts as an administrative tribunal and reviews requests filed by those whose access to or correction of their personal information has been denied. The members assigned to the adjudicative division generally sit in at hearings, during which the parties involved have the opportunity to make their case.

After hearing from the parties, the commission may decide on any question of fact or of law and make any appropriate order to safeguard the rights of the parties. The decision rendered by the commission is public. The decision is binding 30 days after the parties have received it and it is subject to a right of appeal provided to the Court of Quebec on a question of law or jurisdiction only. When a decision becomes binding, it can be submitted to the Superior Court. It then has the same force and effect as if it were a ruling rendered by that court.

Under its oversight functions, the commission is responsible for promoting access to the documents and the protection of personal information. It also ensures that the legislation is applied in those matters. To do so, it can carry out audits and investigations into potentially problematic situations brought to its attention, in order to ensure that public bodies and private enterprises comply with the legal provisions.

The commission may make recommendations and compliance orders upon completion of its investigations, which are carried out in a non-adversarial way. The orders made by the commission may, under the Act respecting the protection of personal information in the private sector, be submitted to the Superior Court for registration. Furthermore, if an order is not complied with, the commission may, in the case of enterprises, release a notice to inform the public. It may also initiate criminal proceedings.

Now, allow me to quickly go over some of the points raised in the commission's 2016 five-year report. In fact, the commission must report to the government every five years on the application of the act respecting access to documents held by public bodies and the protection of personal information and the Act respecting the protection of personal information in the private sector. In the report, it makes recommendations to improve the government's transparency and the protection of personal information in Quebec. The report, tabled in the National Assembly, may lead to legislative amendments.

In its last report, just like in the previous one, the commission stressed the need to strengthen the protection of personal information in both the public and private sectors, especially since the Act respecting the protection of personal information in the private sector has not undergone any significant amendments since it was passed more than 20 years ago.

● (1600)

Among other things, it calls on the government to amend the Act respecting the protection of personal information in the private sector in order to include an obligation for corporate responsibility and to provide for the designation of a person responsible for access and the protection of personal information. This amendment would help to develop a corporate culture that protects personal information, to ensure more transparency and to increase public confidence.

It also calls on the legislator to update the concepts inherent to the protection of personal information in the private sector. Actually, for a number of years, the commission has noted, particularly because of the proliferation of electronic platforms, that some of the concepts under the Act respecting the protection of personal information in the private sector no longer fit, or correspond with limited effectiveness, to the new business models that result.

A number of those models, whether free or paid, are fed by information gathered here and there, from users or without their knowledge. Because of the emergence of those new business models, we often hear that personal information has become the petroleum of the 21st century, that it is worth a fortune, or that it is the lungs of the digital economy.

So, in order for the Act respecting the protection of personal information in the private sector to be fully applied to those new business models and to restore user confidence, in its five-year report, the commission calls on the legislator to revisit some of the concepts set out in the act. For instance, these include the concepts of a file, of the disclosure of information or of consent.

In terms of the concept of a file, I should first specify that a number of the obligations under the Act respecting the protection of personal information in the private sector are related to that notion. Right now, the legislation imposes obligations on businesses that create or keep a file for an individual. However, the fact is that more and more companies gather images, identification, use and location data, creating profiles to analyze the behaviours of users in order to improve the goods and services provided online or to attract their attention with targeted advertising.

Those companies gather information likely to identify an individual often without their knowledge and without necessarily establishing a contractual relationship. Although those companies hold personal information, they don't always keep it in a "file" with the person's name on it. So, although the concept of a file is sufficiently comprehensive to be interpreted broadly and to apply to electronic environments, the examples described above have prompted the commission to propose that the term "file" be replaced with the "purpose of the collection", a principle underlying a number of personal information protection systems. As a result, corporate obligations would be linked to the initial reason for the collection of personal information.

As for the obligation of disclosure to the person in question when personal information is collected, the commission notes that it is one of the obligations that are met the least in the Act respecting the protection of personal information in the private sector. However, the protection of personal information is a shared responsibility. How can people assess how their personal information is protected by businesses and determine whether they are trustworthy, if they are not even informed, at a minimum, of the nature of the information the enterprise has and the subsequent use?

That is why, just like in the previous report, the commission has called on the legislator to amend the Act respecting the protection of personal information in the private sector, in order to specify when the information must be given to the person in question, to include the obligation to disclose the personal information collected and how it was collected. The commission also stresses the importance of the information being clear, intelligible and accessible, regardless of the platform used to collect the personal information.

In terms of consent, it must be noted that consent is the driving force behind the protection of personal information. In principle, it allows users to control what companies can and cannot do with their personal information. That's only in principle, because the notion of consent is increasingly criticized and considered inadequate in some contexts.

This raises the question of how to give consent its true meaning back. How can it be ensured that it truly means that individuals have agreed to a company managing and using their personal information, giving them real choice in the matter, rather than an opaque legal text created to limit the responsibility of companies to obtain an all-encompassing and irreversible "I agree"?

● (1605)

Therefore, although the Act respecting the protection of personal information in the private sector states that the consent must be manifest, free, and enlightened, and given for specific purposes and that it is valid only for the length of time needed to achieve the purposes for which it was requested, the commission notes that the scope of the criteria for consent is not well understood by enterprises. It therefore feels that clarifications about the obligations of enterprises under each of the criteria for consent should be included in the Act respecting the protection of personal information in the private sector. It also believes that the legislator should indicate that consent may be withdrawn at any time subject to restrictions under the act.

