HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 072 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, September 26, 2017

Chair

Mr. Dan Ruimy

Standing Committee on Industry, Science and Technology

Tuesday, September 26, 2017

● (1100)

[*English*]

The Chair (Mr. Dan Ruimy (Pitt Meadows—Maple Ridge, Lib.)): Welcome, everybody. We have a full house today. It's exciting to see.

Welcome to meeting number 72 of the Standing Committee on Industry, Science and Technology. Pursuant to the order of reference of Wednesday, June 14, 2017, and section 65 of An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying Out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, this is a statutory review of the act. That's more than a mouthful.

Today, we have witnesses from the Department of Industry. With us is Mark Schaan, director general of the marketplace framework policy branch in the strategy and innovation policy sector, as well as Charles Taillefer, director of the privacy and data protection policy directorate in the digital transformation service sector.

We also have with us, from the Canadian Radio-television and Telecommunications Commission, Steven Harroun, chief compliance and enforcement officer; Neil Barratt, director, electronic commerce enforcement; and Kelly-Anne Smith, senior legal counsel.

We are going to get started. We have a busy meeting ahead of us.

We'll start with Mr. Schaan. You have 10 minutes to present to us. After the 10 minutes, we'll go to the CRTC.

[*Translation*]

Mr. Mark Schaan (Director General, Marketplace Framework Policy Branch, Strategy and Innovation Policy Sector, Department of Industry): First of all, I would like to thank you, Mr. Chair, and members of the committee for the invitation to appear before you this morning.

My name is Mark Schaan and I serve as director general of the marketplace framework policy branch in the strategic innovation and policy sector of Innovation, Science and Economic Development Canada.

While our sector broadly includes such policy areas as innovation, telecommunications, and trade, my branch specifically analyzes and proposes improvements for the role of marketplace frameworks in meeting the department's objectives. This includes analysis of corporate governance, bankruptcy and insolvency, competition, and intellectual property to support an efficient marketplace and innovation economy.

[*English*]

More recently, my branch was assigned responsibility for Canada's anti-spam legislation, CASL, and the Personal Information Protection and Electronic Documents Act, PIPEDA, which are key pieces of legislation that are part of a broader legal underpinning that provides a regulatory foundation for commerce, including electronic commerce. Both seek to promote commerce and innovation through facilitating trust and confidence in the digital marketplace.

I am here with Charles Taillefer, director of the privacy and data protection directorate within my branch. His team is responsible for providing policy advice, guidance, and support with respect to CASL.

CASL has its origins with the anti-spam action plan for Canada, which was launched in 2004 and established a private sector task force chaired by ISED. The task force was responsible for looking into the issue of unsolicited commercial email, or spam. By the end of 2004, spam accounted for 80% of all global email traffic. In that same year, the task force on spam held national consultations with stakeholders, and it issued a report in May 2005. In order to combat spam, the report recommended that specific legislation be created.

Canada's new anti-spam law was passed in December 2010. The law, as the chair has pointed out, does not have a short title. Its actual title is “An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying Out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act”.

Given the substantive changes represented within this new framework legislation, a transition period was built into the implementation of the act and, following a Governor in Council order, it entered into force on July 1, 2014.

● (1105)

[*Translation*]

CASL helps protect Canadians by encouraging the use of safe and secure electronic commerce to carry out commercial activities in the online marketplace.

CASL generally protects Canadians from spam and other electronic threats, while ensuring that businesses can continue to compete in the global marketplace.

The law prohibits: sending of commercial electronic messages without the recipient's consent; altering transmission data in an electronic message without express consent; installation of computer programs without the express consent of the owner of the computer system; using false or misleading representations online in the promotion of products or services; collecting personal information through the illegal access of a computer system; and collecting and using electronic addresses through computer programs, which is also known as electronic harvesting.

[*English*]

Responsibilities for meeting the objectives are shared by a number of federal organizations. ISED operates the national coordinating body for CASL, which is responsible for the policy oversight and coordination of the anti-spam initiative. This also includes monitoring the implementation of the legislation and assessing whether it's meeting its stated objectives.

In addition to the national coordinating body, there are three independent federal agencies responsible for enforcing the act. The Canadian Radio-television and Telecommunications Commission, the CRTC, of which we have representatives with us today, can issue administrative monetary penalties for violations of the anti-spam law. The Competition Bureau can seek administrative monetary penalties or criminal sanctions under the Competition Act. The Office of the Privacy Commissioner also has powers under the Personal Information Protection and Electronic Documents Act related to ensuring the privacy of personal information and handling breaches.

The office of consumer affairs, which is also part of ISED, has an important role to play in terms of information and outreach, as they manage the fightspam.gc.ca website in liaison with the three mentioned agencies and the national coordinating body.

Despite new e-communication filters and blockers, spam and malware remain a significant issue for electronic commerce, and a serious security threat. Spam, while being reduced from the level of 2004, still accounts for over 50% of global email traffic in 2017. Moreover, spam is used as a means to introduce malicious programs, such as ransomware, into computer systems of both consumers and businesses. For example, after the WannaCry ransomware attack, malicious spam rose by 17%.

The scope of the issue is global and requires coordinated international efforts, and our enforcement agencies participate in international forums to impose administrative monetary penalties and conclude investigations on an international scale.

CASL is a key element of the Canadian legal framework to support development of the digital economy. Its stated purpose is to promote the efficiency and adaptability of the Canadian economy by regulating commercial conduct that discourages the use of electronic means.

There is evidence that CASL is working. Since the law has been in force, the amount of spam sent from within Canada has been reduced by more than a third. CASL provides for a suite of enforcement tools, including a private right of action, to support anti-spam efforts. The private right of action was scheduled to come into force in July 2017, the same time as the scheduled statutory review under the act. Some Canadian representatives from industry, academia, and civil society had raised concerns over the scope of the private right of action under CASL. As noted in recent ISED consultations with stakeholders, there is a significant sentiment that some aspects of the law could be further clarified.

[*Translation*]

As all of you know, the coming into force date of the provisions was suspended on June 2, 2017, pending a legislative review by this committee. Legislation such as CASL is foundational to building trust in the digital economy and it is sound practice to review such rules on a regular basis to ensure that they respond effectively and adapt to new developments in this fast-evolving digital marketplace.

In today's markets, business success depends heavily on the flow and utilization of information, making information itself one of the primary raw materials of the modern economy. Consumers and businesses need to trust that this information is managed responsibly for the digital economy to flourish. That is why a balanced and efficient regulatory framework is key, and CASL is a central part of Canada's response to this challenge.

I would be happy to respond to any questions that you may have with respect to ISED's role in administering CASL. My colleagues from the CRTC are also here today and are best placed to respond to questions related to enforcement activities, including interpretation of CASL.

Thank you.

● (1110)

[*English*]

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

We're going to move directly to Steven Harroun from the CRTC. You have 10 minutes, sir.

Mr. Steven Harroun (Chief Compliance and Enforcement Officer, Canadian Radio-television and Telecommunications Commission): Good morning.

Thank you, Mr. Chair, for inviting us to appear before your committee to share the Canadian Radio-television and Telecommunications Commission's, the CRTC's, experience with Canada's anti-spam legislation, CASL.

With me today are my colleagues Kelly-Anne Smith, senior legal counsel, and Neil Barratt, the director of electronic commerce enforcement.

This is our first opportunity to discuss the act with you since its introduction, so I think it would be helpful to provide a high-level overview of our responsibilities under CASL.

[*Translation*]

The legislation gives the CRTC the authority to regulate certain forms of electronic contact to provide Canadians with a secure online environment, while ensuring that businesses can compete in the global marketplace.

