HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 059 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, May 9, 2017

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, May 9, 2017

● (1535)

[*English*]

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

Welcome to the 59th meeting of the Standing Committee on Access to Information, Privacy and Ethics.

Pursuant to Standing Order 108(3)(h)(vi), we are studying the Personal Information Protection and Electronic Documents Act, PIPEDA.

We are very pleased to have with us as witnesses today from the Department of Innovation, Science and Economic Development, Steve Joanisse, legal counsel, innovation, science and economic development legal services; Krista Campbell, director general, digital policy branch, spectrum, information technologies and telecommunications sector; and Charles Taillefer, director, digital policy branch, spectrum, information technologies and telecommunications sector.

From the Competition Bureau, we have Josephine Palumbo, deputy commissioner, deceptive marketing practices directorate; and Morgan Currie, associate deputy commissioner, deceptive marketing practices directorate.

From the CRTC, we have Steven Harroun, chief compliance and enforcement officer; and Daniel Roussy, general counsel and deputy executive director. Welcome, all.

We'll start with opening comments from the organizations in the order you were introduced. I believe that means Madam Campbell we'll start with you for up to 10 minutes, please.

Ms. Krista Campbell (Director General, Digital Policy Branch, Spectrum, Information Technologies and Telecommunications Sector, Department of Industry): Thank you.

[*Translation*]

Mr. Chair, members of the committee, it is my pleasure to be here today to discuss the Personal Information Protection and Electronic Documents Act.

[*English*]

We've introduced colleagues. I'm pleased to be here with counsel and my director responsible for this piece of legislation.

The responsibilities of my team include providing advice, guidance, and support to the minister for his role as the lead minister of PIPEDA.

I should note that we hold similar responsibilities for Canada's anti-spam legislation, also known as CASL. We operate the national coordinating body for CASL, which is responsible for the policy oversight and coordination of the anti-spam initiative.

It's a best practice to review marketplace rules on a regular basis, particularly in the case of legislation that is foundational to building trust in the digital economy. I commend the committee for undertaking this important work.

The Personal Information Protection and Electronic Documents Act is a key element of the Canadian legal framework to support development of the digital economy. It is the principal instrument for protecting personal information within the context of commercial activities. It is designed to balance privacy protection with the needs of organizations for information to conduct their business.

[*Translation*]

As stated by the Privacy Commissioner during his testimony, there is evidence that PIPEDA still provides a solid foundation, but that does not preclude refinements and adjustments to the act to ensure that it remains relevant.

Witnesses have proposed legislative changes in a number of areas. Innovation, Science and Economic Development Canada (ISED) looks forward to the committee's thoughts in each of these areas. The results of the study of consent currently being undertaken by the Office of the Privacy Commissioner will also greatly inform this discussion.

[*English*]

My objective for today is to highlight some of PIPEDA's unique and important features and the reason why the act is the responsibility of Innovation, Science and Economic Development, which is the microeconomic department for the Government of Canada.

First, we must consider the purpose of the act. When PIPEDA was introduced in 2000, the industry minister at the time stated that the act was created with a single policy goal: to build trust in electronic commerce, for the purpose of growing electronic commerce. PIPEDA creates trust by preventing organizations from doing things with personal information that the average person would think are not reasonable in the circumstances. At the same time, it allows information to flow so that businesses can provide the products and services that customers have come to agree to and expect.

This balancing of privacy and economic considerations has afforded PIPEDA much success, as you have heard from some previous witnesses. It has adapted to an evolving landscape and the unique circumstances faced by the wide range of organizations that are subject to this act.

The Office of the Privacy Commissioner has successfully conducted investigations into complaints under PIPEDA pertaining to technologies and business models that were unforeseen when the act was first implemented, including online behavioural profiling and social media applications.

PIPEDA is also mindful of other important public policy objectives, such as freedom of expression and public safety. For example, PIPEDA recognizes the right to freedom of expression by permitting information to be collected and used without consent for journalistic or artistic purposes. Any changes to PIPEDA should be made in consideration of these various objectives and must seek to balance those considerations.

Second, we must consider the scope of PIPEDA and the fact that it cannot be understated. It protects all personal information captured in the course of business. It applies to nearly all private sector organizations, with the exception of those governed by substantially similar provincial legislation. Therefore, we must ensure that the act remains flexible. Flexibility ensures that PIPEDA is scalable and that organizations can adapt the act's requirements to the size of their business, whether they're a small dry cleaner or a large multinational corporation. In fact, PIPEDA was designed specifically to apply to all economic sectors.

[*Translation*]

Finally, we must consider the need for harmonization with other privacy regimes. PIPEDA is based on 10 internationally recognized principles that protect individual privacy by giving individuals control over their personal information. These same principles are the basis for privacy laws around the world.

Harmonization with provincial privacy laws, and those of our international trading partners, provides a huge advantage to Canadian businesses that operate in multiple jurisdictions.

[*English*]

This harmonization also facilitates the free flow of data across borders, which is essential to the growth of electronic commerce, both domestically and internationally.

Related to this, you've heard from many witnesses on the importance of PIPEDA's adequacy status with the EU. This adequacy status relies on PIPEDA maintaining a similar level of protection and redress for EU citizens as afforded by the EU's own privacy regime. As others have remarked, our adequacy will be reviewed at some point in the future. We are working closely with colleagues at Justice Canada, Global Affairs, and Public Safety to engage the European Commission officials in discussions to understand what this review may entail—in particular, the timing and the scope of the next potential review.

I would also highlight that we are still in the process of implementing amendments that arose from the passage of the Digital Privacy Act in 2015. These changes included new enforcement tools for the commissioner, the aim of which was to provide the commissioner with greater leverage to encourage compliance with the act.

Another change implemented by the Digital Privacy Act is the enhancement of the consent requirements. This was implemented primarily in response to calls to strengthen privacy protection for children online. The approach to this amendment respects provincial jurisdiction over minors.

Recent changes also included new exceptions to the requirement to obtain consent for disclosure of personal information, both for public interest reasons, such as prevention of fraud, and to reduce red tape for businesses, such as for managing their employees. We will be closely following the adoption of these legislative changes and their impacts on the marketplace.

The most high-profile change, which has yet to be implemented, is a new requirement for organizations to report data security breaches that pose a risk of harm to individuals. These requirements will come into force when regulations related to the provisions are finalized. We are working with the Department of Justice in support of these regulations. These changes and others were designed to maintain the important balance in PIPEDA between privacy protection, economic development, and innovation, and other public policy goals.

● (1540)

[*Translation*]

As I mentioned earlier, we look very much forward to hearing the committee's views at the conclusion of this important study. In the meantime, my officials and I are at your disposal to answer questions about the act.

[*English*]

Thank you for your interest in this subject.

The Chair: Thank you very much, Madam Campbell.

We now will go to the Competition Bureau and we'll have remarks from Ms. Palumbo.

Ms. Josephine Palumbo (Deputy Commissioner, Deceptive Marketing Practices Directorate, Competition Bureau): Thank you for the invitation to attend this committee meeting as well. I'm joined by my colleague from the bureau, Mr. Currie.

I understand the committee is looking into PIPEDA, and in that context has questions about the bureau's role with respect to Canada's anti-spam legislation, or CASL, as well as the bureau's experiences with administrative monetary penalties, or AMPs.

I'll begin by providing some context about the Competition Bureau and its mandate, and then move to your specific concerns. I will not be commenting on PIPEDA per se, as that is outside the bureau's purview.

[*Translation*]

The Competition Bureau, as an independent law enforcement agency, ensures that Canadian consumers and businesses prosper in a competitive and innovative marketplace. Headed by the Commissioner of Competition, the Bureau is responsible for the administration and enforcement of the Competition Act and three labelling statutes.