In closing, I must clarify that the commission does not claim to think those amendments will provide a solution to all the current consent-related issues. It believes that discussions must continue and that other avenues must be explored. To that end, in its five-year report, the commission stresses the importance of considering the amendments made to European legislation on the protection of personal information.

Mr. Chair, thank you. I will be pleased to answer any questions you and the other members of the committee may have.

The Chair: Thank you, Ms. Chassigneux.

[*English*]

We will now proceed to our first round of questioning.

We'll start with Mr. Bratina, please, for seven minutes.

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

Thanks, everyone, for really continuing to confuse me over this very complicated situation.

First, to Mr. McArthur, what's the use of provincial or territorial boundaries in describing PIPEDA? We're seeing that Europe seems to have a more robust set of regulations and penalties, and we're not able to come up to their standards—so far, although maybe we will through these discussions. On the question of equivalency, should these kinds of regulations be made by a larger body rather than by many territorial or provincial bodies in order for it to really work properly in the world that we live in?

Mr. Drew McArthur: Well, first, while I agree that information flows and really knows, often, no boundaries, it's the information of citizens in particular jurisdictions that is of interest to those citizens, whether it's federal or provincial, as is the case in Canada, or whether it's country by country or the European Union, in Europe. I think those decisions are best left to the legislators in those countries and in those particular territories.

To us in Canada, I don't think it has been complicated. It's well understood that B.C. citizens are protected by our private sector act, and we have the opportunity to focus on their particular concerns when addressing their complaints.

Mr. Bob Bratina: Go ahead, Mr. McEvoy.

Mr. Michael McEvoy: There's a recognition as well in this country, on the part of our offices that have jurisdiction over the private sector, that we work together. For example, when you have breaches that happen in companies that operate across the country, the B.C., Alberta, Quebec, and the federal offices work together in a coordinated way. It's important to our citizens to do that, but it also provides a unified face, if I can put it that way, to the private sector companies that they're not having to deal with the offices individually.

We also extend that, frankly, to the international sector, where we increasingly co-operate with data protection authorities around the world on data breaches. You may be familiar with the recent Ashley Madison breach, where the Canadian office worked with authorities in the United States and Australia and other places. We were also involved in that. There's an increasing level of co-operation between data protection commissioner offices around Canada and around the world.

Mr. Bob Bratina: Mr. McArthur, you brought up the question of mediation. I'd be very interested in hearing an example of a mediation, without your giving any specifics of it. Could you give me a general idea of how mediation would work?

● (1610)

Mr. Drew McArthur: Essentially all of the private sector complaints that come into our office go through a process of mediation, where the interests of the parties are examined and investigated, and the rights of the individual are balanced with the obligations of the organizations. We say it's a process of mediation in addressing a complaint and determining an outcome in which both parties' interests are given consideration. Organizations, understanding that we do have order-making powers, are certainly more compelled to work creatively or effectively with us through that process.

Mr. Bob Bratina: Could I ask Ms. Clayton in Alberta about the 750 breach reports? It sounds like a big number. Is that a manageable number for your office?

Ms. Jill Clayton: Well, it continues to increase; every year we receive more reports under PIPA. We have managed so far. I will say I have some concerns. There is some expectation that we'll be seeing mandatory breach reporting in the health sector in Alberta sometime in the fairly near future. That will probably tax the resources of my office.

I will perhaps just say a bit about the structure of breach reporting notification requirements in Alberta, because they are fairly unique — certainly in Canada. While there are some similarities to what's proposed for PIPEDA through the Digital Privacy Act, they're not exactly the same.

In Alberta, the threshold for reporting a matter to my office is where there is a real risk of significant harm. This is the same threshold as for PIPEDA. However, the framework in Alberta gives me the ability to require an organization to notify affected individuals. The act in Alberta does not require the private sector organization immediately to notify. It instead requires them to tell me. If there is a real risk of significant harm, if a reasonable person would think that threshold had been met, then it's an offence for an organization not to report it to me.

When those reports come in, out of the 750 reports that we've received in almost six years, I have an active role in reviewing them. I review the assessment of harm and the likelihood that harm will result from the incident, and I issue a decision for each one.

Mr. Bob Bratina: Should we harmonize our regulations with Europe? It seems that the standard is there.

Ms. Clayton, would you comment on that?

Ms. Jill Clayton: I think it's very important to be aware of what is happening in Europe. As I mentioned in my comments, one of the things I said to the committee in Alberta that was reviewing our Personal Information Protection Act was that—at least with respect to mandatory breach reporting and notification—I'm feeling pretty good about that. It looks like that's going to be a requirement under the GDPR when it comes into force, and I think we're ahead of the curve as far as that goes.

So yes, I think that's something we all need to be aware of. We certainly need to be thinking about how to strengthen our legislation. Mr. McArthur said that information knows no boundaries, that it's flowing globally. It doesn't work to have a patchwork. You're only as good as your weakest link or your lowest water level.

Mr. Bob Bratina: Thanks very much.

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

We now move to Mr. Jeneroux, please.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, everybody, for being here virtually.

Ms. Clayton, it's nice to see you in the staff again. Let's start with you because you're from my favourite city, Edmonton.

You spoke a little about the right to be forgotten. Could you maybe touch on, first of all, why you've seen the increase just recently, and also how you will find that balance? It's fascinating to me how somebody's opinion of what's right to be forgotten and somebody else's opinion are probably quite different. I guess if you could help with some of that opinion....