[*English*]

The fundamental underlying principle is that activities can only be carried out with consent. CASL is an opt-in regime. This means that consent must be obtained before sending commercial electronic messages, altering transmission data, or installing software. Commercial electronic messages, whether email, text message, or other format, must contain an unsubscribe mechanism that is clearly and prominently set out and readily performed. This allows recipients to withdraw their consent if they no longer wish to receive messages. Messages must also identify the sender or the person on whose behalf the message is being sent and contain contact details such as an email address, mailing address, and website.

Our objective is to promote and ensure compliance with the act. During the past three years, the CRTC has made it a priority to offer information sessions across the country and publish guidance materials for businesses, consumers, and the legal community. For example, my staff and I delivered six information sessions last May in Toronto to more than 1,200 businesses. These presentations help to raise awareness among businesses of their responsibilities when marketing products and services to Canadians and allow us to share lessons learned from investigations. As we do in every seminar, I made it clear that the CRTC is available to offer advice and support to help businesses comply with the act.

We also promote CASL to Canadians through our website, interactions with consumer groups, and on the phone and by email with our client service specialists. Consumer alerts are published on our website to warn Canadians of non-compliant online practices so they are aware and report any suspected violations. We want Canadians to report violations, and they are doing so, in great numbers.

The CRTC acts on the complaints it receives and has a number of tools to bring individuals and businesses into compliance, including the issuance of notices of violation, with accompanying administrative monetary penalties.

We look at a variety of factors to determine what the appropriate enforcement action should be. Our compliance approach includes interventions ranging from education to enforcement.

Our options include a warning letter regarding a minor violation requiring corrective action. We can also issue a notice of violation. This enforcement measure often includes an administrative monetary penalty.

We also enter into undertakings with parties who voluntarily agree to come into compliance. This often means that the party implements a corporate compliance program to prevent future violations. It can also entail paying a specified amount, although this payment is not considered an administrative monetary penalty. This has been a particularly useful tool, as we have reached undertakings with several parties that co-operated with our investigations.

Depending on the nature of the violation, the CRTC can impose up to $1 million per violation in the case of an individual, and up to $10 million per violation in the case of other persons, for example, corporations. We also have the authority to seek a judicially pre-authorized warrant to enter a residence or business to verify compliance with the act or determine if a violation of the act has occurred.

The CRTC has had success enforcing the legislation in the short time that it has been in force. For instance, along with national and international partners, in December 2015 the CRTC took down a command-and-control server disseminating spam and malicious malware, located in Toronto, as part of a coordinated international effort. This disrupted one of the most widely distributed malware families, which had affected more than one million personal computers in over 190 countries.

● (1115)

[*Translation*]

Of course, in today's interconnected world, spam and other electronic threats are not confined to Canada. One of the tools Parliament provided the CRTC is the ability to share information and seek enforcement assistance from our international counterparts. To date, the CRTC has entered into agreements with enforcement agencies in the United States, the United Kingdom, Australia and New Zealand.

[*English*]

Internationally, we also co-operate with partners through the Unsolicited Communications Enforcement Network, or UCENet. The purpose of this network is to promote international spam enforcement co-operation and address related problems such as online fraud and deception, phishing, and the dissemination of viruses.

Through UCENet, the CRTC has signed a memorandum of understanding with 12 enforcement agencies from eight different countries. We share our knowledge and expertise through training programs and staff exchanges and inform each other of developments in our respective countries' laws.

Domestically, CASL allows us to share information and co-operate on investigations with our partner enforcement agencies, the Competition Bureau and the Office of the Privacy Commissioner. In 2013, the CRTC signed a memorandum of understanding with our partners to facilitate co-operation, coordination, and information sharing. However, there are limited tools within CASL to allow the CRTC to share information with other domestic law enforcement and cybersecurity partners.

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

Mr. Chair, I'm not suggesting that the act is perfect. I suspect that you will hear a lot of suggestions about what needs fixing from the various witnesses who will address the committee in the months ahead. The CRTC would welcome the opportunity to appear before your members again before you wrap up your review and begin writing your report. We will closely follow the proceedings and can provide feedback on the ideas you may hear and respond to any questions you may have about what will or will not work.

As you and the members of the committee are aware, legislation must be enforceable in order to be effective. As you conduct your review, it is important to keep in mind that CASL has been in force for a relatively short period of time and covers a broad range of activities. The activities and ensuing investigations under the act are complex, and we have yet to fully apply the legislation.

We now welcome any questions you may have.

The Chair: That's excellent. Thank you very much.

We're going to move to you, Mr. Longfield. You have seven minutes.

Mr. Lloyd Longfield (Guelph, Lib.): Thanks, Mr. Chair, and thanks, everybody, for starting the process for us and getting some information on the table.

I want to start with Mr. Schaan. We're talking about global rules and where Canada plays into global rules or how we participate in the development of global rules. A lot of the spam that we have in Canada, as you mentioned, comes from outside Canada. In studying this, how much of our study should include the global rules that are being developed?

Mr. Mark Schaan: Thank you for the question. I think there are two elements to that.

One is that CASL has been successful at reducing the amount of spam that originates from within Canada, and that's been quite helpful, but to your point, spam is very much an international domain, in that there are a number of other spam-producing entities that exist outside of our borders.

That's why the coordinated international efforts of our enforcement agencies participate in a whole series of international fora, such as the Messaging, Malware and Mobile Anti-Abuse Working Group and the Unsolicited Communications Enforcement Network, which my colleague has mentioned. I think those sorts of efforts have been able to ensure that we work in tandem with other international enforcement agencies to get at the real root of spam, because it is a coordinated effort across borders.

● (1120)

Mr. Lloyd Longfield: I should have mentioned, Mr. Chair, that I'd like to share some of my time with Mr. Jowhari.

I have another quick question for you, Mr. Harroun. I'm looking at the notices of violation and the limited tools we've been using. Are we seeing a trend since the legislation has been introduced? How does the curve look?

I was also surprised that you're still doing hearings. I was involved as the president of a chamber of commerce when this came forward in 2010. We did all kinds of hearings and had all the businesses working towards compliance. Is compliance still an issue?

There are two questions there.

Mr. Steven Harroun: I'll start with the 5,000 complaints a week to our spam reporting centre. I would suggest that compliance is still an issue.

Certainly compliance is key. I'm the chief compliance and enforcement officer. The compliance part of my title is critical to ensuring that businesses are aware of the rules, understand how they can comply with the rules, and understand what's necessary with respect to following the rules. Those education outreach sessions are extremely important.

The ones we did in the early days in 2014 when we were first getting off the ground and the ones we did a couple of months ago are very different. In the early days, we were talking about how you must have an “unsubscribe” and it must link to this, etc. Now, we're providing more guidance and interpretation on recent decisions and compliance programs.

Businesses, individuals, and the legal community are looking at our decisions, interpreting them, and saying, “Oh, I understand now what you mean when you say this”, or “I understand how you're applying this particular regulation.” We're trying to provide that clarity. It is an ongoing initiative. We will do it every year, I would suspect, because there are always people knocking at our door and saying that they need help to understand.

Mr. Lloyd Longfield: On the second part of the question, in terms of the tools that you've been using, there have been some recent decisions that have large dollar figures attached to them. We have pushed out the legislative piece and are using tools in the meantime until the legislative piece has been nailed down.

Mr. Steven Harroun: I'd like to think we have a great suite of tools. Certainly I know my colleagues at the Privacy Commissioner's office would say that having administrative monetary penalties is very useful. I know they're looking for it themselves. We have a broad range of tools to effectively ensure compliance now and, for enforcement purposes, in the future. The tools that the CRTC has been afforded are very useful. It's a broad range. It allows us lots of flexibility depending on the type of case, the magnitude of the case, or the nefarious activities involved.

Mr. Lloyd Longfield: Thank you.