[*English*]

The Competition Act provides the commissioner with the authority to investigate anti-competitive behaviour. The act contains both civil and criminal provisions and covers conduct such as bid-rigging, false or misleading representations, price-fixing, and abusing a dominant market position, among other things. The act also grants the commissioner the authority to make representations before regulatory boards, commissions, or other tribunals to promote competition in various sectors.

As noted above, when conducting investigations, the bureau uses the Competition Act's relevant criminal and civil provisions. The introduction of CASL brought about specific amendments to the Competition Act that enabled the bureau to more effectively address false or misleading representations and deceptive marketing practices in the electronic marketplace, such as false or misleading sender or subject-matter information, electronic messages, and website content, such as a locator, meaning a website or an IP address. The changes provided technologically neutral language to allow us to better address competition offences in the digital economy. I would note that the bureau had these powers before CASL, but now the requirements of proof have been lessened.

For the most part, the bureau's investigations are commenced following a complaint. Such complaints may come from a number of sources, including consumers, businesses, industry associations, the media, or stakeholders.

As a law enforcement agency, the bureau conducts its activities, including investigations, in confidence, meaning that all non-public information gathered by the bureau in enforcement matters, whether obtained voluntarily or through the use of formal powers, is held on a confidential basis.

● (1545)

[*Translation*]

This is fundamental to the Bureau's ability to effectively continue to advance its investigations in the public interest.

[*English*]

The law requires that we not comment publicly on an investigation until the matter has been made public either by the party, or certain steps have been taken, such as the filing of an application with the Competition Tribunal, or the announcement of a settlement.

[*Translation*]

Even in those instances, we are required by law to keep confidential any information which is not public. This is done both to protect the integrity of the Bureau's investigations as well as to protect the parties and others.

[*English*]

That said, the Competition Act's “confidentiality” provision, section 29, does allow the bureau to share confidential information with other law enforcement agencies for the purpose of the administration and enforcement of our act.

Turning now to AMPs, the bureau may only seek them in a civil context, not criminal. Also, the bureau does not impose AMPs. They are either reached through a settlement with the target of an investigation, or they are imposed by the Competition Tribunal or a court after a finding of reviewable conduct under the Competition Act.

[*Translation*]

The goal of an administrative monetary penalty for civilly reviewable conduct is to promote compliance in a market and deter companies from misleading Canadian consumers, all of which is in the public interest.

[*English*]

Let me give you three recent examples where the bureau has obtained AMPs under the Competition Act. First, in June of 2016 the bureau announced its first settlement involving the new CASL provisions. The settlement with Avis and Budget resolved an investigation wherein the bureau had concluded there was false or misleading advertising for prices and discounts on car rentals and associated products.

Specifically, certain prices and discounts initially advertised by the two companies were not attainable because consumers were charged additional mandatory fees that were only disclosed later in the purchasing process when making a reservation. The prices were advertised on Avis' and Budget's websites, mobile applications, and emails, as well as through other channels. As part of the settlement in this case, Avis and Budget paid $3 million in an administrative monetary penalty to promote compliance with the law going forward.

Earlier this year, the bureau settled its case with Amazon where we again utilized an amended Competition Act provision introduced through CASL addressing false or misleading representations in all forms of electronic messages. In this instance, Amazon often compared its prices to a regular or list price, signalling attractive savings for Canadian consumers.

The bureau's investigation concluded that these claims created the general impression that prices for items offered on Amazon's website were lower than prevailing market prices. The bureau determined that Amazon relied on its suppliers to provide list prices without verifying those prices were accurate. In this case, the savings claims were advertising on Amazon.ca, in Amazon mobile applications, and in other online advertisements, as well as in emails sent to customers. The bureau negotiated a $1-million AMP in this instance.

Finally, on April 24, 2017, the bureau announced it had reached a negotiated consent agreement with Hertz Canada Limited and Dollar Thrifty Automotive Group Canada, Inc. where both companies will pay a total of $1.25 million in an administrative monetary penalty, ensure their advertising complies with the law, and implement new procedures aimed at preventing advertising issues in the future.

The consent agreement is the result of an investigation where the bureau concluded that Hertz and Dollar Thrifty were advertising enticing low prices to attract consumers. However, those low prices were unattainable because mandatory fees were systemically added to those prices. The bureau concluded that the companies' price representations on their websites and other channels were misleading, and it was not sufficient for the companies to provide an estimate of the total price before consumers completed their reservation.

It is important to understand that, when negotiating an AMP or advocating in favour of one before the Competition Tribunal or the courts in relation to false or misleading advertising, the bureau considers a number of aggravating or mitigating factors that are listed in the Competition Act. Those factors include the reach of conduct within the relevant geographic market, the frequency and duration of the conduct, the vulnerability of the class of persons likely to be adversely affected, the effect on competition in the relevant market, the gross revenue from the sales affected by the conduct, the financial position of the person against whom the order is made, the history of compliance with the Competition Act by the persons against whom the order is made, and any other relevant factor.

In the interests of time, I will end my comments here.

● (1550)

[*Translation*]

I would be happy to answer any questions you have.

[*English*]

I would like to thank the committee for the opportunity to appear here today.

The Chair: We're so glad to have you. Thank you very much.

Now our last witness will be from the CRTC.

I believe we're going to start with Mr. Harroun, please.

Mr. Steven Harroun (Chief Compliance and Enforcement Officer, Canadian Radio-television and Telecommunications Commission): Thank you, Mr. Chair, for inviting us to appear before your committee.

My name is Steven Harroun, and I'm the CRTC's chief compliance and enforcement officer. With me today is my colleague Daniel Roussy, general counsel and deputy executive director of the CRTC's legal sector.

We appreciate the valuable work that your members do to protect Canadians' privacy, a significant concern in today's digital age, and we recognize that the focus of your current work is on the Personal Information Protection and Electronic Documents Act. The CRTC follows the privacy legislation, as do all federal government departments and agencies, but has no direct experience as a regulatory body with this act.

However, we understand that the committee is interested in hearing about our experiences in enforcing Canada's anti-spam legislation. We believe there are aspects of our experience that may be useful to consider as part of your study, in particular, our ability to impose administrative monetary penalties.

Mr. Chair, let me begin with a brief overview of the legislation to provide context for our observations about the effectiveness of such penalties. In a nutshell, Canada's anti-spam legislation, known as CASL, is meant to provide Canadians with a secure online environment while ensuring that businesses can compete in the global marketplace. CASL gives the commission the authority to regulate certain forms of electronic contact, consisting of the sending of commercial electronic messages, the alteration of transmission data in electronic messages, and the installation of computer programs on another person's computer system in the course of commercial activity.

The fundamental underlying principle is that such activities can only be carried out with consent. The CRTC is responsible for CASL's administrative monetary penalty framework, which includes the imposition of penalties for violations. CASL is an opt-in regime, which means that consent must be obtained prior to the sending of commercial electronic messages to Canadians. CASL applies to the commercial electronic messages sent via email and through social media accounts, as well as text messages sent to cellphones.

Consent to receive these messages can either be express or implied, as stipulated in the act. Express consent means that the person has clearly and proactively agreed to receive the message, for example, someone voluntarily opts in by signing up at a website. Once express consent is obtained, commercial electronic messages can be sent, until the recipient notifies the sender that he or she no longer wants to receive them.

Consent can be implied, for example, through an existing business relationship with the consumer based on a previous commercial transaction. It also pertains to personal or family relationships, or in an existing non-business relationship, such as a membership in a club, association, or volunteer organization. In every case, CASL sets out that the burden of proof regarding consent rests with the person alleging consent.

In addition to consent, senders of commercial electronic messages must clearly identify themselves, and each message must also contain an unsubscribe mechanism, which is clearly and prominently set out, that allows consumers to readily unsubscribe if they no longer wish to receive messages.