Again, Ms. Clayton, I'll start with you and then go around the room if you don't mind.

Ms. Jill Clayton: I certainly think some of the reasons there is interest in this issue have to do with the explosion or proliferation of technology and social media. You can't pick up the papers without hearing about sexting, cyber-bullying, or information that has been posted that you can never get rid of, but is out there. I think some of that contributes to public awareness: the Internet generally, social media sites, and the amount of information that is out there.

Of course, what has gone along with that is the rise of some of websites in particular. In the office we've seen examples of websites where ex-girlfriends or ex-boyfriends can post information about somebody, and it doesn't necessarily have to be accurate, but it's out there, and they're concerned that it's out there. They're concerned that it will be out there forever and that they will never be able to get rid of it. They're concerned that it will affect their ability to hold a job or get a job, so I think there can be real ramifications.

What is the balance? I mentioned in my opening comments some of the concerns around privacy and freedom of expression. We had a matter under Alberta's PIPA that went to the Supreme Court that was balancing just that. The court found in favour of freedom of expression with respect some political information that a union might post. I think all of these issues in this conversation, this technology, and use of social media sites are pushing discussion about it. So I think we will have to be talking about and dealing with them. Court decisions are also furthering that conversation.

As for finding the balance, I think there is a really important role that regulators have to play, that I, as a regulator, have to play, and that the rest of us who are appearing before you today have to play, as information and privacy commissioners, in being able to balance that. Frequently, under freedom of information legislation—which is access to information and protection of privacy legislation—we are trying to balance privacy with the public interest and the right to access information.

There is often a tension that needs to be resolved. I think we have some experience in that as information and privacy regulators. I often don't hear that as part of the conversation around the right to be forgotten. It's often more of a question of whether there are charter issues and how the courts will resolve this, but I do think that there's potentially a role for information and privacy commissioners.

Does that answer your question?

● (1615)

Mr. Matt Jeneroux: Yes, that's good.

Maybe just quickly before we move on from Ms. Clayton, do you agree that the privacy commissioner should have enforcement powers?

Ms. Jill Clayton: Absolutely. Enforcement powers [*Technical difficulty—Editor*] infrequently. As I mentioned, close to 90% of the cases that come into our office are resolved informally. We make recommendations, the organization agrees to implement those recommendations, and the matter is resolved. The complainant is happy, and that's the end of it. A small percentage of cases go to inquiry and result in a binding order. It's a very, very small percentage. I think that only once in 10 years have we actually gone to court, filed an order in court—and even that ended up being resolved before the court heard the matter. It's a helpful tool in the tool box, but it's a last resort.

Mr. Matt Jeneroux: Mr. McArthur, I didn't hear you really touch on the right to be forgotten. Do you have an opinion on how you find that right balance, if you don't mind?

Mr. Drew McArthur: Yes, thank you.

There are a couple of points to be made on the right to be forgotten. Today, with the Google v. Spain decision, the right to be forgotten is one of delisting, whereby the results of a search do not display the information, but the source of the information is still available. In the general data protection regulation in Europe, the right to erasure is broader than just delisting or limiting the results of a search. These two differences, where in one case the personal data of a subject can be erased versus where it is just prohibited from being displayed by search engines, are not subtle differences between some people's interpretations of the right to be forgotten, and it needs to be carefully considered when dealing with legislation.

Mr. Matt Jeneroux: Cynthia?

[*Translation*]

Ms. Cynthia Chassigneux: In Quebec, another piece of legislation about the private sector provides for the possibility of correcting or deleting information that is inaccurate, incomplete or equivocal. In fact, a request for rectification from an individual has been filed with the Commission d'accès à l'information. This request was considered by the adjudicative division, but not by my division, namely the oversight division. So it was not a complaint.

This person requested that their personal information be deleted from the site of the company for which they had worked. The company said that the information had been deleted after the dismissal of the person. The person found that this had not been done and that it was still possible to find their information if they did a search through a search engine. The evidence showed that the information about the person came from a website called Wayback Machine, which allows people to take screen shots of a site at a given time. So the company was not responsible. The company had deleted all the information it had on that person from its database.

It was determined that, and I quote: "the right of a person to have incorrect, incomplete or equivocal information corrected in a file about himself or herself is not the 'right to be forgotten', which aims to erase information from public spaces."

Yes, a decision has been rendered by the adjudicative division, but to my knowledge, no complaint has yet been made to the commission's oversight division. We follow this closely, taking into account what has happened in Europe and the various decisions that may have been made, in order to see how Europe's regulations could be tied in with Quebec's.

● (1620)

The Chair: Thank you very much.

[*English*]

We now move to Madam Trudel, for seven minutes, please.

Welcome to the committee.

[*Translation*]

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

Thank you very much for your presentations.

As my colleague Mr. Bratina said, this is a very complex issue. Since I am new on this committee, you will forgive me if don't use the proper terms.

My questions are for you, Ms. Chassigneux. I am from Quebec and I am pleased to speak to you about Ottawa.

When you talked about consent and the phrase “I agree”, images popped up in my head. Yesterday, I was actually surfing a site and I had no way of accessing it without agreeing to give my consent. I’m going to ask you about that, but beforehand, I'd like to hear your opinion on another issue.

In your presentation, you said that European legislation has explored other avenues and you left it at that. Could you elaborate on those other avenues? What should we do to make our lives easier and to bring Canadian legislation more in line with the European legislation?