Mr. Majid Jowhari (Richmond Hill, Lib.): Thank you, Lloyd.

Welcome.

I'm going to start with Mark.

In the interests of time—I have only about two and a half minutes—I have a quick question. As you know, the heart of what's in front of this committee has to do with the PRA and the fact that certain sections of the act, sections 47 to 51 and section 55, were actually suspended a month before it was supposed to go into effect.

In your statement, you also specifically said that the scope of the PRA under the CASL raised a lot of concerns, and that the suspension of those sections came from the ministry and the minister. Can you tell us, briefly, what those sections, specifically sections 47 to 51 and section 55, are all about, why the department and the minister felt they needed to be suspended, and what type of consultation you're looking for?

Thank you.

Mr. Mark Schaan: With respect to the private right of action, the number one concern that we heard from stakeholders across a wide variety of areas—academia, industry, and broader stakeholders—was that the private right of action upped their initial concerns around compliance. Because the PRA would introduce the possibility of significant monetary penalties and legal risk, absent clarity on exactly how to comply, and to ensure that they were able to pursue CASL in its fullest form, they would be subject to significant risk. Given that its suspension corresponded exactly with this review, it seemed timely to take on some of those concerns, and to have a full hearing about what the anxiety was, before proceeding on what we heard from many people was going to cause significant risk and anxiety within their daily operations.

CASL was always framed to have a coming into force of the regulations. The act was passed in 2010; the initial regulations came in during 2014, and the malware pieces for computers came in during 2015. PRA was to come in during 2017, and even with that long lead time there was considerable anxiety from a host of stakeholders that compliance was still unclear and that a lack of clarity on compliance meant a huge legal risk.

● (1125)

Mr. Majid Jowhari: Is it fair to say compliance is taking much longer than anticipated, despite the fact that we have a lot of good tools, etc., and that's one of the reasons we are pushing for more consultation time?

The Chair: You have about five seconds to answer that one.

Mr. Mark Schaan: Yes, I would say there are elements of CASL that stakeholders have told us need to be clarified to support increased compliance, and that has taken some effort.

Mr. Majid Jowhari: Thank you.

The Chair: Thank you very much.

We're going to move to Mr. Jeneroux.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, everybody, for being here today, and to your staff who, I'm sure, prepared a lot of the briefings here.

I want to jump into a bit of background, hopefully some context, that you can set for us, describing the step-by-step enforcement process once you've been made aware that there might be a violation. What triggers you to start the process, and where do you go from there?

Mr. Steven Harroun: I'll have my colleague, Neil Barratt, describe our investigative enforcement process.

Mr. Neil Barratt (Director, Electronic Commerce Enforcement, Canadian Radio-television and Telecommunications Commission): One of the things we have at our disposal is the spam reporting centre. Through the "fightspam" portal that Mark mentioned, Canadians can submit complaints of spam that they've received. They can also fill out a detailed form and provide us with additional information relating to the message and other information they may have available.

For us that is a huge resource in terms of information. To date, since coming into force, we have more than 1.1 million complaints in the SRC. That's our primary source of intelligence. Our intelligence analysts look through that information. They try to identify trends. They look, obviously, at high-volume complaints to see if there are relationships. They're trying to identify links between different messages and different sending campaigns. Based on that, they'll develop some material for my enforcement officers to look at. We'll review that with them to decide what the viable cases are. That's the main source. We also have other information that we look at. We work with private sector partners who run giant spam honeypots that can see a broader scope of what the issue looks like.

At the end of the day, however, it's a conversation of our enforcement officers with our intelligence analysts to look at cases that are likely to succeed, that will promote compliance, and cases that can provide guidance to businesses.

Mr. Matt Jeneroux: Let's say I find that I'm getting spam. I make a report to you guys. You guys then investigate that. What would you do to investigate it? Do I send you my email and you take that for what it is and shut it down?

Mr. Neil Barratt: It's important to note that the emails in the spam reporting centre are not validated. They may be a potential violation, but they may also be incorrectly identified as a violation. The first thing we do is try to validate the complaint, if that's the main basis for the investigation. Depending on the level of information we receive from the Canadian who submitted the email, we may return to them, collect further details, and take a witness statement, things of that nature.

More broadly, we also look at collecting information from the companies in question, from email service providers, from hosting companies, from domain registrars, and from a whole suite of the people who are involved in that email from the time it's sent to the time it's received. Obviously, depending on the type of case, we also want to discuss with that business and request information from them on how they maintain their email lists, how they ensure compliance, and how they ensure they're working from a consent-based list, actioning unsubscribes, and ensuring that all the different pieces of the legislation are respected.

Mr. Matt Jeneroux: So if it's an honest mistake by an organization sending it out, there's at least an investigation to tell them maybe they shouldn't do this. They can say, "Oh, our apologies. We won't do it again." Is that what happens?

Mr. Neil Barratt: The investigations vary widely in scope, in scale, and in complexity. Certainly it depends on the size and the sophistication of the business involved, and on the number of emails sent. All of those factors will play into the appropriate enforcement response. As Steven mentioned, one of the tools we have available is a warning letter to make clear where there are alleged violations and to provide a bit of guidance to companies to help them improve their practices.

● (1130)

Mr. Matt Jeneroux: Okay.

Have you noted any particular negative effects on specific industries, for example, the not-for-profit sector? Have there been higher levels of complaints against them?

Mr. Neil Barratt: In terms of the complaints we've received in the spam reporting centre, I can't say there's a clear trend out of those numbers. It really does touch a lot of different industries and businesses of all different sizes.

Mr. Matt Jeneroux: Do you have those kinds of numbers, by industry?

Mr. Neil Barratt: I'm not sure that's always obtainable based on the information that's filed with the complaint.

Mr. Matt Jeneroux: Okay.

I want to bring up some of the comments you made, Mr. Schaan. You said that the amount of spam sent from within Canada has been reduced more than a third. Can you provide a little bit of background on how you get to that number? I imagine we're probably.... We don't know what we don't know, in a lot of ways. If no one is reporting it, based on Mr. Barratt's comments, it seems that it would be difficult to ascertain how much is actually not being sent anymore.

Mr. Mark Schaan: We've relied on a number of third party reports to be able to get an assessment of the degree to which spam makes up the email flows of Canadians. We get it in two ways. One is the degree to which we can rely on the senders to understand their practices, for instance, working with folks on the "Canadian Digital Marketing Report" or others that tell us about senders as well as some information related to recipients.

One year after CASL's implementation, for instance, there was 29% less email in Canadians' inboxes, and a 37% reduction in spam originating from Canada. That came from an organization called Cloudmark, in a 2015 study.

We have data from CIRA and Ipsos that indicates that 84% of Canadians who knew about CASL took advantage of the coming into force to triage the emails coming into their inboxes. The spam reporting centre has received just over 1.1 million submissions. We're trying to triangulate multiple sources of data to be able to get at the issue.

On the sender side, Litmus and others have told us, for instance, that 49% said that CASL had no impact on their email marketing program; they were continuing to market through email because they felt they could be compliant. Twenty-three per cent said that CASL had minimal impact, so clearly there were some shifts. Twenty-seven per cent said that it had a significant or dramatic impact, which means that, potentially, they were significantly addressing their current practices.

The data is third party, and by and large, as we say, we try to get it from a number of sources, to really get at the root of the issue.

The Chair: Thank you very much.

We're going to move to Mr. Stetski. You have seven minutes, sir.

Mr. Wayne Stetski (Kootenay—Columbia, NDP): Thank you. It's good to join the committee today.

I also have with me Katrina Van Genderen, from the University of Toronto's women in House program, who is here shadowing me today.