● (1555)

[*Translation*]

Mr. Daniel Roussy (General Counsel and Deputy Executive Director, Canadian Radio-television and Telecommunications Commission): Mr. Chair, Canada's anti-spam legislation was never intended to eliminate all spam. Its objective is to deter the most damaging and deceptive forms of spam and other electronic threats such as identity theft, phishing and the spread of spyware and malware.

When it is alleged that a violation has occurred, the Chief Compliance and Enforcement Officer has a number of tools at his disposal to ensure the act is complied with.

[*English*]

Our enforcement tools include a warning letter to bring to the attention of the business a minor violation requiring corrective action, and a notice of violation, which is issued for more serious offences. The enforcement measures may include monetary penalties. Notices are also published on our website. We warn Canadians of illegal online practices so that they are aware and can report any suspected violations.

An undertaking, which is similar to a negotiated settlement or agreement with the other party, is where the company or individual undertakes to come into compliance. For instance, the party might need to implement a corporate compliance program and report on its activities, or it may have to pay a specified amount, although this payment is not considered a monetary penalty as such.

The chief compliance enforcement officer uses his discretion in selecting and applying the most appropriate enforcement response. Our goal is to ensure compliance with the law and to prevent recidivism.

Underpinning these enforcement tools are the CRTC's outreach and education program efforts. Before the law came into force, CRTC delivered information sessions to interested parties across the country to explain the new requirements and encourage compliance. To this day, we continue to undertake an education outreach program and share lessons learned from enforcement actions taken.

[*Translation*]

It's important to understand that administrative monetary penalties are just one part of our toolbox. Penalties tend to be used as a last resort after all other efforts have failed. While we have issued warning letters, monetary penalties have been reserved for the most egregious cases.

Depending on the nature of the violation, the CRTC has the authority to impose up to $1 million per violation for individuals. And up to $10 million per violation for a corporation or group. There are factors laid out in the legislation that we must take into consideration when determining the appropriate penalty.

[*English*]

The tools provided to us in CASL to protect Canadians are not limited to monetary penalties, of course. The chief compliance and enforcement officer also has the authority to seek a judicial pre-authorized warrant in order to enter a residence or business to verify compliance with the act.

For example, along with national and international partners, the CRTC took down a command and control server disseminating spam and malicious malware located in Toronto in December 2015 as part of a coordinated international effort. This disrupted the Win32/Dorkbot, which was one of the most widely distributed malware families and which had infected more than a million personal computers in over 190 countries.

Mr. Steven Harroun: Of course, in today's interconnected world, spam and other electronic threats are not confined to Canada. One of the most important tools Parliament provided to the CRTC is the ability to share information and seek enforcement assistance of our international counterparts.

To date, the CRTC has entered into international agreements with the Federal Trade Commission and the Federal Communications Commission in the United States and the Department of Internal Affairs in New Zealand.

As well, to address the challenge of spam coming from outside our borders, we collaborate with our international partners through the Unsolicited Communications Enforcement Network, or UCENet. The purpose of this network is to promote international spam enforcement co-operation and address spam-related problems such as online fraud and deception, phishing, and dissemination of viruses.

The CRTC has also signed a memorandum of understanding with 11 enforcement agencies from eight different countries throughout UCENet. These countries include the United States, Australia, New Zealand, the Netherlands, the United Kingdom, Korea, and South Africa. We share our knowledge and expertise through training programs and staff exchanges and inform each other of developments in our respective countries' laws.

Working with our partners, we are better equipped to ensure that people who distribute commercial messages, local or foreign, comply with Canada's anti-spam legislation.

In conclusion, we are convinced that administrative monetary penalties, when used with other enforcement methods, are a deterrent to non-compliance. We believe that companies have changed their practices to avoid potential penalties. This observation is based on our experience with CASL to date, as well as our experience in enforcing telemarketing over the past decade.

If we have any advice to offer, Mr. Chair, it is that enforcement agencies need a broad range of tools in their arsenal that they can tailor to the circumstances of each case.

We welcome any questions you may have.

● (1600)

The Chair: Thank you, Mr. Harroun. We appreciate it very much.

We're going to proceed to the rounds of questioning now. The first round will be seven-minute questions followed by five-minute rounds. Then we'll see how much time we have left.

I'll let everybody know that we do have a bit of committee business to take care of at the end of this meeting. When that happens, we'll be moving in camera to discuss that, and I'll ask for the expeditious clearing of the room.

We'll start with Mr. Saini, please.

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

I'm going to concentrate on two different regimes. First, I'm going to concentrate on Europe and then on the United States. You can answer the questions as specific to your area of expertise.

Something that we've heard a lot about from other witnesses in front this committee is maintaining the adequacy status with the general data protection regulation, GDPR, which is coming into effect in May 2018.

Are you preparing for that, or is there any movement to making sure we maintain an adequacy standard with the EU because of the competitive advantage it would offer?

Ms. Krista Campbell: It think it's one of the most important things that businesses are focusing on right now, and there's interest in knowing exactly what will be coming.

The EU has indicated that they will be looking to review Canada. They have not launched any kind of formal process at this point. We have begun reaching out at my level, at the working level, with European Commission officials to start a discussion around timing and scope of the review. We've had discussions with them about how they've gone about their recent reviews with other countries; what did and didn't work well in terms of providing information; and where there are best practices or good standards they thought were very useful.

We have face-to-face meetings with European officials next week. Then we hope to exchange some preliminary information on what Canada's privacy regime looks like. It'll be broader than just PIPEDA, but we'll give them a good primer on PIPEDA; the Privacy Act; changes that would have been made under Bill C-51; and Security Of Canada Information Sharing Act, SCISA; as well as some information about the fact that, because we're a federation, we have a unique set of requirements that include both provincial privacy laws as well as federal laws. Then we'll work from there on what they think they want to discuss with us more formally once they trigger the review. As I said, it hasn't been formally triggered yet. We definitely are starting the work on planning for what the scope and timing would look like.

Ms. Josephine Palumbo: My only comment with respect to the Competition Bureau is that many of the markets we deal with are global in scale. The bureau co-operates regularly with its international counterparts, the United States and the European Union, and has developed a number of partnerships and MOUs with a number of national and international agencies. We currently have 18 instruments involving 14 different jurisdictions with respect to competition worldwide. Certainly the dialogue continues in the area.

Mr. Steven Harroun: From the commission, I would echo my Competition Bureau colleague's remarks in that we undertake a memorandum of understanding with countries around the world so that we can share information and ensure that those countries comply with our legislation. We're obviously not experts on theirs, but....

Mr. Raj Saini: One of things that's worrisome, and that other witnesses have spoken about, is the administration of penalties and sanctions against companies. As you know, some of the figures you mentioned in your opening remarks were not as high as they would be in the European Union. In the European Union the maximum penalty would be 4% of annual turnover, or 20 million euros.

Is there some...? I mean, if you're going to have adequacy, then you're going to have to have penalties on both sides.

Ms. Josephine Palumbo: Well, we think that the legislative framework under the Competition Act is working quite nicely. Since 2015 we've registered with the Competition Tribunal 13 consent agreements, which totalled $26 million in administrative monetary penalties—$24 million with respect to restitution to Canadian consumers and $1.5 million in terms of donations to public interest groups.

We think we're making a difference. We're working within our legislative framework, looking at aggravating and mitigating circumstances when we're assessing the proper quantum of an administrative monetary penalty. Our ranges in terms of the quantum of an AMP can be as high as $15 million for a corporation and as high as $1 million for an individual. That's within the context of a civil regime. If the offences at issue are criminal in nature, then we're looking at potential jail time for some of the offenders, including fines and jail time of 14 years for an indictable offence or one year for a summary conviction.