Ms. Cynthia Chassigneux: In my presentation, when I spoke of other avenues, I was also referring to the consent document of the federal commissioner's office and the document submitted to committee members. These documents show the different possible avenues.

Last fall, the federal commissioner's office conducted a consultation. The other avenues considered related to the issue of whether we should move toward no-go zones where it wouldn't be possible to collect personal information and whether we should have much more detailed privacy policies. Also, in its 2011 five-year report, the Commission d'accès à l'information had already recommended that legislators establish detailed privacy policies.

In other words, there would be a fairly detailed general policy and a simplified policy. It's what we call multi-layered policies. These simplified policies can be adapted to each communication tool, such as a cellphone, tablet or computer. There could be even icons or pictograms showing that the required consent concerns people under the age of 13 or parents. It would be something very visual.

As you said, we can't access certain sites without clicking everywhere or filling in all the boxes. To provide a simple email address, does the person's location need to be known and does all sorts of information need to be collected? It happened to me this past weekend. I won't name the site, but we can't register for it without filling in an entire page that contains at least 10 questions.

In this type of case, is our consent truly free and informed? We must ask ourselves these questions. The answer lies in the question.

● (1625)

Ms. Karine Trudel: Thank you. I appreciate what you're saying. We may not have consulted the same site, but the same thing happened to me.

I think the consent issue should be better regulated. We aren't free to either access these sites or refuse to disclose our personal information.

I'll go back to the consent model, since I have problems with this aspect in particular on both a personal level and in the study.

What can we do?

You spoke earlier about a person and the right to be forgotten. Another site had captured the images of this person. For me and no doubt for many others, the Internet is a vast territory. It goes on for miles and miles.

My question is really limited, but I want to know what can be done to prevent these incidents from happening after a person has provided personal information and agreed to its disclosure.

Could we implement stricter processes to prevent this type of situation, including the one you mentioned earlier?

Ms. Cynthia Chassigneux: Some people think the sites should be required to set preference parameters. When we enter a site, we can agree that our information may be shared for a particular purpose. However, sometimes the site then changes its business model or approach. As a result, our preference settings may be changed. However, in these types of situations, the site should notify us that the privacy policy or preferences have been changed. When a site changes its business model, the preferences indicated by people on the site should be maintained. The businesses are responsible for doing this. That's a fact.

However, as I said earlier, consent is a shared responsibility. One person shouldn't be carrying the entire burden. That person is not responsible for making sure the privacy policies are suitable. A Quebec resident or business can read the policy. However, we all know that, in general, we don't necessarily have enough time and energy to read the privacy policies. Studies have even determined how much time would be needed to read all the privacy policies of the sites we visit each day.

Our preferences must be maintained if a site changes its business model. It would then be our job to check from time to time whether our preferences are still the same. It's a shared responsibility and a matter of finding a balance. That's one solution. I can't think of any others for the moment. If you want, I could provide more information to the committee later on the subject.

Ms. Karine Trudel: Thank you.

[*English*]

The Chair: Thank you very much.

We'll now move to the last of the seven-minute rounds.

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

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

I wanted to touch on Mr. Bratina's point because I wanted some clarity.

We know that in May of 2018, the GDPR is going to come into effect. Having just recently signed CETA, we know that for our business people, we have to come in compliance with that data protection regulation. We also know that if the United States wants to do business with Europe, it will have to come under that regime also.

Am I assuming correctly?

● (1630)

Mr. Drew McArthur: Are you addressing that question to—

Mr. Raj Saini: Yes. Just the line of questioning....

If we have to come to the standard of the GDPR, I would assume that the United States would also have to come to the standard of the GDPR.

Now, when I look at the privacy regimes in Canada, I see there are actually four. There is PIPEDA, and then there's what they determined in Alberta, B.C., and Quebec to be substantially similar privacy information protection acts. If you look domestically, if we're looking at reducing internal trade barriers and also looking at the fact that business people in provinces across Canada will have to raise their level to the European standard, would it not be...? Even right now there are differences between Alberta and B.C. Alberta and B.C. have three types of consent. Alberta has a privacy breach provision; B.C. and Quebec don't have a privacy breach provision. Ultimately, if we're going to rise to the GDPR level to make sure that we trade, eventually the whole country will have to have something that's much more substantially similar than what we have now—and also if the United States rises to that level, would it not be better to create one regime across the whole country?

Mr. Michael McEvoy: May I just make a comment about the U. S. regime?

I think they have some significant challenges. They have used a mechanism described initially, I think, as a “safe harbour”, which is almost a self-certification system for U.S. companies doing business in Europe. That was challenged in court in Europe and in fact went down; it was ruled contrary to European law. They then developed a privacy shield, and I gather that there are challenges to that.

The United States has a very patchwork approach to privacy, and it's often sectoral. There might be a law for child protection; there might be a law through the Federal Trade Commission for unfair trade practices. They don't have a uniform, standard approach to these things.

Frankly, this may actually be a Canadian competitive advantage in dealing with our European colleagues.

I wouldn't overstate the differences among our Canadian jurisdictions. There's some similarity in the consent provisions. I think we would agree that on the mandatory breach notification, everybody is going to have to come up to that standard. Nonetheless, said, there is some degree of uniformity across the country, in addition to the fact, which we mentioned earlier, that there is cooperation among our offices across the country.

Ms. Jill Clayton: I would like to add to that, to back up what Michael has said.