My question will probably go to Mark. Back in 2009, Canada was ranked fifth in the world for spam-originating countries. Can you please tell us where we stand today? Has this legislation proven to make a difference nationally and internationally?

Mr. Mark Schaan: Canada is no longer in the top 10, and according to some sources, since CASL came into effect, it is no longer a top 20 spam-producing country.

Again, we have to triangulate lots of information to get at that, but by rankings, we're not in the top 10 and maybe not even in the top 20.

Mr. Wayne Stetski: Can that be attributed to the legislation?

Mr. Mark Schaan: Causality is always challenging in these situations, but I think the fact that we have a robust anti-spam legislation that has significant compliance requirements for all senders is a useful mechanism to be able to highlight that spam is important and that we want to cut it down. It's not directly attributable, but one can see that pre-CASL and post-CASL there has been significant progress.

Mr. Wayne Stetski: So much of the spam is still originating from other countries around the world. You did mention briefly working with other agencies to try to deal with that.

Has the Canadian government had much success in getting other countries to prosecute spam originators? I guess that's the way I'll put it. I would imagine that is not covered under this legislation but would have to be covered under legislation in their own country.

Do you need any additional tools to try to deal with that issue?

● (1135)

Mr. Mark Schaan: On international enforcement, we have had some success in the international space. I'll turn to my colleagues in a second and they can tell you their own success stories. The enforcement agencies that are empowered by CASL have the capacity to work in the international zone with their peers. That has included the taking down of a botnet server, which I'm sure the CRTC may want to suggest as their own victory, so I'll turn it over to my colleagues.

Mr. Steven Harroun: As I mentioned in my opening remarks, we were afforded by Parliament great information-sharing privileges with our international jurisdictions, which is fantastic. We've executed MOUs with various different countries. We are a member of UCENet, which we talked about. It is an international unsolicited communications network of enforcement agencies. That allows us to call on those specific agencies and countries whose spam legislation falls within...to execute warrants and get information for us. We do the same for them. It is a back and forth, so we're able to help them, and they are able to help us. I think that's probably been the most successful piece from an international perspective.

I think the committee is right in pointing out that it's domestic legislation for a global problem.

One of the things I mentioned in my opening remarks, since you're asking, is that I am required to collaborate and co-operate with my partners at the Privacy Commissioner and the Competition Bureau, but my domestic sharing is actually rather limited. It's difficult for me, within Canada, to actually share with my colleagues at the RCMP, Public Safety, or wherever to move forward on cases. I made a point of that in my opening remarks, so I'll make it again. That's probably where we find the biggest challenge. Internationally, I can share more easily than I can across the street with my RCMP colleagues.

Mr. Wayne Stetski: That's an area of potential improvement, from your perspective.

Mr. Steven Harroun: Absolutely, from an enforcement perspective.

Mr. Wayne Stetski: Since 2009, have any new electronic threats not covered by legislation developed? Are you able to describe these for the committee? It seems the world is changing so quickly, so I imagine the evolution of spam might be changing, as well. Is there a way to combat these, and is the legislation broad enough or flexible enough to adapt to any new threats or changes coming forward?

Mr. Steven Harroun: From an enforcement perspective, the act is written as technology neutral, which is helpful. We are certainly seeing different types of spam. You're right. I think it's moving faster than we can keep up.

I have a team of technical experts and forensic analysts who are constantly challenged by the next thing. As soon as we think we understand one form of spam or one form of malware, we are challenged by yet another new form.

We can ponder this when we return perhaps, but at this time, I would suggest that the way the act is written—it's technology neutral—we have the flexibility to move. I would argue that trying to keep pace is our challenge. It's not the act.

Mr. Wayne Stetski: How many investigations have taken place since 2014, and out of those, how many charges have been laid resulting in fines? Do you have that information?

Mr. Neil Barratt: We've conducted several investigations, more than 30.

Investigations aren't always closed the moment a warning letter or a notice of violation is issued. A big part of our job is ensuring that companies remain in compliance after they've been the subject of an investigation. For instance, we have several investigations where, after we issue a warning letter, we'll do some follow-up to ensure compliance is achieved and monitor their activities, check in on their compliance programs.

I believe that, to date, we've issued about a half a dozen notices of violation. We've issued more than 10 warning letters and several other kinds of enforcement actions. Undertakings, especially, are quite helpful. We have the ability to engage in a negotiated discussion with the subject of an investigation when it wishes to voluntarily come into compliance. That's a particularly effective tool for us. We can negotiate the terms with the party involved and ensure part of that includes a robust compliance program going forward.

Mr. Wayne Stetski: Do they ever become criminal investigations? At such a point, would they get turned over to the RCMP?

Mr. Neil Barratt: When we learn of information, when we receive information in the spam recording centre that relates to a criminal violation, we share it with the RCMP. Our colleagues at the bureau have the ability to pursue violations, either civilly or criminally. They would be the best people to talk to about that.

● (1140)

The Chair: Thank you very much.

We're going to move to Mr. Sheehan. You have seven minutes.

Mr. Terry Sheehan (Sault Ste. Marie, Lib.): Thank you very much to our presenters. That was very informative.

Way back in the day, about 20 years ago, I worked with the first commerce-enabled website in northern Ontario. What a difference a day makes, though, in this particular business.

In preparing for today I was thinking about the different places we have been to since I started around 1997. We used to employ methods, instead of interruption marketing, in permission marketing, trying to get people's emails by various means, whether it was by offering some sort of product or service in return for that email. It was really thought out. It was explained really well to the person in order to get that particular email and any other information that we wanted. We employed that for a very long time.

The reason the spam legislation came along in 2004 is that no one was asking for permission. There were very different methods of grabbing those emails, just pounding people with messaging. Sometimes they would have detrimental results as they were trying to put in the malware, and various things. I applaud the efforts of the government in trying to deal with that. Recollecting as I go down that timeline, in 2004 there was something else that was launched, not only this task force, but of course Facebook.

To begin my line of questioning, in your opinion, how well has this particular piece of legislation, which was introduced recently, been able to keep up with the new tactics people are employing to pilfer emails? What's the success rate?

I understand, through the testimony, that the efforts here in Canada have been great. I've read the story about what happened in Toronto. It was wonderful. But a lot of the complaints are international. I know we have some particular agreements with international countries, but there are countries that are in the news all the time that.... How can we deal with those particular countries, going forward?

Mr. Mark Schaan: I'll start, and then I'll turn it over to my colleagues from the CRTC.

To the point that was made earlier, in general, because the law was framed as technology neutral, by and large it has been able to keep up. I think our own sophisticated understanding of the tools and techniques that are being used by entities requires quite a bit of constant study and work on our part, but the law itself has generally been able to continue to allow for enforcement to be carried out.

I would say, with respect to the notion of consent, that even the Privacy Commissioner in his own report just last week indicated that obtaining meaningful consent has become increasingly challenging in the digital age, where data is ubiquitous, commodified, and maybe processed by multiple players, totally unbeknownst to the individual to whom the data belongs. I think that is something that we continue to examine and analyze and understand. It's something that is changing, as we say. Your point about 2004.... It allowed people to share both very personal information about themselves as well as pictures of their dinners, but also created quite an interesting conceptual issue around consent.

I think from a legal perspective, by and large, we've been relatively successful in keeping up with the technological advancements.

With regard to enforcement, I'll turn to my colleagues.

Mr. Steven Harroun: I'll build on what Mark has been saying.

From an enforcement perspective, the opt-in regime is actually very helpful, because we are able to understand very clearly if someone has given their permission to receive information or emails, etc. That's a very helpful piece.