We believe that our legislative regime that's in place is quite effective and has been garnering results on behalf of Canadians.

● (1605)

Mr. Raj Saini: The second area I want to focus on is the United States. As you know, on January 25 executive order 13768 was executed, which affected the privacy rights of Canadians. Perhaps I can read you this part of the executive order, which affects section 14 of the Privacy Act in the United States:

> Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.

Do we have some response to that, or is there some mechanism that we're putting in place to protect the privacy of Canadians?

Mr. Charles Taillefer (Director, Digital Policy Branch, Spectrum, Information Technologies and Telecommunications Sector, Department of Industry): To my understanding, that piece of legislation would be equal to our Privacy Act, so it wouldn't necessarily have an effect in terms of private-sector personal information collection. That order applies to government institutions in the same way our Privacy Act would, so it wouldn't necessarily be related to PIPEDA.

Mr. Raj Saini: But private businesses doing business on both sides of the border would contain the information of Canadians, would they not?

Mr. Charles Taillefer: The order that was issued in the States applies to government organizations in terms of the privacy protections provided on the information that they collect, not the information that is collected by private sector organizations.

The Chair: That's an important distinction.

Thank you very much.

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

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): I'd like to thank you for being here today—and to also thank your staff for helping to prepare you for today.

I want to start my questions along the line of the order-making powers being requested by the Privacy Commissioner. In 2007, when we went through a similar review, they were not requested to be part of this act. However, since then some things have changed, particularly with the Privacy Act and Access to Information Act. He now has order-making powers.

I'm hoping to get an opinion from all three groups here on whether or not you think granting the Privacy Commissioner order-making powers under PIPEDA is fair to do, or appropriate. As well, do you think it's essential that the Privacy Commissioner has order-making powers under all three pieces of legislation?

Ms. Krista Campbell: We've had a lot of success with PIPEDA and with the model that we have with the Office of the Privacy Commissioner. It was established as an ombudsman model and was very much an education-first, collaborative organization that worked with businesses and individuals that had concerns or complaints and tried to find collaborative ways to discuss and get to solutions.

As we watch technology change—and technology is specifically referenced in the purpose statement for PIPEDA—it's very clear that data is now regularly called the new oil. It is flowing internationally and is critically important. It is collected in ways that we didn't even foresee in 2000, when this was first enacted, and that creates pressures in terms of how an organization treats its data. It also creates real concern for individuals about how their data is handled and whether they even know what was collected and how it's being used.

When we look at the model we have for the Privacy Commissioner—and as you said, in 2015 we increased the tools that he had available to him with the introduction of compliance agreements—and as we move into any kind of thinking around the next review of the act, the question will really be around balancing whether we want an ombudsman model with the same types of powers, or whether we move to a different type of model.

The nature of the mandate could be very different. If you give order-making powers but still want to be able to have open conversations with business, saying, “Come in and talk to us early on and we'll work with you on how you go about designing new products and services,” then having greater order-making power in the same organization could cause some concerns about what the core mandate priorities are. A holistic review of the Office of the Privacy Commissioner and PIPEDA would need to be undertaken before we would decide to give new powers.

That being said, lots of organizations have stronger powers, and they are able to balance those stronger powers with a really effective regime of working with businesses and individuals. There is pressure to ensure that the Privacy Commissioner is seen to be a best practice, both domestically and internationally.

● (1610)

Mr. Matt Jeneroux: Going back to your comments on page 3, you highlight that you're still in the process of implementing amendments that arose in the passage of the Digital Privacy Act in 2015. It's now 2017. Are you having challenges with some of those, with regard to powers?

Ms. Krista Campbell: There are no challenges specifically. Part of the timing issue, though, was the election in that period, which required that we stand down on any consultations. This was an area where we wanted to make sure we did very full consultations, so we have been able to get out a lot. Actually, the consultations have provided a great deal of information on the regulations, which we've been able to rely on to say that we likely have found some pretty common middle ground for a lot of the initiatives going forward. We expect to have something in the *Gazette* relatively soon, hopefully within the next couple of months.

Ms. Josephine Palumbo: From my perspective, again, I'm not in a position to comment on the appropriateness of the power for the Office of the Privacy Commissioner, but I can say that the framework that's in place within the Competition Bureau mandate is quite effective.

From the bureau's perspective, AMPs are an important component of the Competition Act. They clearly act as a means of promoting compliance with the law. They act as a disincentive for targets of investigations to continue to break the law. When you look at them within the context, for example, of the consent agreement framework, whereby consent agreements are registered with the Competition Tribunal and then become court orders, we clearly see them having a tremendous impact because they avoid the costly and lengthy nature of litigation.

Within our legislative framework, we think they're working, they're working quite well, and they're producing results for Canadians.

Mr. Steven Harroun: As I said in my opening remarks, the broader the range of the tools, the better it is for the Privacy Commissioner. What's important is the construct around that. For example, at the CRTC, as I am the chief compliance and enforcement officer, my team leads investigations. I issue notices of violation, etc. The businesses or individuals who are subject to those violations always have the option to make representations before the commissioner writ large—the CRTC writ large—to present their case there if they're not in favour with my views. The construct will be important.

Mr. Matt Jeneroux: I have about 50 seconds left. With that, I'll throw out the question for anybody who wants to get on record first, and hopefully we'll come back to it later in the questioning.

It's on the right to be forgotten. The Privacy Commissioner, right now, says he's on the fence on what to do, and what not to do, with it. He's studying it. Unfortunately, it's not going to be finished before our committee is complete, but it's something that I think is important, not only in public service roles like ours and in those of many around the table, but long term for those of us around the table who have kids as well.

I'll throw it open for about 10 seconds before the chair cuts me off.

Ms. Krista Campbell: I agree. I would assume that maybe we'll come back to that. I think that we're maybe a lot in the same boat that this requires more thought and study. It's a challenging issue, and there are a number of principles that need to be applied. You're very right about the issues around the right to be forgotten if you did something when you were 14—and technology is so readily available—versus you said something last week online that you now regret having said. How do we find a reasonable balance in that?

● (1615)

The Chair: Anyone else? No. I wish I could remember some of the stuff I did when I was a teenager.

Madam Trudel, seven minutes please.

[*Translation*]

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

Witnesses, thank you very much for your remarks and for being here today.

My questions will be primarily for the CRTC.

Just now, you talked about administrative monetary penalties. Can you elaborate on what the administrative monetary penalties are? What is the exact process that leads to such penalties?

Mr. Daniel Roussy: An administrative monetary penalty is one of a number of ways to ensure, or to try to ensure, that a company or an individual, who seems to have gone astray, gets back on the right track. The penalty is neither punitive nor criminal, as my colleague from the Competition Bureau mentioned earlier. The purpose of the penalty is to encourage someone or a company to return to the right path. We do not want to prohibit them from doing business, we want to encourage them to do it properly. This is the basic philosophy behind an administrative monetary penalty.

Furthermore, as we mentioned in our opening remarks, administrative monetary penalties are one part of a whole host of other tools, which allows them to be effective. In itself, the penalty would be ineffective if it were not combined with other things at the same time.

Let's now turn to the method. Generally, each law has its own details or its own recipe, if you will, for administrative monetary penalties. In this case, section 20 of Canada's anti-spam legislation sets out the methods or procedures for assessing how to impose such a penalty. In addition, in recent years, the courts, particularly the Federal Court, have rendered many decisions that we can use to assess cases.

For example, if I take the English copy of the legislation I have before me, the nature and extent of the violation are part of the criteria for determining the amount of a penalty. Questions may come up. Is it a big or small violation? How many violations were there?

In our case, still under the legislation, the individual's ability to pay is a determining factor. Other questions arise. Can the person pay a large or small penalty? Will the penalty for the violation allow or encourage the person to stop his or her actions that might be outside the scope of the act?