Remember that Alberta's legislation and B.C.'s legislation, for example, were drafted at almost the exact same time using almost exactly the same language, so they're very similar. Both have been deemed, along with Quebec's legislation, to be substantially similar to the federal PIPEDA.

Yes, it has been the case that certain provinces have gone ahead with.... We talk about “made in Alberta” legislation. That's the way the legislature wanted to act back in the early 2000s. The idea was that made in Alberta legislation could better address the issues of small and medium-sized businesses, and there was a lot of support for local enforcement, frankly, with a commissioner who has order-making power.

Having said that, we have seen efforts to bring all jurisdictions to the same level. Even though reviews have happened provincially and at a federal level, I think we're all going in the same direction, getting there at slightly different times, perhaps.

I would also like to go back to the comment that I think Michael made earlier, that we cooperate across the country in the private sector jurisdiction. We meet and discuss as regulators and make an effort and devote a lot of energy to making sure that we are regulating in a consistent and harmonious way, to not introduce challenges where there don't need to be challenges. There are differences in the legislation, but generally the acts are quite similar.

Mr. Raj Saini: I want to go back to a point you raised about children and their privacy. In the United States, the FTC handles the privacy of children under the age of 13, and with the GDPR regulations coming out, the age will be 16. I don't know whether in PIPEDA we have defined in law the age of a child who is considered a minor, but we know that many websites in the United States, especially children's websites, are more highly tracked than adult websites.

Should certain children's websites be no-go zones from which no information can be collected or processed? Under the FTC right now, any child under the age of 13 on certain websites needs parental permission, and for anything over that, the permissions can be circumvented by a child. Should there be a no-go zone in certain children's websites to make sure that their information is not tracked or their privacy breached in any way?

● (1635)

Mr. Drew McArthur: I'll take a first shot at answering that.

PIPEDA does not recognize age as an issue for the collection, use, or disclosure of personal information. Citizens of all ages are protected under PIPEDA.

In the B.C. act, a minor who is capable of exercising his or her rights may legally do so under the act, and if the child is not capable, someone acting in the best interest of the individual may act in their capacity. Children, then, are protected already under the B.C. act, and personal information of any citizen, regardless of age, is currently protected under PIPEDA.

The Vice-Chair (Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): That takes us to the end of the seven-minute round.

We begin the five-minute round with Mr. Kelly.

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

Commissioner Clayton, in your opening remarks, you talked about discussing our exercise of identifying areas for improvement or shortcomings, if any, in the subject matter we're looking at. What shortcomings have you identified in PIPEDA, or for that matter in PIPA, your own act?

Ms. Jill Clayton: I'm happy to answer that. If I can clarify, when I was talking about areas for improvement, that might have been specifically in some comments I was making about consent. Is your question specifically about limitations of the consent model?

Mr. Pat Kelly: No, it's not.

Ms. Jill Clayton: Or is it just about general limitations in the legislation?

Mr. Pat Kelly: It's limitations in the legislation.

Ms. Jill Clayton: I'll start with my own legislation. I did make a submission recently on Alberta's second legislated review of its PIPA. That concluded at the end of last year. My submission to the review committee included 10 recommendations for strengthening the legislation. I said I thought that PIPA worked quite well. I think it's strong legislation. Again, the made in Alberta solution was supposed to be legislation that would make sense to smaller organizations. The feedback I've had from small and medium-sized businesses is that it works quite well from an enforcement point of view as well.

We've had very few recommendations, and some of them are not applicable in the federal context. For example, I had asked to extend the scope of Alberta's legislation to include all non-profit organizations, which is the case in British Columbia, but is not the case in Alberta.

Mr. Pat Kelly: There's no glaring shortcoming that's crying out for immediate action?

Ms. Jill Clayton: I think there is. That's my concern.

One of the things we did talk about, and a recommendation I made to amend our provincial legislation, was to require that organizations have a privacy management program in place. This does speak to some of what we're expecting to see when the GDPR comes into force. Alberta, B.C., and the federal office all came together in 2012 and came up with a published joint guidance document called, “Getting Accountability Right with a Privacy Management Program”. That document sets out the basic foundational building blocks of a privacy management framework and says, before you can do privacy compliance, you need to have these basic things in place. We all agreed on that, across the country.

● (1640)

Mr. Pat Kelly: If I think of some of the very smallest enterprises, particularly organizations or enterprises that may not conduct business on the Internet, is that recommendation a bit onerous? Does the local curling club need a privacy officer, a written privacy policy, and a privacy management framework to have people curl at their club, for example?

Ms. Jill Clayton: I think somebody should be responsible for privacy, and that's already in our legislation. They do need to have policies, but they don't need to be written, according to Alberta's PIPA. I can't speak for PIPEDA or B.C.'s PIPA. I think any legislation of a requirement to have a privacy management program does require that some mindfulness be given to scaling such a program to the organization. I'm not sure that these small organizations shouldn't be concerned about privacy, because it could be a very small organization with only two employees collecting, say, credit card information. As a consumer, I would want to know that if I'm giving my credit card information to this very small organization, they have an obligation to safeguard that information. I do think it's scalable.

The Chair: Thank you very much, Mr. Kelly. We're at five minutes.

Mr. Erskine-Smith, you now have five minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much.

I wanted to start by asking about enforcement powers. One model is order making. Another model is fining powers, administrative monetary penalties, and/or a combination of the two.