On the international front, I stand by the fact that we are very active in the international sphere. For example, I've mentioned UCENet, which is an international network of enforcement agencies. Just last year, we held a workshop with the International Institute of Communications on nuisance communications. The importance of that venue was that they are the policy folks, and there are people and countries involved in the IIC who had never met the enforcement side of the piece. We brought those two sides of the puzzle together at a workshop to look at the varying ranges of legislation available to these countries, so that the developed and the developing countries could exchange with each other their lessons learned. We can learn from the enforcement side of the house about what works and what doesn't. If you're about to institute legislation, how can that help?

We at the CRTC took it upon ourselves to sponsor this workshop and bring those two worlds together, and we'll be doing a follow-up actually, later in October, to discuss the next steps, how we can get everybody on the same page moving forward, and who can pick up the ball on particular pieces to ensure that we keep furthering the elimination of nuisance communications to everyone around the world.

It's ironic that you say you get calls from everywhere else. I know we've cited good stats. We still get calls from international partners asking us to help them against the servers in Canada. It's interesting. They see it from the other side of the fence. Across the pond, they say it's over there in Canada. They're the ones doing the spamming. They may not be spamming Canadians, but they're spamming someone else around the world.

● (1145)

Mr. Terry Sheehan: Is there an international agreement that most countries belong to, or should there be?

Mr. Steven Harroun: I would say no. I definitely think UCENet as an enforcement network is very helpful, and Mark had mentioned the M3AAWG and malware analysis group, which also includes countries from around the world.

There is certainly no one central point and that is why we, as the CRTC, branched out to get the policy folks in. Now we've included the IIC. There are certainly other fora, for sure, in which we could participate. The challenge, of course, internationally is that the legislation differs in different countries. The commitment by certain countries is different from what we would suggest. We have a strong commitment here in Canada. There may not be the same level of value in other countries. So one-stop shopping is probably not the way to go. I think it would be challenging, and we might never get anything done because no one would agree.

Mr. Terry Sheehan: Thank you very much. That's very informative.

The Chair: You're bang on for timing.

We are now going to go to Mr. Eglinski. You have five minutes.

Mr. Jim Eglinski (Yellowhead, CPC): My first round of questions goes to Mr. Harroun.

I notice in your report that you say the CRTC has entered into agreements with enforcement agencies in the United States, the United Kingdom, Australia, and New Zealand. Then two paragraphs down—I'm a little confused—you say the CRTC has signed memorandums of understanding with 12 enforcement agencies from eight different countries.

Is this a different set of parameters than the first set of parameters? Can you clarify that for us, please?

Mr. Steven Harroun: Absolutely, and I apologize if there was any confusion.

Our memorandums of understanding with Australia, the U.S., and New Zealand are with the government departments responsible for spam legislation. The 12 enforcement agencies in the nine different countries are the enforcement side of the house, so more the RCMP or public safety kind of officials in the UCENet space. They are two different organizations, two different sides of the house, if you will, referring back to my policy side versus enforcement side.

Mr. Jim Eglinski: What kind of teeth does that have with the other countries? Do you have good working relations? Are other countries positive in getting back and working both ways?

Mr. Steven Harroun: Absolutely. I would suggest the MOUs are drafted in such a way that we can share. From a very simplistic perspective, we help them and they help us. We get calls, I won't say every week, but definitely every month. We are probably more in contact with our colleagues in the FCC and the FTC than other countries. We receive requests all the time for assistance.

Mr. Jim Eglinski: I have a question for Neil.

Neil, you stated something about doing 30 active investigations, and there are no monetary penalties when someone asks that question here. At some other committees I've been on, where I've asked questions about enforcement policies by different directives, I've heard about directives where they'd rather negotiate, work with the client, educate the client, and hopefully get the client compliant.

Do you have a similar policy? You definitely didn't include any monetary actions taken.

Mr. Neil Barratt: Just to clarify, we do have the ability to impose administrative monetary penalties, and we have on several occasions.

Overall, we have a broad suite of tools. In each case it's dependent on the facts of that investigation and our assessment of what the best outcome is to produce compliance. In some cases that is a negotiated agreement with the party, where it voluntarily agrees to come into compliance, and sometimes it pays a prescribed amount as part of that agreement. In other cases, parties might not be willing to negotiate with us, and in such a case we might pursue a notice of violation, including an administrative monetary penalty.

Mr. Jim Eglinski: So you have had several monetary penalties imposed?

Mr. Neil Barratt: Yes.

● (1150)

Mr. Jim Eglinski: Okay, thank you.

I have a further question. It deals with the section on the private right of action. It has been suspended. Is that correct?

Mr. Neil Barratt: That's correct.

Mr. Jim Eglinski: How is our portion—it's not there right now; it's suspended—working or comparing in relation to our partners', say, the U.S., Australia, New Zealand? Do they have legislation in there for private parties to proceed?

Mr. Mark Schaan: I'll ask my colleague to chime in on that one.

Mr. Charles Taillefer (Director, Privacy and Data Protection Policy Directorate, Digital Transformation Service Sector, Department of Industry): Yes. For example, the U.S. has a private right of action, but it's only available to Internet service providers, not individuals. There are other jurisdictions. Australia and New Zealand have similar private rights of action, but for example, Australia talks about application for compensation and civil liability events. So there are similar provisions in allied countries, basically. The U.K. has similar provisions as well.

To what extent they mirror exactly the provisions of the Canadian legislation, I would have to....

Mr. Jim Eglinski: Thank you.

I have about 30 seconds left, and I have another quick question.

You mentioned that you have done study sessions in Toronto. Everybody talks to us about Toronto. I'm worried about the rest of Canada. Toronto can be on its own. What have you done?

Mr. Steven Harroun: Absolutely. I was going to say I could pull out a list, but even just last year we travelled from P.E.I. to Victoria. We do this across the country.

Mr. Jim Eglinski: Thank you.

The Chair: Excellent. Thank you very much.

We're going to move to Mr. Baylis. You have five minutes.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): It's nice again to see you, Mr. Schaan. I'm starting to see you an awful lot, so I assume you're an expert in a lot of fields.

When we look at spam, there's obviously the great work you're doing internationally and then there's work that's being done in Canada. I'm very happy to see the international work, but I also think we should always get our own house in order before we start getting things done internationally.

I want to focus this part on what we're doing in-house.

Mr. Schaan, you mentioned that the amount of spam within Canada has been reduced by 30%. Is that acceptable? I'm asking this to Mr. Schaan and Mr. Harroun. Is that what you would have liked to see, or would you have liked to see more? If you want to see more, what tools do you need to get more done within Canada?

Mr. Mark Schaan: With respect to the first question, as I said in my opening remarks, the origination for CASL in and of itself was Canada's appearance on the top five countries for origination of spam. As I said, we are now out of the top 10, so in terms of whether it was the result we were aiming for, I'd say that in general, it's a positive outcome as a whole. I think it's a double-edged sword or it's a two-headed challenge in some ways.

With respect to what we would like to see, I think the degree to which organizations in Canada have the capacity to understand and thereby comply with CASL should be at its maximum, to be able to ensure that no one is receiving a message that they haven't consented to, and that the expression of that consent was understood by both parties. To that degree—

Mr. Frank Baylis: What do we need to do to get there, though?

Mr. Mark Schaan: I think it's clarification around compliance. You'll hear from a number of witnesses over the course of this study about what that could or should look like. I think you'll hear from some who say, "It's pretty clear," and you'll hear from others who say, "No, we really need to have a much more refined understanding and prescriptive understanding of what consent would look like." I think that's a key element of the degree to which this is a successful piece of legislation. Insofar as people understand their obligations, they can then live up to them and consumers can then hold them to account.

Mr. Frank Baylis: With that statement, then, you're saying that a lot of it's not malicious. A lot of it is just that we still don't have enough education out there.