So a bunch of factors are put together. These factors are left to the discretion of the head of Chief Compliance and Enforcement Officer who looks at them when a penalty is required.

Ms. Karine Trudel: You're talking about section 20 and all the tools that the legislation gives you. Do you think the legislation is sufficiently comprehensive to set those penalties, or are there improvements to be made?

Mr. Daniel Roussy: The current framework of the act is extremely flexible. This inherent flexibility enables us to act with some latitude through a precise framework within which to suggest answers.

To answer your question specifically, you no doubt know that the legislation is still quite new. We are talking about 2014. So it's difficult for me to answer directly as to whether it gives us as much flexibility as possible.

At the moment, there are ongoing investigations, others have been completed and decisions have been made. We are really at the very beginning of our mandate.

So I'm a little embarrassed. I cannot answer that question now. I do not really have the answer.

Ms. Karine Trudel: We'll wait a little longer.

Mr. Daniel Roussy: Thank you very much.

Ms. Karine Trudel: My questions are for Josephine Palumbo.

Earlier, in your speech, you said that investigations were launched after complaints had been filed.

Do investigators in your organization conduct audits or are investigations only launched after complaints have been filed?

● (1620)

Ms. Josephine Palumbo: Investigations are a very important part of the Competition Bureau's work. With respect to complaints filed under the Competition Act, we first look at the information to determine whether it raises a problem under the act.

[*English*]

Complaints are a big part of what we do at the Competition Bureau. They can come to us from a number of sources, including the public and the media. We also receive complaints from industry associations.

We analyze them to see whether or not they raise issues under our law. If they do, then we may initiate an investigation or launch a formal inquiry. When we do that, we gather additional information. How? We can approach the courts with production orders under section 11 to obtain documents or written returns of information, or to require persons to appear under examination before a presiding officer. We will analyze information that's received as well through other tools, such as search warrant powers. We may execute search warrants or seize computer systems. As well we have the opportunity to garner information through the Criminal Code, through production orders.

[*Translation*]

Ms. Karine Trudel: Thank you.

[*English*]

The Chair: For the last of the seven-minute rounds we'll go to Mr. Erskine-Smith, please.

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

Ms. Campbell, in your remarks you mentioned that PIPEDA is largely effective. You mentioned some fine tuning, I think, with respect to the mandatory breach reporting that has already been implemented. We're obviously undertaking a study on what possible recommendations we should come up with to improve PIPEDA. Is your department undertaking a similar review of further improvements that could be made to PIPEDA, and if so, what's the status of that review?

Ms. Krista Campbell: We haven't launched a formal review of the act at this point. It recently went under its five-year review. The changes have been implemented, getting the act updated. The data breach reporting regulations are clearly a priority.

I would suggest at this point that work going on along two parallel tracks is really important. Let the act have a bit of breathing time so we can see how these new tools and commitments work themselves out. Businesses need to get comfortable with them. We need to figure out if there are gaps in understanding how the new provisions work with technology as it continues to evolve.

Mr. Nathaniel Erskine-Smith: Do you mean specific to the mandatory breach?

Ms. Krista Campbell: I mean mandatory data breach reporting, the compliance regime, the compliance agreements that the Office of the Privacy Commissioner can enter into, fine tuning for consent. For example, the idea that if you're selling to children or providing a service such as an app or a game to children and you need consent from them, you should be using language that's appropriate for a child, so they could understand what you're asking of them.

Those changes were important in strengthening PIPEDA, and we need to have some experience in seeing how they work.

We have work that will go on in a more formal way as we understand what the EU wants to discuss with us. Do we need a more formal research agenda? And we have the work that's going on with the Privacy Commissioner around things like consent, data, big data, analytics, the Internet of things; how all those kinds of pressures will change privacy and the perception of privacy.

Mr. Nathaniel Erskine-Smith: With respect to harmonization and a question from my colleague Mr. Saini, with respect to the adequacy review, you listed a number of considerations: PIPEDA, the Privacy Act, Bill C-51, provincial privacy laws. Has your department identified any areas of concern?

Ms. Krista Campbell: At this point, it's not so much areas of concern as trying to understand where the EU would like to focus what it's doing. I think the European Commission and the EU rules definitely take a very citizen-oriented approach to data protection. It is very clear that with thoughts about a more "opt-in" regime, they are handing a significant amount of power to the individual to control their data and to understand where it's going. It is different from PIPEDA. In the past, we have had very good discussions around the privacy regime related to PIPEDA. It has been reviewed more than once by the European Commission and has been found to be a strong regime.

For us, as we continue to work in some of our international fora—I would point to two that are particularly important—we'll be able to evaluate how PIPEDA is standing up internationally. Also, on two of the important fora, the OECD, the Organisation for Economic Co-operation and Development, has very important guidelines that they've put out on privacy and digital security, which were recently reviewed and updated.

Canada was the lead on the subcommittee that resulted in these updated guidelines being put out. One of the purposes of the guidelines is to say that we want to understand how to make privacy regimes interoperable, because if the data can't flow across borders and is kind of landlocked, it's not very useful. Effectively, we want to prevent non-tariff barriers being imposed on this very important economic driver.

● (1625)

Mr. Nathaniel Erskine-Smith: On that point of harmonization and improving our privacy protections, you mentioned a citizen-oriented privacy model. The Privacy Commissioner was before us and spoke about consent and how the consent model is under attack. I have just a couple of examples.

A majority of Canadians apparently don't read privacy policies on mobile apps, yet in the Privacy Commissioner's Internet of things analysis, there's an estimate of 50 billion connected devices by 2020. In the department's view, is the consent model under PIPEDA something that you are looking to improve?

Ms. Krista Campbell: I think that understanding the consent model will be absolutely fundamental to ensuring that PIPEDA stays relevant and current.

As for what that means in terms of whether it's changes to the act or work that the Office of the Privacy Commissioner could be doing, for example, are there new tools or ways of going about doing business that could educate businesses more? Are we doing enough to help businesses understand this concept of "privacy by design"? That is, if they incorporate privacy aspects earlier, which could include things like simplifying the consent provisions.... I believe the Privacy Commissioner has spoken of things such as trustmarks, so that you understand what it is you're signing up for and so you don't have to read something and scroll through screen after screen every time.

I think there's a range of tools that would definitely need to be considered.

Mr. Nathaniel Erskine-Smith: Yes. We had an interesting witness before us who recommended a model code that would allow us to shorten privacy policies and would require express consent if there were deviation from that model code.

In regard to another recommendation, a 2014 study noted that 24% of grade 4 students and over 50% of grade 7 students had their own cellphones, which suggests that consent from parents ought to perhaps be obtained.

Also, with respect to the right of erasure, which I think my colleague Mr. Jeneroux mentioned briefly, it's noted that over 60% of 13- to 17-year-olds have at least one profile on social networking sites. Is this something that we're taking a serious look at in our policies, especially in light of the EU review?

Ms. Krista Campbell: Yes, I would absolutely agree that consent is one of the core areas and needs to be given considerable review, but I wouldn't want to leave the impression that the piece of legislation we're working with currently or the tools that exist are insufficient. I think one of the strengths of PIPEDA is just the idea that it's principles based and technology agnostic, technology neutral. For these principles around consent, accountability, transparency, the limited use of collection, storage requirements, and all of those kinds of things, we need to continuously stress-test them as the technology evolves.

You're very right. The Internet of things, with its billions of connected devices—and with the devices talking to other devices, not devices talking to a person and getting consent from a person—will change the landscape. We need to continuously think through what that means, but I wouldn't want to leave the impression that we don't have a robust regime that doesn't evolve with the technology.