We heard testimony the other day that in the EU there are significant fining powers. I think it's up to 4% of company revenue.

What are your comments on whether we should empower the Office of the Privacy Commissioner with such administrative monetary penalty powers? Would that be a good idea?

Mr. Drew McArthur: In the B.C. act, there are fines, but they've never been imposed.

In terms of the adequacy of compliance or alignment with the GDPR, I think both Canada and the provinces are going to have to examine the amount of their fines, and to bring them more in line with what the GDPR is looking at in order to be considered adequate.

Mr. Nathaniel Erskine-Smith: With respect to transparency, the previous privacy commissioner suggested that there be public reporting requirements. Under PIPEDA, law enforcement agencies and institutions can obtain personal information from companies without consent or a warrant for a relatively wide range of purposes. The previous commissioner recommended ensuring that the public be made aware of how often this occurs. Do you think that's fair?

Does anyone have objections to that idea? Maybe that's a better way of phrasing it.

Mr. Drew McArthur: I think it's important that the public be made aware of when or how often law enforcement agencies are approaching certain organizations. We're now seeing organizations taking the opportunity to voluntarily publish transparency reports that indicate how many times they've been approached.

There may be times when an organization may be prohibited from doing so, and the laws currently recognize that. The organization may be prohibited from disclosing the fact that they've been approached, either by a national security organization or a law enforcement agency, but for the most part, I think it's important that Canadians be made aware of how many times their personal information is being requested under lawful access.

Mr. Nathaniel Erskine-Smith: So you favour openness by default, subject to national security or other overriding public interest concerns?

Mr. Drew McArthur: Correct.

Mr. Nathaniel Erskine-Smith: With respect to a further question on accountability, the previous privacy commissioner spoke of enforceable agreements. Where there has been an audit per se, and the OPC has issued recommendations for compliance to organizations that there would be enforceable agreements that would be entered into. He further recommended that the accountability-related principals in the act, from schedule 1, section 4.1, be reviewable by a federal court.

I don't know if there's a view from your three offices on that. Would there be any opposition to those recommendations?

● (1645)

Ms. Jill Clayton: I wouldn't have any objection to that, but I think you would want to look at it within the entire toolbox of enforcement powers. For example, I did not go to the committee that was reviewing PIPA, to talk about the need for enforceable agreements, because I have order-making power.

If you're looking at something like order-making power, you might not be in a position where enforceable agreements—

Mr. Nathaniel Erskine-Smith: That makes sense.

We had the commissioner before us the other day, and he talked about the potential need for alternatives to a consent model under PIPEDA. That struck me as odd, in part because I understand the consent model under PIPEDA to be quite flexible and that it can grow over time with different technologies. Should we be looking at alternatives to consent?

Mr. Drew McArthur: In the case of the B.C. act, I've indicated already that we haven't seen challenges, but where technology is taking us in the analysis of big data, there is a large amount of discussion around the analytics that can be unleashed upon information that was not originally collected for a purpose that might become apparent upon the running of those analytics.

The challenge that exists now is the ability of organizations to innovate with the data that they have within the context of consent when they don't necessarily understand what might be unveiled at the end of the analytic process.

We see technology now allowing for greater possibilities. At the end of the day, we believe there needs to be protection. People should be aware that their information is going to be analyzed. If it's going to be de-identified, there need to be protections built in so that it's not re-identified.

Mr. Nathaniel Erskine-Smith: I've run out of time, but if your offices have different models or alternatives to consent that you think this committee should consider, I would appreciate it if you would submit those ideas in writing.

Thanks very much.

The Chair: Thank you very much.

We now go to Mr. Jeneroux for five more minutes, please.

Mr. Matt Jeneroux: Great. Thanks again, Mr. Chair.

Your offices deal with businesses and in the context of people's relationships with businesses. I'm curious to know if you have any performance indicators, satisfaction metrics, or public consultation information you've done, which you can point to, that support or don't support some of your comments.

We'll start again with Ms. Clayton.

Ms. Jill Clayton: It depends on which topics you might be looking for performance metrics. We did a general population survey back in 2015 to get a sense of how individuals feel about privacy. We asked if they think it's important, if they feel their information is protected, if they are aware of our office, and if they think this is an important issue. That's on our website.

We also did a survey of the stakeholders that we regulate in all three sectors, and asked them questions about their privacy management programs. Do they do training? Do they have written policies? Do they have incident reporting mechanisms? Do they do privacy impact assessments? We asked a whole lot of questions around those sorts of issues, as well as our own processes and things like that.

Those documents and reports are both available on our website. The plan is to have a five-year interval, so probably it will be next year that we'll do it again and see whether or not there's been any movement.

Mr. Matt Jeneroux: Okay.

Mr. McArthur, go ahead.

Mr. Drew McArthur: First of all, we publish—as do other commissioners—annual reports on how our legislation is being enforced and our enforcement activities. We've just undertaken our first public awareness survey to assess people's awareness of the functions of our office and their privacy rights, whether in relation to the public or private sector.

We do not have any information to add to the mix that says whether or not people are comfortable or happy with how businesses are performing under that.

Mr. Matt Jeneroux: Sorry, I just want it to be clear: is that also in the context of the businesses, and not just the individuals? You do go out and ask, as Ms. Clayton said, the usual suspects, for lack of a better term....

● (1650)

Mr. Drew McArthur: Our public awareness survey surveyed about 1,000 citizens. It was more about their awareness of the functions of our office and their rights. It was not related to specific businesses, or whether or not they were comfortable with business practices.