Mr. Mark Schaan: I think it's twofold, On the one hand, on the malware, ransomware, other sorts of factors, that's by its very nature malicious. It's intended to do bad things to your computer system and to do bad things to users. That's an international problem. I think we really are working in collaboration with other enforcement agencies to take down botnets and take down malware and ensure that we can take appropriate action.

The domestic side, though, is a lot about understanding what the law requires, and I think consumers in Canada get frustrated by both. One, they're a great risk, and the other, they're quite frustrated.

● (1155)

Mr. Frank Baylis: Mr. Harroun, I know you mentioned that it's complex, that we have yet to fully apply the legislation. Are you needing more resources to get that education out? What do you need to further move the ball down?

Mr. Steven Harroun: I'll touch on a couple of things that were in your previous question as well.

The most shocking thing I'll say at this committee is that CASL was never going to eliminate all spam. We might as well all understand that now.

Going back to your domestic and international perspective, most companies and individuals in Canada want to live up to their expectations with the government and the regulator. What CASL does is it puts everyone on the same level playing field. Everyone who wants to abide by the rules will follow the rules and they will not be spamming anyone anymore.

Going back to the sophistication side of the house, what happens there is that everyone who wants to abide by the rules abides by the rules; the more nefarious activities rise to the top. Cream rises to the top, and when everyone is following the rules, these guys rise to the top.

Going back to nefarious activities, our complaints are changing. We talk about 1.1 million complaints—

Mr. Frank Baylis: You're seeing a shift in the types of complaints.

Mr. Steven Harroun: Exactly, so the 1.1 million complaints are no longer.... Of course in 2014, day two, it was about a well-known Canadian national company that didn't have the right to email me. That is not happening today, which I think is the most important part to my colleague's statistics about the reduction of spam. The companies in Canada are complying, which I'd like to think is partly due to our education on compliance.

Mr. Frank Baylis: Do you have any percentages of how many were non-malicious to malicious? Is that changing? Do you have any numbers on that?

Mr. Steven Harroun: I don't have any numbers but I was just talking to my folks yesterday on what we are seeing. The sophistication is changing. It's no longer just about an “unsubscribe”, or it's no longer about their not having an existing business relationship with me. This is a very different activity. They want me to open up this particular attachment. They want me to do these particular things.

I don't have stats just because it's not really how we organize the spam reporting centre. It's a work in progress as well.

I'll go back to it being only three years since we've been in force. There are certain pieces of the legislation we haven't even applied yet because we haven't got to that more nefarious activity, because we've been busy getting everyone....

Mr. Frank Baylis: The low-hanging fruit....

Mr. Steven Harroun: Yes, exactly. It was not so much the low-hanging fruit; it was ensuring that everyone is complying.

The Chair: Thank you very much.

[*Translation*]

Mr. Bernier, you have five minutes.

Hon. Maxime Bernier (Beauce, CPC): Thank you very much.

My question is for officials from the CRTC or the Department of Industry. It pertains to compliance with the law.

Have you conducted a study or a cost analysis of compliance with the law for the private sector? How much might it cost a company to comply with this law? Does anyone know how much it costs?

Mr. Charles Taillefer: We have done some studies but we do not have exact figures. The amount depends on the organization and the computerized systems they had to implement to make compliance automatic.

We have received feedback from certain organizations which indicated that the initial costs of compliance with the law were quite high. We do not have any specific figures, however, since the cost varies from organization to organization and depending on how they communicate with their clients.

We have noticed that this created a need in industry. For example, certain companies offer automated compliance services. In this regard, there has been some innovation in order to facilitate compliance.

We do not have exact figures at this time but we could follow up on this.

Hon. Maxime Bernier: Do you know if the technology has evolved and if there is a program that consumers can use to block spam? Do you think the reduction of spam in Canada could be attributed to a new technology that consumers can use for that purpose? Does that have an impact on the reduction of spam in Canada?

● (1200)

Mr. Mark Schaan: I think that can be explained by two factors. First of all, spam has been reduced by the new technologies that consumers can use. Moreover, there has been a reduction in the number of emails from companies that have not obtained consumers' consent. I think both of these factors are at play.

Hon. Maxime Bernier: Thank you.

Mr. Chair, just over 48 hours ago, I tabled a motion that I would like the committee to consider at 12:30. It pertains to government consultations. You have received the motion. It pertains to the document entitled "Tax Planning Using Private Corporations", which is the proposal published by the Minister of Finance on July 18, 2017. The motion requests that "the committee hear from witnesses on this topic for 5 meetings", that public hearings be held on the impact of these changes on small and medium-sized businesses in Canada, "that the findings be reported to the House", and that "the government provide a response to the recommendations made by the committee".

I would like the committee to consider this immediately and for us to discuss it.

[*English*]

The Chair: If I understand correctly, you'd like to debate that when we go in camera at 12:30.

Hon. Maxime Bernier: I'd like to know if my colleagues are in agreement with debating that. Yes, it is important to have this debate as soon as possible.

The Chair: We have half an hour left for our witnesses. We have to establish the parameters of this study, so I would like to do that as well in this time frame, at 12:30. If the committee agrees, we can have that discussion at 12:30 when we go in camera.

Mr. Jeneroux.

Mr. Matt Jeneroux: Are we able to have that debate in public?

The Chair: The motion is valid.

Mr. Matt Jeneroux: I'm sure most Canadians would like to know—

The Chair: The motion is valid, so the choice is yours at this point. You may wish to debate that now, or you may wish to debate that at a future time. Again, we are scheduled at 12:30 to go in camera to discuss the parameters of this study. It's up to you, but the motion is valid.

Hon. Maxime Bernier: Yes, I understand that. Most important for me is that this debate be public. I don't think we have to do it at 12:30. Maybe we can schedule another meeting to have a public discussion about that motion.

The Chair: Mr. Longfield.

Mr. Lloyd Longfield: We could discuss the handling of this at 12:30 p.m. and figure it out. We have witnesses here from whom I'm dying to hear some more information.

The Chair: Okay, we will continue the interview with the witnesses, and then when we go in camera we can have a further discussion, if that's okay with you.

Hon. Maxime Bernier: Yes and no. I know that the witnesses are here, and it's very important to have the discussion.

Let's have further discussion, and we'll see when we discuss it. Maybe at 12:30 we have another agenda. Having the public discussion can be done at another time.

The Chair: Thank you.

If I understand correctly, we're going on to more questions.

Some hon. members: Agreed.

Hon. Maxime Bernier: Yes. It's okay from the standpoint of my time.

The Chair: We are moving, then, I believe, to Ms. Ng. You have five minutes.

Ms. Mary Ng (Markham—Thornhill, Lib.): Before we start, I also want to acknowledge a couple of wonderful students here from the University of Toronto who are shadowing us parliamentarians today.

With that, I'll begin.

You talked about the legislation being technology neutral so that it enables you to look at other forms of spam that are not just email. My question is, does the public know when they are getting a range of spam? I'm thinking about people in vulnerable communities, seniors, as an example. We are seeing a higher rate of usage and participation in social media such as Facebook by seniors. While enforcement allows technology neutral, is there a way for the public, particularly people such as seniors, to report and to understand even, that they can report and that this actually applies to them?

● (1205)

Mr. Steven Harroun: I'll start and then go to my colleague.

We talk about compliance and reach out to the business community and individuals to comply. Another side of what we do is ensuring that Canadians are aware of things that are happening.

We're very fortunate at the CRTC. As an independent agency, we're very active on Facebook and Twitter. We do lots of consumer alerts, if you will, along with my colleagues at the office of consumer affairs, to let Canadians know that this activity has happened, that this scam is out there.

We've all heard about the vacation scams and about the Microsoft scams for tech support, etc. We are very active in that space to let Canadians know: first, that this is what's happening; second, that this is what we've been investigating; and third, that if you have given us a complaint about a certain company, this is what has happened.

We try, then, to be active in the space to let Canadians know that they should be aware. Obviously, we can't solve all the problems of the world, but at least we can make awareness important. That's why in our social media space it's very important. As you say, it's no longer the tweens; it's everyone from 12 to 92.

Mr. Mark Schaan: I'll just quickly add—I'll give a shout-out for my colleagues at the office of consumer affairs—that the fightspam.gc.ca website has been a successful centralized point to receive consumer complaints as well as to provide information. They've received more than 1.1 million submissions.

Interestingly, the "unsubscribe" mechanism that's required in emails provides consumers with tools to control their commercial electronic messages, and 84% of Canadians, when surveyed by CIRA and Ipsos, said that they had used the opportunity of CASL to triage the emails coming into their inbox. For some that meant a hit of the unsubscribe button; for others it was, "No, I want to receive this and I'll continue to receive this communication."

Ms. Mary Ng: Thank you for that.

Here is my second question. While I know that this is the work of the committee that is proceeding, both of your organizations have had quite a lot of experience with and work with this piece of legislation. As we proceed as a committee with the study, is there any advice you can give us around witnesses we should be reaching out to listen to, witnesses who can give us a perspective and help us understand the efficacy of the legislation and where it's working, and where it's not? Whether they are consumers groups or whoever, do you have any advice for the committee, both of you, on those we might consider calling?

Mr. Mark Schaan: I might start by saying that there was a task force working group originally on the Task Force on Spam in 2005 that tried to have a wide reach to get at this issue. It included.... I'll just note that the co-chairs were Roger Tassé and Michael Geist, but the member organizations were a broad range that included the Coalition Against Unsolicited Commercial Email, Amazon, Bell Canada, the office of consumer affairs, the Privacy Commissioner, and PayPal. All of these I think indicate that there is wide interest in the legal, academic, consumer, and commercial zones that rely upon this legislation, all of which have views, certainly.

Ms. Mary Ng: Do I have more time?

The Chair: No, not any more. You used it right there. I'll take your extra 10 seconds and I will pass them on to Mr. Stetski.

Mr. Stetski, you have two minutes.

Mr. Wayne Stetski: This is particularly for the CRTC.

The legislation contained language that would repeal the do-not-call list in order to bring it under the Electronic Commerce Protection Act, the ECPA. Is this still in the works and if so, when would that actually take place? Is the do-not-call list still current? Can people still send in complaints on that legally? What's the whole status on the do-not-call list?

Mr. Steven Harroun: You are correct. The statute allows for the provision of that. It's never been exercised. The national do-not-call list is also something that falls under my purview at the CRTC. It is very active. Canadians still register their telephone numbers and it's definitely more mature. It's been in effect since 2008, so we're almost at our 10-year anniversary, but we are very active on pursuing those who violate the do-not-call list rules. It's working in its own regime, for sure.

There is a provision and I'm certain my legal counsel can talk about that. It's never been exercised. The regimes are very different, so I think that would be an interesting discussion.

● (1210)

Mr. Mark Schaan: Go ahead.

Mrs. Kelly-Anne Smith (Senior Legal Counsel, Canadian Radio-television and Telecommunications Commission): Okay.

The framework already exists within CASL to take out of the Telecommunications Act and all its regulations and decisions, the existing do-not-call and unsolicited telecommunications framework and to roll it into CASL. That could be done very easily by a GIC provision. There are really no changes that are required.

As my colleague suggested, the regimes are very different, since one is an opt in and one is an opt out. Before you did that, I would think that you would want to do a lot of consultation with the telemarketing community to see if they would be agreeable to that sort of provision.

I think that there would be a lot more additional authorities that would be available to the commission in order to deal with telemarketing regulations that do not exist in the Telecommunications Act. On that side, there would be pros and cons, but certainly, it should be done.

Mr. Mark Schaan: Super quickly and I know we're out of time. I just want to say that the original intent was an anticipation that voice-over Internet protocol calling would essentially replace telephone calls and that those would be considered electronic messages and therefore, come under CASL. That was the original intent for why the do-not-call suspension provisions are there.

The Chair: Thank you.

We actually have time for one round of five minutes each, so we are going to go to Mr. Jowhari. You have five minutes.

Mr. Majid Jowhari: I'm going to reframe my question one more time. Let me acknowledge that I understand that there is a scheduled review planned for July. I get that. I also understand that we suspended the PRA section and we combined the two.

In your statement, what you specifically said was that Canadian representatives from industry, academia, and civil society have raised concern over the scope of the PRA. As well you said, as noted in recent ISED consultation with stakeholders, there is a significant sentiment that some aspects of the law could be further clarified.

I have a two-part question. First, can you tell me what those top three concerns are? Second, can you tell me which aspect of the law you think needs further clarification? I believe those would be able to help us frame our discussion.

Mr. Mark Schaan: Yes, you're quite right.

The phasing was essentially as I indicated: the original regulations, then the malware regulations, then the PRA. I think the concern on the PRA is particularly related to the possibility of class action suits and legal liability that may arise from compliance. While a number of organizations and entities have attempted to be as compliant as possible, I think they fear that moving from a system, where potentially they're under a CRTC-type enforcement where there's an opportunity for a helpful exchange and maybe a warning letter, that it could move very quickly to a legal dispute, where potentially there may be a significant legal risk.

I think the zones where we hear the most concern is around this notion of consent. It gets at what the Privacy Commissioner indicated, which is that, in an electronic age, where potentially you're collecting a lot of different information for different purposes, what constitutes consent can be a challenge. Also, ensuring that when the consumer or the user has consented to the receipt of the electronic message, how explicit does that have to be to be able to send the messages? I think the concern about the PRA was that this would then become a litigious action that potentially raised a compliance risk and potential legal uncertainty.

Mr. Charles Taillefer: I want to add that what we've also heard is that the act provides for statutory damages. In terms of the actions that would be brought forward by individuals, there's compensation for actual harm done, but there's also prescribed statutory damages that can be awarded. That is based on.... Non-compliance, in and of itself, would be a factor in granting individuals compensation for that. What we heard from stakeholders is that was a particular concern in the context of the private right of action, specifically, where you didn't necessarily have to demonstrate harm, that statutory damages could be awarded simply for having received a commercial electronic message that you didn't consent to. For this you could be awarded compensation. That's what elevated that risk.

● (1215)

Mr. Majid Jowhari: Thank you.

I'm going to share the rest of the one and a half minutes.

Mr. Frank Baylis: I'd like to talk very quickly about resources. If you had to make the act better, you had mentioned, Mr. Harroun, domestic sharing, which is limited in the act. I'd like to know, if you had one thing to change in the act—very quickly as we don't have much time—what would you change? What would you change, Mr. Schaan?

Go ahead, Mr. Harroun.

Mr. Mark Schaan: I'll just say as a public servant, we don't have views on these sorts of issues. I think what we've heard from some stakeholders, and what ultimately led to the suspension of the PRA, is that we want the obligations in the act to be as clear as possible. Over the course of the testimony and this study, you'll likely hear about zones where people will want a greater degree of specificity.

Mr. Frank Baylis: Invest in clarifications of the act to help the people who want to comply comply.

Mr. Mark Schaan: I think we all want to make sure that the act is understood, yes.

Mr. Frank Baylis: You had mentioned sharing with domestic—

Mr. Steven Harroun: I think it's enhanced information sharing domestically.

Mr. Frank Baylis: Enhanced information sharing domestically and clarifications. Those would be the two main things we should focus on.

The Chair: Excellent. Thank you.

We're going to move to Mr. Jeneroux. You have five minutes.

Mr. Matt Jeneroux: Perfect. Thank you.

Yes, that was a very public service answer, Mr. Schaan. I appreciate it.

Voices: Oh, oh!

Mr. Matt Jeneroux: As you guys were speaking earlier, something tweaked in terms of what aspects of the act or compliance of the act Canadians are falling short of.

Is it failing to get consent initially? Is that the biggest problem? Is it the context of some of the correspondence? Is that it? What specifically is the biggest fail?

Mr. Steven Harroun: Just generally, I think the top two are consent, one, and identification of the sender.

Mr. Matt Jeneroux: Fair enough.

I'm going to share my time with these two guys.

Hon. Maxime Bernier: I just have one question. You told us about complaints that were coming from consumers. Did you receive any complaints about the emails that the politicians were sending to them? As you know, we're exempt under that legislation.

Mr. Steven Harroun: You are exempt under the legislation. There may be complaints in our spam reporting centre about that, but that goes back to validating the complaint, whether or not it's valid. We also get complaints about a not-for-profit charitable organization as well, which may also be exempt for certain reasons.

Hon. Maxime Bernier: Do you think we should be under the legislation as politicians?

Mr. Steven Harroun: From an enforcement perspective, I will enforce accordingly, and I'll leave it to my colleagues at the department.

Voices: Oh, oh!

Mr. Mark Schaan: From a policy perspective, as a public servant, I have no view.

Voices: Oh, oh!

Hon. Maxime Bernier: I like that. What I don't like is that politicians are not under the legislation. We are voting in legislation here, and we are sending emails to people, but it doesn't apply to us. I think that is not transparent. When we think about changes, we must think about that. We must have legislation that is in line for everybody or have no legislation at all. That's only my thinking about that. In politics, I try to fight for fairness, and I think that it is not fair that we are not under the legislation.

Mr. Mark Schaan: I'd have to go back to the original RIAS, but I think in the explanation for why the exemption was initially provided, the communications between politicians and their constituents were seen as vital and, therefore, not one to which one could consent because it was necessary for democracy. I think that was the original intent.

Mr. Steven Harroun: I would suggest, Mr. Bernier, that there is no reason why you and your colleagues cannot follow the rules of CASL, even though you don't fall under those rules.

Voices: Oh, oh!

Hon. Maxime Bernier: I like that. Yes, you're right.

● (1220)

Mr. Jim Eglinski: I have a question for Mr. Barratt. We're all clear that violations under Bill C-28 are not criminal offences. Have you had any problems with private hackers going into the system and spamming or using people's programs and so on to spam? Have you had any violations in that way, where you had to go...? I notice under the act that you can go to court and get an injunction to force a person. Have such things occurred?

Mr. Neil Barratt: It's definitely something we see. Network security is always evolving, and there are lots of institutions out there that aren't always on the cutting edge, or that through no fault of their own have some vulnerability in their system. We've definitely seen universities and other public institutions where somebody takes control of their email server and just shoots emails out, rapid fire, to everyone.

That's something we look at when we're investigating, to make sure of where the emails actually came from, that the institution was in fact the sender. Part of our job is to work with our partners and make sure institutions are aware when that happens, so that we can give them a bit of guidance or at least point them in the right direction in terms of how to secure their facilities and their infrastructure.

Mr. Jim Eglinski: Have there been any violations? Have you charged anybody? There's a pretty good penalty system that you have out there.

Mr. Neil Barratt: A lot of times in cases like that, the person who actually committed the violation is not going to be readily found or be within the area.

Mr. Jim Eglinski: All right, thank you.

The Chair: Thank you.

We're going to move to the final five minutes, for Mr. Stetski.

Mr. Wayne Stetski: Thank you. I want to go back to the do-not-call list for a minute. Do you think it's still desirable to bring the do-not-call list under the Electronic Commerce Protection Act?

Mr. Mark Schaan: Again I would say we're agnostic on that view. The original reason the do-not-call list had the capacity to be brought under CASL was that our view was that voice over Internet protocol, which would constitute an electronic message, would necessarily bring messages sent through VoIP under CASL. As we've seen, that hasn't necessarily come to be the case, so phone calls that are not electronic messages are still being received. Insofar as those continue, the do-not-call list provisions still apply.

Mr. Steven Harroun: From an enforcement perspective, we are enforcing the do-not-call list . It's a very mature program. It works very well. As my legal counsel pointed out, I have a broader suite of enforcement tools available to me under CASL, so that would be one of the advantages for sure. I really don't have a view as to whether it should or shouldn't. The two programs are very different and would require some study, I would suspect.

Mr. Wayne Stetski: I think Ms. Smith wants to jump in.

Mrs. Kelly-Anne Smith: Thank you.

I just want to add one thing, which is that the Telecommunications Act provisions permit the chief compliance and enforcement officer to have more flexibility, thanks to the tools he has at his disposal. He can have a staff member issue a request for information letter, and the party has to respond. They have no opportunity to appeal or any recourse.

CASL, and this is a good thing in some cases, has many different appeal mechanisms built into it, so that causes a lot of delay to investigations. We issue a preservation demand or a notice to produce, and the party has an opportunity to appeal to the commission, and then even to the Federal Court of Appeal. So although he has more powers at his disposal in CASL, the Telecommunications Act is more nimble and the investigations are less complex. For the most part, although they are becoming more complex with spoofing, the Telecommunications Act provisions work really well.

That's my comment. Thank you.

Mr. Wayne Stetski: Thank you.

I'd like to try to benefit my constituents as best I can with my last question.

A couple of years ago, there was a phone scam going around communities, where it was supposedly the CRA on the end of the line. You had two hours to write them a cheque or they'd be at your door arresting you. I contacted the RCMP and reported it as a spam and a scam, and they said there was really not much they could do about it because the source of the phone calls changed too quickly and they couldn't really track them.

What should people do if they get a phone call or a spam email? How should they deal with it, moving forward? Do you have that same problem trying to track down sources of spam that the RCMP said they had with phone calls?

Mr. Steven Harroun: Most definitely we have the same challenges. I like to think we do a good job at the commission and informing Canadians about those types of scams, phone calls, emails, etc. There is no easy answer. The easy answer is if you get a call or an email from your bank or CRA, or anyone you have a relationship with, if you feel remotely uncomfortable, ask to call them back. If you call back the legitimate phone number that you've found on a website or on the back of your bank card, etc., they will let you know if they were really trying to contact you or not.

We certainly work with a lot of legitimate companies that have been victims of these things, such as CRA. We work with our federal partners to make sure the message is out there that the CRA will never contact you that way, for example. The banks do a very good job. They even post on their websites that these are the current scams and they'll never contact you this way. Unfortunately, Canadians should just be on their guard a bit when they're giving personal information over the phone or via email.

● (1225)

Mr. Wayne Stetski: I just have a very quick comment.

I continually receive spam, but I don't think I've ever received an email advising on what we should do with spam, so I'm wondering about the educational role that you have. If you could send me and my constituents an email on how to deal with this, then we would not consider you to be spamming us.

Mr. Steven Harroun: I'll deem that as your consent.

Mr. Wayne Stetski: Yes, you could. Quite seriously, though, I continually get spam, but very little education on what to do with it.

The Chair: On that note, I'd like to thank all of our guests for coming in today. It's extremely valuable information, and it will really help us understand the direction in which we need to go.

I would also like to thank our vice-chair for being very cordial and allowing us to continue with our testimony.

We're going to take a break and then we'll go in camera.

I'm just curious. Out of the MPs here, how many have people shadowing them?

I'm going to ask a question because I'm not sure. Do you want to keep your shadows here for this portion?

We have shadows from the University of Toronto, but nobody else.

Hon. Maxime Bernier: That's all right.

The Chair: Are we all agreed that our shadows can stay? Thank you.

We're going to suspend for two minutes.

[*Proceedings continue in camera*]