Mr. Nathaniel Erskine-Smith: I've run out time, but I would encourage you to be proactive rather than reactive with respect to the EU.

Thanks very much.

The Chair: We will now move to the five-minute rounds, starting with Mr. Kelly, please.

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

I'd like to talk a bit more about administrative monetary penalties, and I'll begin with you, Ms. Palumbo. You have spoken a bit about this, and you've characterized them as being very effective, particularly your consent order model, which I'm maybe going to get to later.

First of all, I'll let you comment further about the effectiveness in general, but I also would like to know where these funds are paid. You mentioned punitive fines. You mentioned restitution. Would you recommend in the case of the Privacy Act or PIPEDA that they be paid to the commissioner's office, to the Receiver General, or to the affected parties? Where should the money go? Where does it go in your case?

● (1630)

Ms. Josephine Palumbo: As I said in my opening remarks, administrative monetary penalties are there to promote compliance with the law, to act as a disincentive to targets of our investigations, and to not continue to violate our legislation.

Where do they go? They're not punitive; they are remedial. They're not punishment, and in fact, our act expressly says that. Determination of an administrative monetary penalty is not with a view to punish. That's one thing I'd like to clarify. They are a debt owed to the crown, so they are payable to the Receiver General for Canada, and fall within the consolidated revenue fund. They contribute to government as a whole, and those funds are then further distributed to benefit programs and initiatives for the benefit of all Canadians.

I'm hoping that's sufficient for you. Again, I'd like to emphasize they're not punitive in nature; they're remedial. They're there to promote compliance with our law.

Mr. Pat Kelly: Right, however, when there is non-compliance, that might be thought of as a failure to deter.

Ms. Josephine Palumbo: On that point, if you look at our track record on consent agreements, which become court orders, they have been respected. We have only one case on record, the Matthew Hovila case, where we had a subsequent breach of a consent order, but that's a rarity. They actually have a very positive effect, in terms of disciplining the industries within which we are engaged.

You see that in the two examples I provided to the committee today. Avis Budget and Hertz were in the same industry, and administrative monetary penalties were obtained in both of those cases. With respect to Hertz and Dollar Thrifty, the commissioner was not on a formal inquiry when that resolution was reached, and it was subsequent to the Avis Budget resolution.

Mr. Pat Kelly: I did hear you say that the consent order does work very well, and you said that industry likes that model, if I understood correctly. The consent order model, from time to time, comes under criticism in other tribunals and other regulatory bodies wherein an accused party may, for the reasons you mentioned that people like the consent model—the reduced cost, the expediency of the thing...Yet, small operators that can't match the crown's resources may indeed opt to go into a consent order when they feel they have not broken the law or contravened any act.

Have there ever been any criticisms around any of your consent orders, or perhaps where people were pushed into a consent order they may not have really wanted to participate in?

Ms. Josephine Palumbo: Consent agreements—they become orders of the tribunal—are negotiated settlements between the commissioner and the targets of our investigations. We assess the evidence in each case, and within the Competition Act we have criminal and civil provisions. For example, where we have conduct that suggests a knowing or reckless behaviour, then in that context, we will refer the matter over to the Public Prosecution Service of Canada for criminal prosecution.

Where we see the evidence before us is of the nature that can be resolved through a consensual process, through a consent agreement, which is registered, which entrenches a court order before the tribunal or the courts, we will endeavour to do that. In fact, our preference is to utilize alternative case resolution to the maximum extent possible before engaging in full-blown litigation, whether it's within civil contexts or the criminal courts.

● (1635)

The Chair: Thank you.

Mr. Ehsassi, for five minutes.

Mr. Ali Ehsassi (Willowdale, Lib.): Thank you very much.

The first question I have has to do with the issue of AMPs. As you know, the Privacy Commissioner has brought up the prospect of improving our legislation to have AMPs. Would you have any guidance for him? Should that be an issue to be examined closely?

Ms. Krista Campbell: I think there's a lot of discussion around whether or not the Office of the Privacy Commissioner has enough tools in his tool kit to do his job effectively. I think any eventual next review of PIPEDA should focus on that question about the mandate and structure of the Office of the Privacy Commissioner and whether or not the tools align well, looking at what other jurisdictions do. In many jurisdictions they do have AMPs.

I think we have a regime currently based on an ombudsman model, with a very collaborative approach where we're trying to get to a good outcome through education, negotiation, and discussion. It's very useful for creating an environment where businesses are able to test out new products and services, try to be innovative, and offer to Canadian consumers what it is they want. We want to maintain that kind of very innovative, open, inclusive kind of regime where innovation is enabled and allowed.

I'm not going to come down on a yes or a no on this one, but I would suggest that the formal review take a really good look at the nature of the concerns that are being raised and whether or not AMPs are the right mechanism at the end of the day, because it is a fairly heavy stick to be given to an office of Parliament to use. It's a balancing question, whether or not this is an effective mechanism and do we have a big enough issue that we need to apply that type of new tool to the problem, if there's a problem, and what the nature of the problem is.

Ms. Josephine Palumbo: In my context I can't comment on the appropriateness of the power for the Office of the Privacy Commissioner, but I can certainly say that within the Competition Bureau framework the administrative monetary penalty regime is working quite well. It is effective at achieving compliance with the law and in garnering results for Canadians, and avoiding lengthy and costly litigation that is associated with litigating a case.

Of course, when we're before the tribunal or the courts, and when we're assessing the quantum of an AMP, we're taking into consideration a number of aggravating and mitigating factors, which I think I outlined in my opening remarks. These would be taken into consideration in terms of what the right number is in a particular case.

Within our context, the administrative monetary regime is quite effective.

Mr. Steven Harroun: At the CRTC, I would suggest that the AMP framework that we have as part of our enforcement suite of tools has been very effective and includes education and outreach, which I think is very important as well. I think it has been really essential in ensuring compliance and encouraging parties to actively participate in an investigation or looking into their activities. I think the AMP tool definitely encourages that active participation, encourages those undertakings, and negotiates settlements so that everyone is playing along with the rules.

Mr. Ali Ehsassi: Since we are asking the CRTC questions now, I was wondering if you could perhaps comment on the Blackstone decision. You were commenting earlier to the question put to you by my colleague that it is a good idea to provide companies the opportunity to actually come before the commission to deal with questions of penalties and issues of that nature. In that particular case, first of all there was a huge delay, because I think it took two years before a decision was rendered. In addition to that, the far more important thing, the penalty was reduced by approximately 80%. I was wondering if you could comment on that.

Mr. Steven Harroun: I'll start and I'll let my legal counsel correct me.

The right for parties to have a recourse mechanism is extremely important. As the chief compliance and enforcement officer, I issue a notice of violation that determines the amount of the AMP that we deem is appropriate, given the circumstances. If there have been 100 violations or 100,000 violations, how participative the company has been...back to my “help negotiate with us.” In the particular Blackstone situation, we issued an AMP for a significant amount of money. The company at that time had not been very co-operative with our investigation. We issued a notice of violation for a significant amount of money.

Those in violation have 30 days to respond to the commission and say they would like to make a representation before the commission. They chose to activate that, and they said, “Okay, we have a whole bunch of additional information now and we're willing to provide some additional information to plead our case.” I think that recourse mechanism is important.

I think the Blackstone case is important in that it shows that the system works. I conduct my investigation, my team conducts their investigation with the information they have available to them, and I issue a judgment, if you will. If the party is not agreeable to that, they can choose to go to the commission and say, “Wait a minute, I don't think they included this information, I don't think they took this into consideration. Oh, we didn't have financial statements at the time but we have them now.” Whatever information they have, they can plead their case to the commission.

We've had cases where the commission has upheld the notice of violation and the amount that the CCO has issued, and there are cases like Blackstone, where they've reduced it. But it shows that the system works.

● (1640)

The Chair: Thank you very much.

We'll now go to Mr. Kelly, again, for five minutes.

Mr. Pat Kelly: I'm going to follow up now still on the topic of the administrative monetary penalties.

How does compliance work with entities—and maybe this is for the CRTC as well—where an entity, if it's an e-commerce scenario where it's operating through foreign servers, or non-Canadian corporations...? How do you pursue non-Canadians who have broken Canadian law in the provision of service to Canadians?

Mr. Morgan Currie (Associate Deputy Commissioner, Deceptive Marketing Practices Directorate, Competition Bureau): That's a particularly important question in relation to the criminal side of our law where some of the false and misleading representations are actually perpetuated from others outside of our country, specifically in relation to violations of our amendments as amended by CASL, and this is where our international coordination becomes very important.

We work actively with our counterparts in Europe, New Zealand, Australia, the United States, and others in order to attack different levels of communication and servers where this may occur. It can be difficult because sometimes the representations to the public disappear shortly after they're made. It is an ongoing challenge in the digital economy, particularly on the criminal side of our law.

Mr. Pat Kelly: Do you have anything to add?

Mr. Steven Harroun: I would echo my Competition Bureau colleague's remarks.

As I indicated earlier, we have a lot of memorandums of understanding with enforcement agencies around the world. We use those relationships to execute warrants and to gather information for us. That's very useful for us and we've done the same for them.

I think we mentioned in our opening remarks that we had an international takedown of what's called Dorkbot, and I can't wait until we get another one because I'm tired of talking about Dorkbot.

We use those international relationships and they use us as well with those memorandums of understanding to execute our duties.

Mr. Pat Kelly: Okay.

Are there entities whose business practices are nefarious by nature and who try to avoid jurisdiction by trying to avoid countries with which you have agreements? Is this something Canadians ought to be concerned with, or is that not a major concern?

Mr. Steven Harroun: Our ultimate goal at the CRTC is to protect Canadians. With people who are providing services or whatever, or contacting Canadians in any way, we enforce the legislation accordingly. Certainly, if anything, CASL does reveal those nefarious actors. It reveals the bad actors. Ninety-five per cent of the persons involved want to be compliant with the legislation. The bad actors will be the bad actors and the legislation reveals those to us through our investigations.

● (1645)

Mr. Pat Kelly: Shifting a bit here for Ms. Campbell, in designing the privacy protection legislation in the review of PIPEDA, would your recommendation be that we should make our priority compliance, or being congruent with our trading partners in our trade agreements, or should the priority be more to examine what we think would be the best benchmark for other countries to follow, perhaps? Where should the emphasis be on compatibility?

Ms. Krista Campbell: That's an interesting question.

I would say I think they have to go hand in hand because the idea of having a regime that is internationally interoperable is critically important. I think many jurisdictions are increasing their focus on privacy protection for data, because of the importance of data and what data can do to drive economic development, and what data can do to drive innovation. Best practices continue to bubble up to the surface in organizations like the OECD or APEC.

For Canada, if we think about where we want to be leaders in some of the digital economy, for example, ensuring that we offer a welcoming environment for organizations that want to set up data centres here, and the idea of applying best practices and having a model that is very usable for international businesses to say that, yes, Canada is a location of choice for data, we need to be leaders in how we think about it. But we can't make a regime that doesn't work internationally with the people we want to trade data with.

The Chair: That's great.

We'll now move to Mr. Long.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Chair, and my thanks to our presenters and your staff for helping you prepare. It's a fascinating topic we've been studying for quite a while now, and it seems as if the more we study it, the more questions we have.

I read an article the other day in *IT World Canada* entitled “Experts worry Canadian firms won't be ready for new European privacy rule”. This is about May 25, which is coming fast, 2018, and GDPR.

Ms. Campbell, do you feel that industry realizes the impact that GDPR will have on them if they are not ready?

Ms. Krista Campbell: I would say lots of businesses understand. The data-savvy businesses definitely are ready. We have regular conversations with business where they are coming in and asking us the status of our adequacy standing.

I would note that our adequacy standing does not change the date that the GDPR comes into force. Our status would only change as the result of an outcome of a review. That's why we've been trying to engage with the European Commission early. We want to ensure that we're able to determine the scope of this review. Businesses will need to ensure that they are proactive in thinking about their privacy regimes. Businesses need to stay on top of the changes happening internationally. Our adequacy status will still stand in May when this comes forward pending the review.

Mr. Wayne Long: I agree with my colleague Mr. Erskine-Smith that we need to be proactive instead of reactive.

I'm going to give you a quote from Ann Cavoukian, executive director of the Privacy and Big Data Institute at Ryerson University. She said that many firms think because the EU has ruled PIPEDA is adequate for complying with current European privacy regulations they are safe.

Can you comment on that?

Ms. Krista Campbell: I think it is probably true that we can't be complacent about what our privacy regime looks like. We know where the Europeans have gone is very citizen-oriented. It creates new rights for citizens. It creates new obligations for organizations that host data, collect data, and use data.

Our privacy regime needs to continue to evolve regardless of what the European Commission does, simply because the Internet of things is coming. Consent among children is a vital issue domestically as well as internationally. We need to make sure our regime is evolving because of changes in technology and the challenges we face—not just because the Europeans are doing it.

I completely take the point that we need to be proactive. We have been engaging the European Commission and saying we want to start this dialogue in advance of their launching a formal review process so we can help set the stage and get things started. We have told them that we don't want to wait for them to send us a letter to tell us to get going.

● (1650)

Mr. Wayne Long: Do you think there are any immediate measures we could take? What can we do?

Ms. Krista Campbell: For us as government, I would say we should take immediate measures to engage with the European Commission and get them started in thinking about Canada. We need to ensure that they fully understand what Canada's privacy regime looks like. I wouldn't say they have spent a significant amount of time reviewing our regime yet, so we need to showcase what we do really well.

As for reviews by PIPEDA, CASL, and SCISA, these reports that committees will put out will be critical. The work plan for the Office of the Privacy Commissioner is important, and it is important to work with businesses to encourage them to think about privacy early and often in the offerings they have.

Mr. Wayne Long: Mr. Harroun, a long line of my questioning has always been about children and PIPEDA and meaningful consent. I'll make a statement: I don't think we're doing enough to protect our children.

Can you give me some insight into what you think we could do with respect to meaningful consent and age?

Mr. Steven Harroun: It's an interesting question. I'm not sure I have a view. The consent models under the CASL legislative framework work well. The opt-in regime works well under CASL, as does the implied consent.

My colleague may have something to answer, but I really don't have a view.

Mr. Wayne Long: That's fine.

Ms. Palumbo, where do you feel the debate about privacy rights with respect to business and consumers is heading over the next few years?

Ms. Josephine Palumbo: Again, I am not here to speak about the collection of personal information and privacy rights. I am here to talk about the Competition Bureau: what we do and what our mandate requires us to do. We enforce our act. We detect, deter, and investigate false and misleading representations and deceptive marketing, which is an important area of focus for the bureau. We undertake civil and criminal investigations based on the evidence that we have before us.

Mr. Wayne Long: Mr. Currie, go ahead.

Mr. Morgan Currie: I just want to add one thing. There is a nexus between competition law and privacy interest that may actually lead us to collaborate with our partners at the OPC in the future, and that is where advertisers may mislead consumers in order to obtain personal information for the promotion of a product or business interest—what representations are being made to people so that they give up their information. That's where our investigation would kick in as well.

Ms. Josephine Palumbo: I'll just pick up on the question you asked about children. While the Competition Act doesn't carve out the subject of children per se, when we investigate, we are looking at conduct that is directed toward the public, and obviously children are part of the public. As well, when we are assessing the quantum of an administrative monetary penalty, we are looking at the class of persons who are affected by the conduct, the vulnerable class of persons. So if that's children, seniors, disabled people, etc., we are going to give that a significant importance. That's how we would address the concern with respect to children.

The Chair: Thank you very much.

Our last questioner, for three minutes, is from the New Democratic Party. Madame Trudel, do you have a few more questions?

[*Translation*]

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

Since I am the last speaker, I would like to thank the witnesses for all this very interesting and relevant information.

Mr. Harroun and Mr. Roussy, I will go back to what you said in your speech.

You mentioned the unsubscribe message. Could you elaborate on that? I wonder whether there is a specific procedure that companies must follow when someone wants to unsubscribe from their site. Some unsubscribe links require several steps to unsubscribe.

Have penalties already been imposed for failure to comply with the unsubscribe procedure?

Mr. Daniel Roussy: To put it directly, the unsubscribe process must be relatively simple. According to the CRTC regulations and the legislation, the unsubscribe link must be readily available to consumers when they want to unsubscribe from a given site.

In 2012, the CRTC issued an information bulletin advising companies of its general views on the matter. We told them that unsubscribing must not be complicated. Having to go through two or three steps to unsubscribe discourages people from doing so. I cannot be more specific because there are things going on, but I can tell you that many of our investigations address this particular point that you have raised.

Thank you for the question.

● (1655)

Ms. Karine Trudel: You say that there are a number of investigations. I think we have often heard that, once a penalty is imposed, the problem is solved. Have you had to intervene frequently and impose monetary penalties?

Mr. Daniel Roussy: A number of companies have already consulted us on obligations, particularly on the unsubscribe issue. They are serious companies that want to continue doing business in Canada and do it properly. As Mr. Harroun explained, the purpose of the legislation is to get people back on track.

Once there was an agreement on a certain amount, those companies redid their link. As far as I know, it works very well right now; it is a success. Our intervention on the amount was timely since the companies responded well. They carry on their business in compliance with the unsubscribe legislation.

Ms. Karine Trudel: Could some companies come to see you pre-emptively? Do they only react when complaints are filed?

Mr. Daniel Roussy: It is difficult to generalize. Clearly, we react when there are complaints, but some companies have come to us directly and said they had messed up. That usually happens at the same time. Complaints are received and the company reacts at the same time. Those things are corrected and there is a fairly good understanding.

We should not underestimate any of the industry's work to raise awareness either. I am talking about the information sessions held across Canada. Businesses are really interested in them. Those sessions help companies get a handle on their compliance obligations. So far, that has been working very well.

Ms. Karine Trudel: Thank you.

[*English*]

The Chair: Thank you, Madam Trudel.

That ends the formal rounds of questions.

We have a little bit of time left, and I have in the past offered members who haven't had an opportunity to ask questions the opportunity to do so.

I believe, Mr. Dubourg, you are going to take me up on that offer. If there's anybody else who wants to, by all means do.

[*Translation*]

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

I have two short questions.

First of all, I would like to begin by welcoming the witnesses who are here.

My question is for the CRTC. We know that the anti-spam legislation has had an impact on the Privacy Act. Could you tell me whether the anti-spam legislation has made things challenging for you?

Mr. Daniel Roussy: So far, our mandates are quite distinct when we think of what Industry Canada, the Competition Bureau and the Office of the Privacy Commissioner will do.

In terms of challenges, the anti-spam legislation allows the three organizations to work very well, and it allows us to compartmentalize investigations and problems at that level, whether with Mr. Therrien's office or the Competition Bureau. I myself have not seen any big problems so far, but I cannot speak for the Competition Bureau or the Office of the Privacy Commissioner.

● (1700)

Mr. Emmanuel Dubourg: Ms. Palumbo, what do you think about that at the Competition Bureau?

Ms. Josephine Palumbo: With respect to the national information sharing system between the three partner organizations, I would just like to say that the Bureau is starting its investigations and must maintain the confidentiality of those investigations.

[*English*]

Under the Competition Act we are obligated by law to maintain confidential our investigations under section 10. We also have our confidentiality provisions under section 29, which preclude us from sharing information.

However, as a result of CASL we are now mandated to work collaboratively and co-operatively with our three partners, with the CRTC, and with the Office of the Privacy Commissioner, and we do that. In 2013 we executed a memorandum of understanding between the three agencies in terms of our enforcement mandate. We collaborate in terms of information sharing, keeping in mind that we do have a regime that requires us in certain circumstances to maintain confidential our investigations and information.

That being said, obviously our law currently requires that we do share information. We are prepared to do that, and it falls within the mandate of the three agencies.

[*Translation*]

Mr. Emmanuel Dubourg: Thank you.

I have one last question for the CRTC officials

You said you were imposing a penalty that could range from $1 million to $10 million, I believe. Is that correct?

It seems to me that there is a discretionary aspect. As you said, section 20 of the anti-spam legislation deals with that, but I still think there is that discretion. It depends on the context and the extent. Are you relying on a percentage? Is the percentage of sales taken into account?

Mr. Daniel Roussy: Thank you for your question, Mr. Dubourg.

I would like to make a clarification. Penalties of up to $1 million apply to individuals. As far as companies are concerned, penalties can be as high as $10 million.

As far as penalties are concerned, there is no percentage. As I explained earlier, the legislation is quite specific about the recipe to follow and the indications to come up with a figure. In addition, there are a number of Federal Court decisions that have provided guidance on the amounts to be imposed. So it's not a matter of a percentage. There is some flexibility that allows us to do our work.

I would like to come back to the fact that an administrative monetary penalty is just one of many tools. It is used in combination with other tools. You see, for the system to work, a number of things must come together.

Mr. Emmanuel Dubourg: Along the lines of what Ms. Campbell said, the purpose of these penalties is to ensure that people or organizations comply with the legislation. They are not intended to be punitive.

Thank you.

[*English*]

The Chair: I would like to thank our witnesses for being here. We appreciate your advice and counsel. If there's any testimony, in hindsight, that you wish you had given, please make a submission to the clerk. These things often happen. I usually think of the best things that I should have said days after.

We're going to move in camera very shortly, and I'll ask anybody in the room who's not supposed to be here to please excuse themselves.

Colleagues, as we prepare to move in camera to discuss a bit of committee business, we do have some outstanding business that we should take care of publicly. With the changing of some of the committee's makeup, the committee finds itself in a situation where it only has one vice-chair. Normally, a committee has two vice-chairs. I would be looking for somebody to nominate our vice-chair, the vacant seat that was left by Mr. Blaikie when he left the committee.

Mr. Kelly, would you like to move a motion?

● (1705)

Mr. Pat Kelly: I move that Ms. Trudel be the vice-chair.

The Chair: Normally, we have 10-minute speeches from people seeking these positions, but we won't do that to Ms. Trudel today.

The motion is moved, and I'll turn it over to the clerk point.

[*Translation*]

The Clerk of the Committee (Mr. Hugues La Rue): Moved by Mr. Kelly that Ms. Trudel be elected second vice-chair of the committee.

Is it the pleasure of the committee to adopt the motion?

(Motion agreed to)

The Clerk of the Committee: Ms. Trudel is duly elected second vice-chair of the committee.

[*English*]

The Chair: Very good, Madame Trudel.

Unlike your predecessor, that was unanimous. I'm kidding, of course.

Madame Trudel.

[*Translation*]

Ms. Karine Trudel: I would like to thank Mr. Kelly for the nomination and for his wonderful remarks. Thank you very much.

I'm just passing through. By June, someone else might take my place.

Thank you for welcoming me. I will do my best to be a good vice-chair.

[*English*]

The Chair: Colleagues, I'll suspend the meeting for a moment and we'll move in camera.

[*Proceedings continue in camera*]