Mr. Matt Jeneroux: Okay.

Ms. Chassigneux.

[*Translation*]

Ms. Cynthia Chassigneux: It's the same thing in Quebec. We also publish annual reports on the number of files, the number of complaints submitted to the Commission d'accès à l'information and the resolved complaints.

I don't think a satisfaction survey has been conducted recently. There may have been one already, but I would need to check. I have been at the Commission d'accès à l'information for six years, and I don't remember any satisfaction survey being conducted with individuals, businesses or public agencies. I know that awareness campaigns are conducted to inform individuals, businesses and public agencies of the commission's existence and role.

At the moment, I can't answer this question. However, I could check and send the information to the committee.

[*English*]

Mr. Matt Jeneroux: That would be great.

There's nothing on your end, Ms. Chassigneux, that would indicate that businesses are pleased, then, or that it's burdensome?

[*Translation*]

Ms. Cynthia Chassigneux: Government directions were provided in late 2015 or early 2016. A parliamentary commission was held and people presented briefs. The only figures that come to mind don't necessarily concern time frames. The complaints may focus more on the processing times for the commission's files, both for jurisdictional matters and for the oversight of research authorizations. We've heard a lot more about this in the press, but I don't have any figures on hand. As I said, I could check with the general secretariat.

[*English*]

Mr. Matt Jeneroux: Thank you.

The Chair: We will now move to Mr. Dubourg for five minutes, please.

[*Translation*]

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

It's my turn to acknowledge the witnesses who presented their briefs. I want to thank them.

We're indeed always saying the subject is complicated. My first questions are for Mr. McArthur.

In your presentation, you spoke of mediation. You said that you resolve the cases submitted to you mostly through mediation. You also said that fines in Canada pale in comparison with the fines in Europe.

Given that you don't seem to impose penalties, do you agree that PIPEDA should establish penalties that are as heavy as or that are similar to the penalties in Europe?

[*English*]

Mr. Drew McArthur: Yes, we are in favour, and have recommended to our parliamentary review committee, that the fining be increased in the public sector, and also in the private sector acts, to have more of a deterrent effect. We are not seeing cases so much in the private sector, but are in the public sector. Information there is being accessed inappropriately, and individuals, even though they are aware of their obligations not to access that information, are still doing so. We believe that we need greater deterrence in the form of larger fines.

[*Translation*]

Mr. Emmanuel Dubourg: Thank you.

I have one final question for you.

You must certainly know Vincent Gogolek, from the BC Freedom of Information and Privacy Association. He appeared before this committee. He told us, among other things, that the federal political parties should also be subject to PIPEDA.

What do you think?

● (1655)

[*English*]

Mr. Drew McArthur: I agree with Mr. Gogolek that Canadians' personal information should be protected, no matter which organization is collecting that information. As I noted in my earlier remarks, in B.C. the political parties fall under the ambit of our act. If a federal political party were collecting the information of a B.C. citizen, we might argue that we would want the ability to investigate that, and we would undertake that.

Mr. Emmanuel Dubourg: Thank you very much.

[*Translation*]

Ms. Chassigneux, in the few minutes I have left, I also want to ask you a few questions.

In your presentation, you said that consent is provided in principle only, and that the term isn't well understood by businesses. Under this legislation, consent is very important, if not crucial.

How can the concept of consent be explained to SMEs and to all businesses?

Ms. Cynthia Chassigneux: First, I hope that I didn't say consent was just a principle.

Mr. Emmanuel Dubourg: You said “in principle.”

Ms. Cynthia Chassigneux: Consent is provided in principle only, but consent is not only a principle. It's a key aspect of privacy. I just wanted to make that clear.

The Act respecting the protection of personal information in the private sector clearly states that consent must be obtained from the person concerned as regularly as possible, and not necessarily without the person's knowledge or from a third party. If consent must be obtained from the third party, it can be done with the consent of the person concerned, or, under some circumstances, without the person's knowledge.

In its recent five-year report, the Commission d'accès à l'information also asked that consent be modified with regard to a person entering a public space or a store with surveillance cameras, for example. The people concerned must be informed about this collection of information and they must know they're in a monitored location. This type of collection of information without a person's knowledge must be shared with the person so that they know they'll be filmed when they enter that location. It's a form of implied or express consent.

Mr. Emmanuel Dubourg: I understand.

Very quickly, Mr. Chair.

[*English*]

The Chair: Go ahead, Monsieur Dubourg, very quickly, please.

[*Translation*]

Mr. Emmanuel Dubourg: I want to ask Ms. Chassigneux whether she has any information to give us. She brought up a point that I also find very important. She spoke of files and personal information found in the files. She now wants us to look at the purpose of the collection.

Ms. Chassigneux, since I don't have any more time, I would appreciate it if you could send us the information.

Ms. Cynthia Chassigneux: No problem.

Mr. Emmanuel Dubourg: Thank you.

Ms. Cynthia Chassigneux: We talked about this in our recent five-year report, but I would be happy to send you the information.

Mr. Emmanuel Dubourg: Thank you.

[*English*]

The Chair: Thank you, Mr. Dubourg. I appreciate that.

We have our last official time allocation of three minutes for Ms. Trudel, from the New Democratic Party.

But colleagues, we do have a little bit of time. If any of the rest of you have questions, especially those who haven't asked questions yet —I see Mr. Long indicating that he does—we'll have a little bit of time to ask some questions at the end before we break.

Then, colleagues, we do have a little bit of committee business that we need to take care of afterwards in regard to a budget for this committee, so we'll consider that as well.

Ms. Trudel, the floor is yours.

[*Translation*]

Ms. Karine Trudel: Thank you, Mr. Chair.

I'll continue to ask Ms. Chassigneux questions.

Earlier, we concluded with a discussion on the changing settings of certain websites. Are there related applications that help find information, for example, in a website and transfer it to another website?

Is platform interconnectivity part of the issue of free consent with regard to personal information?

Ms. Cynthia Chassigneux: Normally, when information is collected on a site and can be transferred to another site, the people responsible for the first site should inform the people providing the information that the information could be transferred to the second site.

If you have a cellphone, you have mobile applications. You also have the possibility of knowing whether the mobile applications can collect the information in your cellphone. When information is transferred from one site to another, it must be done transparently. People must be able to know how their information is getting around.

Does the information remain on the first site? Does it go from the first site to the second site? Where is the information? Where is it retained? Is it retained in Quebec, if we use Quebec as an example? Is it retained outside Quebec?

This must all be transparent, and the businesses must be transparent. We're saying that businesses must establish a culture of privacy. I'm not saying that businesses don't currently have this type of culture. That's not what I mean. I don't remember which of the two commissioners talked about it, but I think it was Ms. Clayton. I'm referring to assessments of the impact of a program's implementation. We need to know what's true, how things are done, who things are done for and why things are done. It's important for the person and Internet user or for anyone who has information that will be collected and shared.

I don't know whether I answered your question.

● (1700)

Ms. Karine Trudel: Yes, you did. Thank you.

[*English*]

The Chair: Thank you very much.

Mr. Long, go ahead please.

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

It's great to be back on the committee again after a week away. You did miss me.

I have a question. I want to continue Mr. Saini's questioning with respect to children and ask Ms. Clayton and Ms. Chassigneux their opinions on meaningful consent.

How do you control and manage that? As Mr. Saini said, there are sites for children in the U.S. that have much more tracking software than sites for adults. I have some friends who have kids who are 10, 11, and 12 years old who are on the Internet all the time, and it's a major concern for the parents to know exactly what sites they're going to, what things they're clicking on as well, and what information they are giving away.

Maybe I'll start with Ms. Chassigneux for your opinion whether PIPEDA actually protects children enough, or on what changes you would make to it.

[*Translation*]

Ms. Cynthia Chassigneux: I wouldn't dare comment on the federal legislation. However, one thing is certain. As mentioned earlier, in Quebec and British Columbia, the discussions about personal information and privacy concern everyone, regardless of age.

In its 2011 five-year report, Quebec did recommend that the protection of minors be taken into consideration. Minors are visiting websites more and more often, or, as you said, spending the entire day surfing on the Internet and on mobile applications. This issue is a concern in Quebec. There have even been awareness campaigns.

Recently, the minister responsible for access to information and the reform of democratic institutions launched an information campaign. In 2011-12, the Commission d'accès à l'information du Québec also conducted an awareness campaign in schools for students. It's important. We're continuing to recommend this in our report. I think the federal legislation should take this into consideration. If we're taking this into consideration, it should also be taken into consideration at the federal level.

[*English*]

Mr. Wayne Long: Thank you.

Ms. Clayton, can you weigh in on that, please?

Ms. Jill Clayton: In Alberta, I think we have essentially the same situation as was described in B.C. and Quebec. The legislation protects everybody's personal information, regardless of age. We do have the idea of a mature minor who is able to thoughtfully exercise his or her rights under the legislation, who can make access requests, for example, and make a complaint with our office. We had that recently—a matter that resulted in an order in our public sector. It had to do with a transgender student who made a complaint to our office.

The legislation in Alberta does not specifically address this issue of children. Are they particularly vulnerable? That's a matter I would address. Sometimes a self-reported breach comes in, and in terms of notifying individuals, that is a factor that I take into consideration. Whose information was breached? Do we have a vulnerable population? Are there seniors, dependants, adults, children? There are lots of potentially vulnerable populations.

I will say that a couple of years ago, we participated, along with my co-panellists, in the Global Privacy Enforcement Network sweep of Internet sites and apps, specifically those that were targeting children, and we found some disturbing results. A lot of these websites and apps are collecting information of children. They're not particularly transparent about what they're collecting, nor are they necessarily collecting only the information that is necessary for their purpose, for example, the service that the app is producing. That doesn't necessarily require anything special, or amendments to the existing legislation, because I'm not sure that some of those apps and websites are complying with existing legislation. I think you can get at some of those issues through existing legislation.

● (1705)

The Chair: Mr. Long.

Mr. Wayne Long: Very good.

The Chair: Does anybody else have any questions they would like to ask?

No?

Colleagues, I'm going to thank our witnesses on behalf of everyone here. Thank you very much for taking the time out of your very busy schedules to join us here as we deliberate on and review the federal legislation when it comes to private sector protection of information.

Colleagues, I'm going to suspend the meeting right now. We're going to go in camera and have a discussion about a few things.

I would like to thank our witnesses. We know we can call upon you again if we need to. For those of you who have committed to sending us some follow-up information, we look forward to that.

Thank you very much. Have a good day.

[*Proceedings continue in camera*]

Published under the authority of the Speaker of the House of Commons

SPEAKER'S PERMISSION

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca