HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 078 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, October 24, 2017

Chair

Mr. Dan Ruimy

Standing Committee on Industry, Science and Technology

Tuesday, October 24, 2017

● (1100)

[*English*]

The Chair (Mr. Dan Ruimy (Pitt Meadows—Maple Ridge, Lib.)): We have quorum, so we're going to move ahead, because we have two separate panels today.

Good morning, everybody, on this rainy, wet, lovely day in Ottawa, and welcome to meeting 78. We continue our review of the anti-spam legislation.

In the first panel, we have with us today, from the Office of the Privacy Commissioner of Canada, Daniel Therrien, Privacy Commissioner of Canada; Brent Homan, director general, Personal Information Protection and Electronics Documents Act investigations; and Regan Morris, legal counsel.

Gentlemen, you have eight minutes. Are you each talking or is it just one person?

Mr. Daniel Therrien (Privacy Commissioner of Canada, Office of the Privacy Commissioner of Canada): I'll make the preliminary remarks.

The Chair: Okay, go ahead, and then we'll get into questions.

[*Translation*]

Mr. Daniel Therrien: Thank you, Mr. Chair.

Thank you for inviting us, my colleagues and me, to appear before you today on your review of Canada's Anti-Spam Legislation.

We think this legislation has been positive in helping to fight spam and address certain online threats that can be harmful to Canadians.

As you know, responsibility for enforcing compliance with the legislation is assigned to three enforcement agencies: the CRTC, the Competition Bureau and the Office of the Privacy Commissioner of Canada.

For its part, the office is responsible for investigating address harvesting and spyware, both of which generally involve the collection and use of personal information without consent.

This responsibility forms an integral part of the office's broader mandate of the Personal Information Protection and Electronic Documents Act, or PIPEDA, in other words, the act respecting the protection of personal information in the private sector, which sets out rules governing the collection, use, and disclosure of personal information in the course of commercial activities.

Canada's Anti-Spam Legislation also empowers the three agencies to share information and collaborate in enforcing the law. We worked with our partners in applying this legislation. In particular, we have accessed and made use of the Spam Reporting Centre at the CRTC to help identify address harvesters or entities suspected of distributing spyware, which has resulted in two major investigations so far.

Our first investigation involved Compu-Finder, a Quebec-based training provider.

Compu-Finder used email addresses—some of which were collected via address harvesting software—to send out recurring email messages to individuals, many without adequate consent.

We collaborated and shared information with the CRTC. Our investigation served to enhance Compu-Finder's practices and provided guidance to businesses in general on responsible email marketing that respects people's information.

Most recently, we completed an investigation into a Canadian company called Wajam Internet Technologies, which distributed its program as an unsolicited add-on to free software. The program tracks a user's online search queries and integrates the results with content shared by an individual's contacts on social media networks.

Our investigation found that Wajam Internet Technologies was not obtaining meaningful consent to install the software and was preventing users from withdrawing consent by making it difficult to uninstall the software.

As a result of our investigation, the company stopped distributing the software in Canada, ceased collecting personal information from Canadians who had already installed the software, and agreed to destroy all Canadian user information in its possession.

By their nature, spyware and address harvesting pose dangerous threats and can be difficult for Canadians to detect.

These issues are not likely to be the subject of traditional consumer-driven complaints or that consumers will recognize them.

This is leading us to adopt a more proactive enforcement approach for Canada's Anti-Spam Legislation matters, including the greater use of commissioner-initiated investigations like the ones I have just described.

Our proactive efforts also include outreach, issuing education and guidance material for consumers and organizations on protecting their computers, and understanding spyware and ransomware.

Canada's Anti-Spam Legislation has also made amendments to PIPEDA, which have improved our compliance outcomes generally, in other words, the compliance of other provisions of the act respecting the protection of personal information in the private sector that go beyond the two behaviours set out in Canada's Anti-Spam Legislation. These were consequential powers associated with the adoption of Canada's Anti-Spam Legislation.

The ability to decline or discontinue complaints has taken us part of the way in allowing us to focus efforts on matters that present the greatest risk to Canadians.

That said, our enforcement resources remain taxed with a continuous high volume of complaints.

The ability to collaborate and share information with domestic and international counterparts—another consequential PIPEDA amendment—has had a profound effect on our office's capacity to deliver impactful enforcement outcomes across the globe.

● (1105)

Since those provisions came into effect in 2011, our office has participated in numerous collaborative and joint investigations, including our first joint investigation with our Dutch counterpart into WhatsApp in 2013, as well as last year's Ashley Madison investigation with our Australian equivalent and the U.S. Federal Trade Commission.

[*English*]

CASL has only been in place a short time, so we're still gaining experience, but from my perspective so far, the law has provided the OPC with useful additional tools. Nevertheless, I believe the following legislative changes to CASL would be worthy of consideration. There are three.

First, give the OPC more flexibility to share information with the CRTC and the Competition Bureau. At present, under sections 58 and 59, the three bodies can share information and use that information, but this is limited to specific CASL-related purposes as set out in those sections.

As noted previously, CASL also amended PIPEDA to give the OPC the ability to share information with domestic and international counterparts, but these provisions do not include the CRTC and the Competition Bureau. In past investigations under PIPEDA, outside of the context of CASL, issues have surfaced that overlap with the jurisdiction of the CRTC or the Competition Bureau, and in those instances we think it would have been very helpful to be able to share information and to collaborate with our colleagues. To address this, either PIPEDA or CASL could be amended to give the OPC more flexibility to share information with the CRTC and the Competition Bureau more broadly, to address matters that intersect between consumer and privacy protection.

The second amendment would be to clarify the conflict provision in CASL, section 2, which states that CASL takes precedence over PIPEDA in the case of a conflict. We would like a reformulation of section 2 to say that CASL can add to the provisions of PIPEDA, but does not lower those standards.

This is not an abstract concern, as we have already encountered one instance where the organization attempted to argue that it did not need to comply with PIPEDA because of an exception to CASL. I would refer the committee to our report of findings in Compu-Finder as an example of why this clarification is required.

Finally, we would suggest clarifying the spyware provision. This is subsection 7.1(3). As a result of CASL, PIPEDA removed the possibility of resorting to consent exceptions to justify the collection or use of personal information that has been made by accessing a computer system, or causing one to be accessed, in contravention of an act of Parliament. To further clarify this provision, we recommend that the reference in the provision to accessing a computer system "in contravention of an Act of Parliament" more explicitly include unauthorized installation of a computer program within the meaning of section 8 of CASL.

In conclusion, Mr. Chair, the OPC works diligently to educate individuals and organizations on the privacy implications of digital technologies, social trends, and business practices, and to enforce privacy protections. CASL enforcement is a key part of this suite of activities. While individuals should take steps to be aware of risks and to protect their personal information, it should not all rest on individuals. Organizations, too, must do their part.

Thank you. I will be pleased to try to answer your questions.

● (1110)

The Chair: Thank you very much.

Could I ask that you actually send that report for Compu-Finder to the clerk?

Mr. Daniel Therrien: This is public—

The Chair: Yes.

Mr. Daniel Therrien: We'll send it, but I believe it can be found as an annex to our latest annual report as well.

The Chair: Thank you. We'll now move to questions.

We'll start off with Mr. Jowhari. You have seven minutes.

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

Welcome to all of the witnesses. I'll start with Mr. Therrien.

In your testimony you specifically mentioned two objectives. Those are sharing information among the three agencies and also enforcing the laws.

On your recommendations specifically around sharing the information, in your handout you underlined "limited". You also said that CASL amended PIPEDA.

When you were doing the investigation, you talked about how the collaboration could have been better when it came to matters outside the context of CASL. Can you give us a specific example?

Mr. Daniel Therrien: Yes. The problem, again at the general level, pertains to the ability to share with our two sister organizations where the conduct that we're investigating goes beyond CASL, per se, but touches on our more general mandate, as in privacy protection, or competition more generally for the Competition Bureau. An example of where we faced the limit of the ability to share was in the case of Ashley Madison. It dealt with the obligation of organizations to properly secure the safety of information that clients gave to them. Because the sum total of the rules allow us to co-operate with various colleagues, we were able to share information with the U.S. FTC on that investigation, but not with the Competition Bureau.

Mr. Majid Jowhari: What would the impact of that be?

Mr. Daniel Therrien: There could be discussions between Canadian enforcement agencies as to, for instance, who is best placed to investigate a given matter and what would make more sense. We were not able to have these discussions with the Competition Bureau. We were limited in our ability to share specific information about the alleged facts to allow us to have that conversation.

Mr. Majid Jowhari: By amending it to allow a greater sharing of information, how are we improving it for the end consumer?

● (1115)

Mr. Daniel Therrien: The conducts that the three organizations responsible for CASL can investigate all tackle different angles of conduct that may be harmful to consumers, that is, consumer protection, privacy protection, and telecommunication issues. We cannot individually tackle all of these problems by ourselves. To be effective collectively in addressing the sum total of these harms, it's better to be able to share information and divide roles.

Mr. Majid Jowhari: Everyone is for sharing information. It will at least help in making sure that the end result is much better. Will it help with the enforcement?

Mr. Daniel Therrien: It would help.... For the enforcement of CASL provisions per se, we have the authorities we need to enforce the conducts prohibited by CASL. In our case, the two conducts are address harvesting and spyware. The recommendation we're making is to broaden the ability to share on other parts of our individual mandates. Here it's privacy protection, the obligation to have adequate safeguards. To have the authority to share information with the two other agencies for broader purposes would allow us to be more effective in our investigations on not the CASL conduct but the other conduct that is the subject of our acts.

I raise this in the context of this study, because the source of authority for sharing information, in our case to enforce PIPEDA more broadly, came from consequential amendments to CASL.

Mr. Majid Jowhari: Okay.

I want to change topics and go to PRA. Specifically, what are your thoughts on the fact that the PRA for now has been put on hold?

Mr. Daniel Therrien: The PRA deals with the enforcement of the mandate of the three sister agencies.

Perhaps I can limit my comments to whether PRA would help in enforcing the two conducts for which the OPC is responsible, spyware and address harvesting. I understand that there's debate around whether CASL goes too far in certain respects, but I would suggest that for the two conducts for which the OPC is responsible, address harvesting and spyware, this is clearly unacceptable conduct. The more tools there are to tackle these unacceptable products, including the private right of action, the better.

Mr. Majid Jowhari: Do you recommend any tweaks to PRA to ensure that, in the two jurisdictional areas you're focused on, the PRA could help them better pr are you comfortable with the PRA as is?

Mr. Daniel Therrien: I would welcome the coming into force of the private right of action as it relates to the two conducts for which I am responsible.

Mr. Majid Jowhari: Do you consider there's a need for any amendment on that?

Mr. Daniel Therrien: No.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): What are those two conducts?

Mr. Daniel Therrien: Harvesting email addresses and spyware.

Mr. Majid Jowhari: I have 30 seconds. I'll bank that.

The Chair: All right, because we're going to be tight on time.

[*Translation*]

Mr. Bernier, you have seven minutes.

Hon. Maxime Bernier (Beauce, CPC): Thank you, Mr. Chair.

This is a very good document. It gives us a lot of information about your role and, most importantly, about the challenges you have to handle on a daily basis.

My question is about your collaboration with other international organizations in fighting spam and, most importantly, ensuring that private and confidential information about Canadians remains that way. You gave the example of a case concerning the Dutch, if I remember correctly. Could you tell us about the steps you follow to ensure the success of your investigations and your collaborations?

Here's the second part of the question: does the legislation include the tools needed to make collaboration even more effective than it is now?

● (1120)

Mr. Daniel Therrien: The investigation in question, the one into WhatsApp, did not deal with illegal behaviour under Canada's Anti-Spam Legislation. We have been granted information-sharing authorities through consequential amendments, as part of our broader mandate.

You are wondering about the effectiveness of the tools and how information-sharing is done. I must say that sharing information with other international data protection authorities has been very important. The starting point of the analysis is that, obviously, the data crosses borders and the behaviours that may be problematic for privacy protection or to consumers also cross borders. We must therefore collaborate with other similar organizations to tackle common and global problems.

How do we do this? We have bilateral agreements with certain colleagues and certain other data protection authorities or multilateral agreements. These agreements allow us to share information, but they also contain provisions that protect the confidentiality of data collected by investigators for investigation purposes. We may share information with law enforcement agencies, but the agreements include provisions that the information is to be used for investigative purposes only and cannot be disclosed. When we conduct an investigation, PIPEDA, which is a federal act, requires our office to process information that is collected confidentially, which is normal. However, once the investigation is completed, we will inform the complainant and the respondent.

Under the federal legislation, I have the power to make certain information publicly available for public information purposes, as well as to learn from such behaviour. If it's in the public interest, I can disclose certain information. We can talk to the investigators within that framework. Unless the public interest requires some information to be made public to better inform the public, I think there are still some limitations.

Hon. Maxime Bernier: Right.

You spoke earlier about the private right of action. Several witnesses have told us that the provisions relating to it should not be put into effect. You have a different opinion.

Do you think this needs to be implemented? Should the right be enforced as is or should it be amended?

Mr. Daniel Therrien: I would prefer to limit my response to applying the right of action with respect to the two behaviours that fall within my jurisdiction. I won't say anything beyond that. Should there be any changes to the plan with respect to these two behaviours? I don't think so.

There was discussion of the amount of fines, for instance, and factors that would allow the regulator to decide on the amount of a fine or whether or not to impose a fine. I think these factors are reasonable. Has the company committed multiple offences? How serious is the offence? These are all factors that seem reasonable to me.

Of course, applying these criteria in a reasonable way is also important. The criteria set out in the legislation make sense. It's about applying them correctly on a case-by-case basis.

Hon. Maxime Bernier: I have one last question about the many exemptions in the legislation. Should the legislation be amended to provide for general prohibitions and fewer exceptions to better protect the privacy rights of individuals, or is the legislation as drafted adequate?

Mr. Daniel Therrien: The two behaviours that fall under my responsibility do not concern consent in the broad sense. It relates to two highly targeted and clearly unacceptable behaviours, namely, the harvesting of email addresses and the installation of spyware.

There is no doubt in my mind that spyware should be prohibited. There should be no exceptions that allow this kind of behaviour. Harvesting email addresses falls under the same category, but less clearly. There is a direct link between harvesting email addresses and the risks that consumers are exposed to, because email addresses can then be used to distribute malware, for instance. Because of the link between the two, I don't think there should be any exceptions.

● (1125)

Hon. Maxime Bernier: Right.

Thank you, Mr. Therrien.

The Chair: Thank you very much.

[*English*]

Mr. Masse, for seven minutes.

Mr. Brian Masse (Windsor West, NDP): Thank you, Mr. Chair. Thank you, witnesses, for being here today.

One of the concerns that has been expressed on a regular basis is that the legislation needs to be adapted, changed, or updated, because of the international spamming that's taking place. For that reason alone, it's not very valued, and it doesn't go back to the discussion or history where Canada really was a safe haven from spam before CASL. In fact, we were known internationally as being an outlier. You mentioned your Dutch involvement and the U.S. Federal Trade Commission. Can you highlight specifically what we could do to advance international support to get at spam, and how the international community needs to deal with this?

Spyware is one thing with regard to privacy, but we also see it heightened to ransomware and other things of that nature. I see a tool that we have, but I'm a bit concerned that we haven't provided the proper opportunities with regard to sharing it internationally. You mentioned the U.S. Federal Trade Commission, and also other international efforts that could be enhanced to protect Canadians if we actually make some changes.

Can you flesh that out a little bit, please?

Mr. Daniel Therrien: I referred, in answer to Mr. Bernier, to some of our efforts with the Dutch under bilateral or collective agreements. I'll ask my colleague Brent Homan to speak to networks, for instance, that have been created between regulators in various countries to tackle that very issue.

Mr. Brent Homan (Director General, Personal Information Protection and Electronic Documents Act Investigations, Office of the Privacy Commissioner of Canada): With respect to networks that have been created, these are enforcement networks that have evolved somewhat organically in order to address issues, whether they be with respect to privacy, such as the Global Privacy Enforcement Network, or Usenet, which is the network associated with electronic threats.

One of the benefits of such networks is the ability to not only come together to share expertise and to identify potential opportunities for collaborating together on investigations, but also to carry out informal actions and enforcement actions, such as global sweeps that have been carried out both by the Global Privacy Enforcement Network in areas such as children's privacy, and most recently with respect to Usenet in this area of electronic threats and spam.

Making use of those networks is a key part of the solution in terms of collaborating with our international partners. Often it can be an ability to identify who we may want to expand our ability to work more closely with on more formal investigations, because we can't in all situations. There has to be some MOU, or some mechanism that allows us to share confidential information.

Mr. Brian Masse: Right. If we allow that, we'll be able to get to some of the more international co-operations that are taking place already, if we change the act to allow for more sharing of information under your department. I want to be very clear. I want Canadians to know this is pretty technical, but they're going to get less spam, and they're going to get less privacy exposure, everyone from children to adults, if we're able to use some of these international collaborations.

Mr. Brent Homan: With respect—

Mr. Daniel Therrien: To clarify, we have these networks. We have bilateral agreements with other countries. In terms of sharing our information to enforce spam legislation, we're good. We have authority under CASL to share information. Our recommendations to improve the legislation with respect to sharing of information deal with domestic agencies outside of CASL per se.

● (1130)

Mr. Brian Masse: Then it still falls within our overall privacy regulations.

Mr. Daniel Therrien: Yes.

Mr. Brian Masse: Exactly. I just want to make this clear as we're getting there.

Mr. Brent Homan: Just to make one point as well, what we're seeing is often an intersection between issues of different regulatory spheres, an intersection between privacy issues and consumer protection issues. The commissioner talked about the one instance with respect to Ashley Madison where, while we were able to share information with the U.S. Federal Trade Commission on something that bled into the consumer protection issues, we ironically were unable to share information with our domestic counterparts. So that's where the mischief—

Mr. Brian Masse: I'll try to summarize it really clearly. We're missing an opportunity to protect privacy and people through our own obstruction, just for clarification here.

Mr. Daniel Therrien: To be generous, I would not say obstruction. I would say there were good authorities who gave us helpful additional tools to share information as consequential amendments to CASL. Parliament just did not cover all of the territory, and we would want all of the territory to be covered.

Mr. Brian Masse: When we had those discussions, some of those things were still forming at that time, and now we're seeing some of the fruits of those other efforts internationally.

Mr. Daniel Therrien: Exactly.

Mr. Brian Masse: With regard to the recommendation on sharing with CRTC and the Competition Bureau, that seems to be like low-hanging fruit we could do internally. On any work that you would continue to do with CASL, inclusion of the CRTC and Competition Bureau still fits within the regular law of how you're governed by Parliament.

Mr. Daniel Therrien: In terms of enforcing CASL per se, yes, we have the authority we need, but we think we need more authority to share outside of CASL.

Mr. Brian Masse: I think it would just be odd. For the CRTC and Competition Bureau, we'd expect that the collaboration would take place. It seems like more of an oversight in terms of the creation of the legislation that we would block you unintentionally from being able to communicate with the Competition Bureau

Mr. Daniel Therrien: I would agree that it's low-hanging fruit.

Mr. Brian Masse: With regard to Compu-Finder, so much has been reported on that. You have in number two here, with regard to the report of findings, the example of clarification that's required. Can you be more specific? How would that benefit consumers and privacy protection in particular if you had—

Mr. Daniel Therrien: Our second amendment?

Mr. Brian Masse: Yes, your second amendment.

The Chair: You have about 10 seconds.

Mr. Daniel Therrien: I'll ask my colleague to respond.

Mr. Regan Morris (Legal Counsel, Office of the Privacy Commissioner of Canada): I think the idea is just to make sure that PIPEDA remains the baseline protection for personal information for consumers. CASL is meant to provide extra additional requirements. PIPEDA is the baseline.

Mr. Brian Masse: The foundation.

The Chair: Thank you very much.

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

[*Translation*]

Mr. Frank Baylis: Good morning, Mr. Therrien.

You mentioned the power to decline or discontinue complaints. You also spoke about advancing so that you can focus on the practices that pose the greatest risks.

Could you tell me more about the changes that have been made following the coming into force of Canada's Anti-Spam Legislation?

Mr. Daniel Therrien: The consequential amendments to Canada's Anti-Spam Legislation go beyond the two activities I mentioned. Previously, because of the ombudsman model, when a person filed a complaint with the office and claimed that the act respecting the protection of personal information in the private sector had been violated, we had to investigate.

Mr. Frank Baylis: You had no choice?

Mr. Daniel Therrien: There were only some extremely limited exceptions.

The consequential amendments to Canada's Anti-Spam Legislation have reasonably expanded the reasons for which we can refuse to investigate. There are half a dozen exceptions; if you wish, my colleague Regan Morris can clarify this.

If another tribunal was dealing with a similar case, we could refuse to investigate, for instance, when a grievance mechanism would achieve the right outcome. We could then direct our attention to other matters.

Mr. Frank Baylis: You want to focus on practices that really pose great risks. Is that it?

● (1135)

Mr. Daniel Therrien: Yes.

Mr. Frank Baylis: So you had little flexibility, correct?

Mr. Daniel Therrien: Basically. We would like to have even more flexibility, but this still helped.

Mr. Frank Baylis: How could you get more flexibility?

Mr. Daniel Therrien: What is fundamental is that we must investigate all the complaints we receive. Given our limited resources, we may not be able to focus on what is most important and what would have the greatest impact on privacy protection.

[*English*]

Mr. Frank Baylis: I have another question to do with implied consent. Many of the witnesses talked about looking at the form of implied consent that comes with PIPEDA compared to with CASL. They were making the argument that we should look at PIPEDA, and that there are forms of implied consent that should be brought from PIPEDA to CASL.

Are you aware of the differences between PIPEDA and CASL when it comes to implied consent or the lack thereof in CASL?

Mr. Daniel Therrien: Generally, yes.

Mr. Frank Baylis: What are your thoughts on that?

Mr. Daniel Therrien: It's an interesting question.

My understanding of the CASL provisions on consent—even though we're not enforcing them, we're generally aware of them—is that it's an opt-in regime in which an individual receives communications from an organization only if they have opted in to that conduct.

PIPEDA, more generally, does not define specifically the relationships that are subject to opt in or opt out. It gives a certain number of general considerations. Under PIPEDA implied consent is permissible, but explicit consent is required based on a number of criteria. For instance—

Mr. Frank Baylis: Without going into the criteria, can you tell me whether that is working for you, in PIPEDA, that general...?

Mr. Daniel Therrien: I'll just mention one criterion that is relevant to your question.

One of the criteria, which are to be assessed on a case-by-case basis under PIPEDA as to whether explicit consent is required, involves the expectation of individuals. If we apply that standard to CASL, the question becomes what the reasonable expectation of consumers is in terms of receiving unsolicited communications from organizations. Do they find them helpful, because they help them make certain decisions, or do they find them unhelpful because—

Mr. Frank Baylis: But in general, PIPEDA's form of consent is working, and that has not been an issue for you in applying that law or in terms of people complaining.

Mr. Daniel Therrien: It works conceptually. There are huge issues in the application of it and whether consumers are properly informed so that their consent is meaningful. We could spend a couple of hours on that.

Mr. Frank Baylis: Okay.

Mr. Daniel Therrien: But in terms of the concepts and whether implied consent can be permissible in certain circumstances, I think that's a workable regime.

Mr. Frank Baylis: Thank you.

I'll pass my question time on to Mr. Lametti.

Mr. David Lametti (LaSalle—Émard—Verdun, Lib.): No, you covered it. Thank you. That was exactly the question.

Mr. Frank Baylis: Okay.

The Chair: You have a minute and a half.

Mr. Frank Baylis: Well, there you go, so I was rushing you for no reason then. Let me explore that a little bit further then.

In terms of PIPEDA, if I can say so, grosso modo, in general, it's working. You might have questions as to whether an individual truly understands or not, but people are not coming to you up in arms, saying, “I didn't really get this right and they've grabbed information of mine that I did not consent to, implicitly or explicitly.” Are you having—

Mr. Daniel Therrien: I'll try to be more nuanced in my answer.

PIPEDA allows for implicit consent and requires explicit consent based on criteria that generally makes sense. Does it work? It all depends on whether meaningful consent is obtained, and people do come to us frequently to say, “Maybe the law allows for implicit consent, but I never understood that I was giving implicit consent for this or that conduct by the organization.” How this applies and what kind of information is given by organizations in order to obtain meaningful consent is the subject of my last annual report. It's a very open question, and I think many improvements would be required.

If I understand the question posed to me in terms of comparing CASL consent with PIPEDA consent, I concede that CASL consent is more onerous for organizations. Therefore, the PIPEDA consent regime could work if proper information was given to consumers, but in addition to that, I would suggest that you need to ask yourself, among other things, what the expectation of consumers is in terms of receiving unsolicited communications from organizations? That's the first question.

I don't have the answer to that question. Different countries have different answers, but one question is, what is the reasonable expectation of consumers?

● (1140)

The Chair: Thank you very much.

We're going to move to Mr. Eglinski for five minutes.

Mr. Jim Eglinski (Yellowhead, CPC): I want to thank the witnesses for coming.

Your website directs people to go to fightspam.gc.ca to report their incident. Who directs, from fightspam.gc.ca, who it goes to, you or one of the other two departments? Who decides that, or do they just throw it out to all three of you?

Mr. Daniel Therrien: I'll ask my colleague Brent Homan to answer.

Mr. Brent Homan: With respect to fightspam.gc.ca, that's one portal by which individuals can identify whether there are complaints. In terms of our process at the OPC, we can also receive complaints directly, related to CASL or other privacy matters.

We have received certain complaints, but by the nature of what we are looking at, as with harvesting and spyware, they're opaque practices, so it's less likely for us to receive complaints. It's less likely for individuals to know whether they've been affected by such practices. As a result, we look at things more proactively, but fightspam.gc.ca might be one portal to identify issues they could relay to different authorities. We have working groups where we are able to collaborate and discuss issues of commonality, but as well, the traditional intake and complaint process is available and that's what's often used.

Mr. Jim Eglinski: Thank you.

Daniel, we've had a number of witnesses over the last two or three meetings talk about the internal departments they have just to deal with the legal concept of CASL. I wonder if you can tell me how many cases over the last few years your department has handled. It doesn't have to be exact. As well, how many people would you have in your department basically dealing specifically with this portion of your department's enforcement role?

Mr. Daniel Therrien: I'll give you an answer. I'm not sure we're the most relevant organization to ask this of, because again, our role in terms of CASL is limited to two activities: address harvesting and spyware, both of which are clearly unacceptable. There are more questions around spam per se and the fact that organizations are unable under that legislation to contact individuals, but our role deals with these two types of conduct. We don't have many cases. That's not the sum total of CASL by far, but these two types of conduct in particular are essentially hidden, so it is very difficult, if not impossible, for individuals to see the harm being done. We act, in part, based on information in the CRTC's spam centre, the analysis of this, to ourselves spot trends, spot problems, and act on our own initiative.

I've mentioned two investigations that we have conducted. There are not many, just two, and they have resulted in reports of finding. We're investigating other activities currently, but they are few.

As to how many people we have to devote to these efforts, there is no one specifically on this. However, we have a handful of people who, among other duties, have as a duty to enforce this particular piece of legislation.

● (1145)

Mr. Jim Eglinski: Okay. Could I stop you there for a moment.

You did mention that you appear to be doing some proactive work —

Mr. Daniel Therrien: Yes.

Mr. Jim Eglinski: —and you are doing reactive work. I want to get into this.

As lawmakers, we have made this law, CASL, for you. Are we providing enough resources—and I'll just go to your department—to handle the caseloads that you're working on?

Mr. Daniel Therrien: To answer that question, I would have to look at the sum total of our responsibilities.

Again, CASL addresses two conducts out of a very large number of activities that affect privacy protection. I think it is very difficult to be effective in privacy protection writ large with the resources I have. Is CASL the biggest problem? I would not say so. It is part of the problem of insufficient resources to tackle privacy protection generally.

Mr. Jim Eglinski: All right.

How are we doing for time?

The Chair: You're done. We're very tight on time.

We're going to jump to you, Mr. Sheehan. You have a very quick five minutes.

Mr. Terry Sheehan (Sault Ste. Marie, Lib.): Thank you very much.

Again, to our presenters, this is very helpful in terms of providing a perspective in terms of some of the very good testimony we've heard so far.

One of the things I've observed throughout the statements being made is that it would seem for the legislation as it stands—it's not necessarily just the legislation, perhaps, but just the way the education and information has been sent out there—companies and people are being very risk averse and their lawyers are telling them, “Just don't send anything.”

In your presentation, you mentioned that you were going to be undertaking some new outreach. Could you expand on that? How will that be different and how will it help educate people? Specifically, what are you trying to educate people about?

Mr. Daniel Therrien: Go ahead, Brent.

Mr. Brent Homan: I can talk about one specific outreach initiative where we thought we would do some reaching out to organizations that may not know they're implicated with respect to address harvesting—address harvesting being the collection of addresses through electronic means. Some organizations that use address lists may think that doesn't have anything to do with them, that they just purchase the lists and use them in order to do their marketing. However, if you've purchased a list that's been compiled without the adequate consent of the individuals through address harvesting, then you're also potentially on the hook for a violation of the act.

For part of our outreach, at least in that specific area, we thought it was highly valuable to say to these organizations, which are broadly across sectors, that if they are using lists, they must ensure that they ask the right questions of the list providers to ensure the list has been compiled with the consent of those people on that list.

That's a good example of what we've done in the area of outreach, at least for organizations.

Mr. Terry Sheehan: That's very interesting.

In the presentation, you also mentioned in your conclusion that CASL enforcement is a "key part of the suite of activities", and you talk about working "diligently to educate individuals and organizations on the privacy implications of digital technologies, social trends, and business practices, and to enforce privacy protections".

We've touched a bit on Facebook and the new platforms that are coming out. I think we're still trying to wrap our heads around what implications going forward there could be for social media with this particular legislation.

Are there any comments on that?

Mr. Daniel Therrien: I'm afraid the question is a bit too broad for me to get my head around it.

Legislation about social media generally...?

Mr. Terry Sheehan: About how CASL may or may not affect social platforms.

Mr. Daniel Therrien: Do you have a view on that, Brent?

Mr. Brent Homan: Well, I can tell you how it can be related.

Mr. Terry Sheehan: Yes.

Mr. Brent Homan: If you look at the recent case with respect to Wajam, you'll see that one of the features of this adware is that it was coupled with social media interactions and delivered to individuals. Social media could be leveraged by organizations that are carrying out some of these other activities, such as in the Wajam situation, in order to facilitate those activities.

Mr. Terry Sheehan: That's exactly what I was getting at. Social media can be used as a tool to spam people. Is that what you're saying?

● (1150)

Mr. Brent Homan: In this situation an organization was coupling the adware with the understanding of the contacts related to social media. It wasn't just social media that was spamming, no. It was this organization that was installing this adware along with other free adware. Social media was a component, but it was not the avenue by which it was delivered.

Mr. Terry Sheehan: How was it a component? I'm still not understanding that.

Mr. Brent Homan: The adware would take a look at social feeds and deliver and identify advertisements related to the social feeds. It was making use of the social network.

Mr. Terry Sheehan: One of the other things you mentioned in your presentation was a particular group that you deemed had been sending emails, but then started to excessively use emails. You deemed that inappropriate. What's the difference between the two? I believe it was the case in which—

Mr. Daniel Therrien: It was Compu-Finder. Because address harvesting harvests many electronic addresses, it can obviously facilitate an excessive number of communications to consumers who do not wish to receive these communications. That's the link we're making. It's excessive from the perspective that numerically many people are affected and receive communications that they never asked for, and address harvesting results in that conduct among other things. Address harvesting can also, in the worst case, be used to disseminate malware and can lead to other privacy risks.

The Chair: Thank you. We're going to have to move on.

Mr. Jeneroux, you have five minutes.

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

Thank you to Mr. Therrien, Mr. Morris, and Mr. Homan for being here today.

Take it back to the Wajam case. How does that come to your office? Is a complaint made through fightspam.gc.ca, and you guys see it and then take it? Does it come through CRTC? Going back to that specific case, what happens?

Mr. Brent Homan: This case was intelligence-driven. It pointed out with respect to these threats, address harvesting and spyware, it's more unlikely that individuals will know that they've been affected and impacted by that. Right from the outset with respect to the coming into force with CASL, we expected to take a more proactive approach. The Wajam case was a result of identifying potential threats and risks out there in the marketplace and knowing that and surveying that there were issues and concerns related to this specific type of adware and its installation and its difficulty with respect to de-installing as well.

Mr. Daniel Therrien: People noticed it was intelligence-based when they tried to reinstall the system and were unsuccessful. Some of them made their views known, but the start of this was intelligence-based.

Mr. Matt Jeneroux: By intelligence-based do you mean you guys did it?

Mr. Daniel Therrien: Yes.

Mr. Matt Jeneroux: Was there any collaboration with CRTC at the time? Did you give them a heads-up that this is what you were doing? Is it looking for work and pursuing the case? I'm trying to connect the collaboration.

Mr. Brent Homan: There was more collaboration with the CRTC with regard to the Compu-Finder investigation because two agencies were carrying out the same investigation. Our office was looking at the collection of addresses whereas their office was looking at the dissemination of messages. To that extent the issue was very complementary. That was where there was closer sharing of information, and just keeping each other apprised of the status of investigations.

With respect to Wajam, there wasn't any specific collaboration, but we also have certain working groups and certain opportunities where we get together and talk and are aware of what each other is doing to see whether there might be an opportunity to collaborate, or to know that we've seen this, is this something of interest to the others or not, and that way we can make a more informed decision about who's best placed to pursue our matter.

● (1155)

Mr. Matt Jeneroux: Would Wajam have been brought up at some of these collaborative meetings?

Mr. Brent Homan: It would have been mentioned at certain meetings that we were pursuing this.

Mr. Matt Jeneroux: Who is at those meetings? Mr. Therrien, are you at these meetings?

Mr. Daniel Therrien: No, Brent is.

Mr. Matt Jeneroux: Who would be the equivalent on the other side?

Mr. Brent Homan: Often it could be the DGs, or the assistant deputy commissioners, or whoever it might be. There are different steering committees. There's the directors general steering committee, where we talk about broader issues as well as about ongoing investigations. As well, there are enforcement working groups that get together and talk about matters ongoing.

Mr. Matt Jeneroux: In the last minute and a bit that I have left, Mr. Therrien, you and I worked together on the ETHI committee with regard to the PIPEDA legislation review. There were a number of recommendations made out of that report. I'm curious if some of that, particularly the order-making powers, would assist on the CASL side of the legislation. Would you be able to comment on some of those?

Mr. Daniel Therrien: Absolutely, yes, it would assist. Again, when we look at the two prohibited conducts under CASL, the two conducts relevant to us, these are unacceptable practices by organizations. Generally speaking, I would say that the more tools that are proportionate to the conduct, the better. A private right of action fits within that, in my view, and order-making to require companies to desist from certain conduct would also be very effective.

A number of companies wish to comply with the law, but not all do. In particular, for the two conducts of address harvesting and spyware, these are conducts where you're not dealing with very legitimate companies or organizations, so order-making would help.

The Chair: Thank you very much.

Mr. Longfield, you have a very fast five minutes.

Mr. Lloyd Longfield (Guelph, Lib.): Thank you. I'm not sure what “very fast five minutes” means, but I appreciate that you're giving us a lot of information in a short amount of time. Let's work with that definition.

You mentioned, Mr. Therrien, we're dealing with the movement of data across borders, the fact that this is a global situation versus a Canadian-only situation. Is there some type of a forum where you get together with counterparts? Let's say we just got a free trade agreement, an economic trade agreement , CETA, with Europe, and we'll be doing a lot more back and forth with Europe. Is there, in terms of trade agreements or other commercial activities, a group that meets internationally to look at legislation among the different countries, to see whether it's harmonized, to see whether they complement each other or if there are any gaps?

Mr. Daniel Therrien: I'll try to answer the best I can with as little time as possible.

The one reality is that privacy laws are not harmonized, but they're not completely dissimilar, either. There are important differences. They're all inspired by the same principles. They are not drafted in the same way. They're not harmonized.

Regulators, other data protection authorities, privacy commissioners have to operate within that environment. It is possible, not perfectly, to work within that environment and enforce our respective laws through the kinds of co-operation that I had referred to in the past, either bilateral or multilateral agreements with other data protection authorities. There is quite a bit that is happening on that front.

There are various networks. There is an international conference of data protection authorities that discusses these issues. There are arrangements under that network. There are other networks. There are a number of networks. The situation is not perfect because, ideally, the laws would be harmonized, and that's not the reality and I don't think it will be the reality anytime soon.

Mr. Lloyd Longfield: Right, so as we review this legislation, in your testimony you've talked about some of your concerns, the three recommendations you've made. In previous meetings we've had other recommendations around the six-month and two-year maintenance of data. Is maintenance of data an issue that countries...or maybe within your own department is that something normal that you deal with under CASL?

● (1200)

Mr. Brent Homan: Maintenance of data...?

Mr. Daniel Therrien: Are you referring to the upcoming data breach regulations?

Mr. Lloyd Longfield: No, I'm looking at the consent rules. We've designated holding data for six months or two years. We've had other testimony saying we should get rid of those consent rules because they are onerous, hard to manage, and place a burden upon businesses.

Mr. Daniel Therrien: I'll ask Regan Morris to complete this, but I would refer to the general regime under PIPEDA, wherein the rule is that information collected from consumers by an organization must be kept only as necessary. That's the concept. There's no prescribed time limit.

Regan.

Mr. Regan Morris: I think your question is dealing with the specific consent provisions that the CRTC enforces in relation to proving that they have obtained consent for the—

Mr. Lloyd Longfield: Yes, you have to prove it, and then you have to store it.

Mr. Regan Morris: I'm not sure we would have a comment on those specific rules. As the commissioner has said, the general rule for storing personal information is to keep it only as long as necessary, and that could be because of legal requirements.

Mr. Lloyd Longfield: My questions in previous discussions have been around there being a lot of external invasion into our networks and about how we manage those invasions, but that's probably not within your mandate—or could you comment on it?

I'm thinking of the Russians getting into the American election and of the things in the media that the public would be familiar with. How do we protect ourselves against that type of activity?

Mr. Brent Homan: If you are talking specifically about the notion of external invasion into networks, then spyware, for example, might be a gateway in order to allow and facilitate such invasions.

Mr. Lloyd Longfield: That's it.

Mr. Brent Homan: To that extent, address harvesting can result from spyware or can result in the application of spyware. They are all interrelated in that these are threats, and when they are threats to the digital economic platform, they're also threats to the networks, whose robustness and constitution impacts upon trust in that platform.

Mr. Lloyd Longfield: —and are therefore necessary.

Thank you, Mr. Chair.

Mr. Daniel Therrien: [*Inaudible—Editor*] are a part of the solution, but are not all of the solution, obviously.

The Chair: I'm sorry, we are over time.

However, Mr. Masse, you have the final two minutes, so make them count.

Mr. Brian Masse: Thank you. I have just one quick question.

The responsibilities of the department have increased with CASL and other types of measures. Has your overall budget reflected that?

Mr. Daniel Therrien: We received funds for CASL, but for other responsibilities, not so much recently. For CASL, however, we did receive funding.

Mr. Brian Masse: That's all for my questions.

The Chair: I'd like to thank our witnesses for coming in today and giving us a lot of information to chew on.

We're going to suspend for a very quick two minutes. We're going to switch witnesses, and then we're going to come right back, because we're already tight on the next committee time.

Thank you.

● (1200)

(Pause)

● (1205)

The Chair: We want to get everybody back. We're on a very tight time schedule and we have already cut back on some of our questioning time.

We're going to keep our first four question rounds at seven minutes. Then we're going to drop to three minutes, just to try to get everybody in.

Welcome to our new panel.

With us we have, from the Canadian Bar Association, Suzanne Morin, chair of the privacy and access law section, and Gillian Carter, lawyer, legislation and law reform.

From the Coalition Against Unsolicited Commercial Email we have Neil Schwartzman, executive director, and Matthew Vernhout, director-at-large.

We're going to start off with the Canadian Bar Association.

If you can keep it to under eight minutes, that would be great.

Ms. Suzanne Morin (Chair, Privacy and Access Law Section, Canadian Bar Association): Thank you very much, Mr. Chair.

Good afternoon, honourable members of the committee. My name is Suzanne Morin, and I am chair of the CBA's national privacy and access law section, and I work for Sun Life. With me today, as you know, is Gillian Carter, who is a lawyer with the law reform directorate of the Canadian Bar Association.

Thank you for inviting us to present our views on CASL. Before addressing some of our main points though, I'm going to ask Ms. Carter to provide some background information on the CBA for your information.

Ms. Gillian Carter (Lawyer, Legislation and Law Reform, Canadian Bar Association): Thank you.

The CBA is a national association of over 36,000 lawyers, law students, notaries, and academics. An important aspect of our mandate is seeking improvements in the law and the administration of justice. That is what brings us here today. Our written submission, which you've received, was provided by the CBA's privacy and access law section, the competition law section, and the Canadian Corporate Counsel Association. These sections consist of lawyers from every part of the country who have in-depth knowledge of privacy and access law, competition law, and issues affecting in-house counsel.

● (1210)

Ms. Suzanne Morin: I'm going to focus on a few main points, many of which have been echoed by others who have appeared before you.

The CBA sections believe that CASL must strike a balance between protecting consumers from damaging and deceptive electronic communications while at the same time allowing businesses to compete in a global marketplace. CASL's interpretation and application need to be clarified to meet the act's objective, which is to protect consumers by really targeting bad actors. In our view, current application and enforcement efforts are not in line with the act's objectives. Instead, legitimate businesses doing the best that they can to comply are being targeted.

In its current form, CASL is confusing and overly complex. CASL is an unclear statute, and there are two separate sets of regulations that go with it. This makes compliance very difficult for organizations, especially for small and medium-sized businesses, as well as not-for-profits, who have limited resources. The CBA sections have set out in our written submission a number of the more problematic interpretation areas in CASL.

One example, and you've heard that many times, is the broad definition of commercial electronic message, which is open to significant interpretation. This overbreadth limits messages that may benefit consumers, and has a chilling effect on innovation and competition. Canadian organizations, out of fear of being non-compliant, have reduced their email marketing efforts, creating an anti-competitive environment.

Another example is the requirement for installing computer programs, which deems express consent if it is reasonable to believe through the person's conduct that they consented. It is very unclear, however, what conduct will be sufficient to meet that threshold.

The CBA sections encourage publishing all in one place guidance materials that are updated regularly. For example, it would be very helpful to have a regularly updated Q and A web page addressing some of the more complex interpretative issues that are being raised from time to time by practitioners.

The limited guidance currently available to address the confusion and uncertainty in CASL increases the possibility, and you've heard this as well, of inadvertent non-compliance. The guidance that does exist is incomplete, out of date, inconsistent, and overly simplistic even at times. For example, the guidelines on the interpretation of electronic commerce protection regulations read obligations into CASL that are not supported by the legislation itself. The guidelines state that consent must be sought separately from general terms of use or sale, but CASL speaks only to keeping CASL consents separate. That's an additional obligation not found in the act.

The guidance is also difficult to find. Some is provided by the CRTC, some by the Competition Bureau, some by the Office of the Privacy Commissioner, and some by ISED.

The CBA sections encourage greater transparency of CASL's enforcement and oversight mechanisms. Currently, there is little information about how the CRTC decides which cases to investigate, and what monetary fines to impose. As well, it is unclear from reported decisions to what extent the CRTC is actually applying the due diligence defence.

Organizations are also not typically advised of complaints prior to commencement of an investigation, nor are they given an opportunity to respond to complaints in an informal manner. We believe this is a missed opportunity.

An informal mechanism that allows organizations to respond to complaints and make the necessary changes during the normal course of business would be a wonderful opportunity to deal with a lot of these complaints that you see coming into the CRTC's complaint spam centre. This would reduce significant investigation costs down the road, and would be particularly useful in cases of unintentional non-compliance, or differing interpretations.

The CBA sections also encourage a thorough analysis of the appropriateness of the private right of action provision, and its scope in the context of the whole of CASL. In our view, bringing the private right of action into force without clear guidance is premature. Even without the private right of action, CASL has a broad range of enforcement tools, and you heard from Commissioner Therrien this morning. In our view, any lack of compliance is more likely the result of the confusing and onerous nature of CASL, rather than the current enforcement tools being insufficient.

We want to note, in particular, the application of the private right of action under the false or misleading representation provisions of the Competition Act. The need for the private right of action in this context remains questionable particularly given the Competition Bureau's existing oversight and enforcement. The relevant provision, section 74.011, is also concerning because certain subsections contain no materiality threshold.

● (1215)

Finally, we also want to note the inordinate cost and resource burden of CASL on charities and non-profits. We would recommend that they be exempt from all of CASL's provisions, except for the ID, content, and unsubscribe requirements as they relate to commercial electronic messages.

In conclusion, the CBA sections once again appreciate the opportunity to share our views on CASL. Given its complexities, we believe a more extensive consultation is needed under the statutory review, and we encourage you to invite more stakeholder feedback and more detailed feedback.

Thank you for having us here today.

[*Translation*]

We will be pleased to answer your questions.

Thank you.

[*English*]

The Chair: Thank you very much.

We're going to move to you, Mr. Schwartzman, for under eight minutes if you can, so we have room for questions.

Mr. Neil Schwartzman (Executive Director, Coalition Against Unsolicited Commercial Email): Absolutely.

With apologies to the Bard of Avon, friends, parliamentarians, countrymen, lend me your ears; I come to praise CASL, not to kill it. The evil that critics of CASL do lives with them; the good is oft imbued in its sections; so let it be with CASL.

CASL's noble adversaries may tell you the law is too ambitious, as if this was a grievous fault.

CASL enshrines the work of the 2005 federal task force on spam. Best practices found in our final report are now global industry standards, but best practices mean nothing without disincentives to bad actors.

CASL is a crowdsourced law, taking input from hundreds of people working tens of thousands of hours. The Messaging Anti-Abuse Working Group, for example, MAAWG, is an industry association of 185 member companies, all anti-spam professionals, such as Apple, Facebook, Google, Amazon, and Bell Canada. MAAWG participated throughout the CASL process and sent a letter to the Prime Minister urging the passage of the law as it was tabled.

My name is Neil Schwartzman. I'm the executive director of the Coalition Against Unsolicited Commercial Email. I wrote the world's first distributed spam filter, and 20 years later, here we are. I'm a management consultant. My clients include the world's largest company and the world's biggest sender of commercial email, neither of which spam. It's not that hard. I also teach cyber-investigation methods to international law enforcement.

Spam filtering costs recipient networks $20 billion a year. We pay for spam. Spam has become much worse of late: ransomware and phishing payloads are vicious. Ninety per cent of the spam that hits our networks is affiliate spam, which you've heard we should allow. Affiliate spam is an open sewer spraying a billion messages per hour at our families, friends, and colleagues. Unsolicited junk email, texts, and phone calls from Walmart, DirecTV, and Fidelity are some of the affiliate spam sent by third parties, earning commissions from the brand to send spam. CASL was purpose-built to remedy such activity.

The Privacy Commissioner and other law enforcement agencies just this year have completed a five-country sweep against affiliate spammers. Results have yet to be published, but we will be hearing about that. Studies from Cloudmark, Inbox Marketer, Return Path, and Cisco have proven CASL to reduce spam coming into Canada and going out of it. That's data, not opinion.

Law enforcement can't possibly investigate, nor do they know about all of the spam attacks. CASL's PRA, a right integral to the American CAN-SPAM Act, has been suspended, lamentably preventing Canadian ISPs, businesses, and organizations from seeking compensation for damages done to their network by spam.

Declarations of CASL's damaging effects that some have made here are laughable. The OECD two weeks ago projected that Canada's economic growth for 2018 is the best in the G7. Quebec is enjoying the lowest unemployment rate in three decades. Our economy is not hurting. We hear about how legitimate companies have been caught in the CASL net. In two cases prosecuted by the CRTC, the marketing departments of Rogers and Kellogg's used spam email lists provided to them by third party firms. Yes, legitimate companies bear costs to become compliant, just as when PIPEDA came into force.

Businesses must be vigilant. Data breaches occur daily. Business email compromise costs tens of millions of dollars. CASL defines modern standards of data integrity and permission that companies must maintain in the global economy. In the EU, the updated GDPR privacy law comes into effect in 2018. Failure to maintain parity with them will put us at a severe economic disadvantage.

● (1220)

Why are some afraid of CASL? It's because it's working. CASL is so frightening to spammers that they lobby Canada's law enforcement and legislators. American groups with direct ties to black-hat spam organizations will present you with information in the coming weeks. They've been invited here.

With this in mind, I exhort you to leave CASL intact. Adjust, yes, and clarify, doubtless, but do not come here to kill CASL. Do Caesar proud.

Thank you for inviting us here.

The Chair: Thank you very much.

Mr. Vernhout.

Mr. Matthew Vernhout (Director-at-large, Coalition Against Unsolicited Commercial Email): I'll be quick.

Good afternoon to our distinguished members of Parliament. Thank you for inviting us to speak with you today.

My name is Matthew Vernhout, and I am here on behalf of CAUCE, the Coalition Against Unsolicited Commercial Email. In my professional capacity, I am the director of privacy and industry relations for the email analytics firm, 250ok; the chair of the Email Experience Council's advocacy subcommittee; and an active member of the global email community.

I participated in the drafting of America's CAN-SPAM Act, and I had the pleasure of speaking to this committee in support of CASL in 2009.

I have published dozens of articles, been quoted in the press, spoken at numerous industry events, and consulted with some of North America's top brands regarding CASL compliance. In fact, one of the comparative benchmark reports I authored for ISED was recently cited in the CRTC's decision on the constitutional challenge by Compu-Finder.

The positive effects of CASL on the email industry are remarkable. I'm delighted to say analysis finds the email industry thriving and experiencing significant growth. Businesses ensure they have recipient consent, and they are seeing the positive benefits of those actions. A common trend has emerged from several published reports in the last three years: more messages are delivered to Canadian consumer inboxes post-CASL, due to better list management practices and consumer trust. A recent industry report shows that two countries with the toughest anti-spam legislation, Canada and Australia, also have the best deliverability of commercial emails to inboxes in the G8 nations studied.

The basic framework of CASL is a series of email marketing best practices that have been the basis of most of my consulting efforts over the last 17 years: ask for permission, honour opt-outs, and be clear as to who you are and why you're sending the messages. CASL has taken these ideas and made them the law of the land.

As my colleague stated, CASL is working to diminish spam. Moreover, it is working to make legitimate email marketing more successful and more effective. There is far too much baseless fear, uncertainty, and doubt being spread by the naysayers of CASL, many of whom are neither anti-abuse nor marketing professionals.

When I speak with marketers about their compliance efforts and the challenges they face to make their digital marketing compliant, I hear, “This is a lot of work, but it's not nearly as difficult as I thought it would be.”

However, we still have a long road ahead of us. The spam reporting centre receives 6,000 complaints per week, totalling more than one million complaints since 2014. For example, blacklist operator SURBL notes that there are currently 70 “.ca” domains spamming counterfeit goods targeting Canadian consumers. There are also active spam gangs set up on hosting providers in Montreal, Hamilton, and Vancouver.

Regarding the PRA suspension, this renders CASL toothless. The PRA should be revisited to allow network operators who carry the cost of spam to avail themselves of redress.

In closing, it is our hope that the law remains a strong and viable tool to protect email marketing, networks, and consumers from unwanted spam messaging. Canadians, like all consumers, deserve nothing less.

Thank you.

● (1225)

The Chair: Thank you very much.

Just so that all of you prepare accordingly, the first four rounds will be seven minutes and we're going to maintain those. Afterwards we'll try to do three minutes, but we might not get through the entire thing. If you really are on the bottom of the list and you want to get up to the top, plan accordingly.

We're going to jump right to Ms. Ng, for seven minutes.

Ms. Mary Ng (Markham—Thornhill, Lib.): Thank you, everybody, for coming today and for your testimony.

I'm going to begin with Mr. Schwartzman.

We heard a lot here at the committee about PRA, and of course, the PRA is suspended. One of the things we would benefit from hearing your opinion on is how this committee might consider PRA in a way that allows it to have the teeth and also consider some of the potential issues that people are raising, that businesses are raising, around compliance and fear of litigious suits that are unmerited. Help us understand that a bit.

Mr. Neil Schwartzman: I think that's an excellent question. There's no denying that I have some open fears about people misusing the law. We didn't intend it to be a cash cow for litigious frivolities. Mr. Vernhout has stated CAUCE's opinion. Our stance is that network operators should be allowed to avail themselves of private right of action, so ISPs, companies, and organizations should absolutely be able to have a right for redress. We're growing softer on the right of individuals to sue a company, or the class action stuff. Admittedly I think that's where the vulnerability lies, and, no, we don't want this to be stupidly abusive. I know we are in a loser-pays environment here in Canada, but that will not prevent frivolous suits from being filed. So let's just focus on the people who actually operate the networks and suffer the damage.

Ms. Mary Ng: Narrowing it is a good suggestion that could, in fact, be a modification here to allow for private right of access to proceed but under that focused mechanism.

Mr. Neil Schwartzman: Yes, precisely. I think we've also heard from the Privacy Commissioner and others about some reasonable sculpting, which makes it less...in fact while I rarely find myself in agreement with Ms. Morin, I have to agree that the “false and misleading” is very vague, and there absolutely need to be standards set before we go with that. Again, it has parity with CAN-SPAM and other places, but it allows a network operator, an ISP small or large, to say “stop”. And, yes, everybody says we can't sue Nigerian spammers, but they exist in this country. The “Nigerian princes” are here. They are everywhere. They pretend to be from Nigeria, but they do exist in this country. There's this kind of fallacious thing of “Oh, we can't deal with international spam.” Private right of action allows us to actually do that.

Ms. Mary Ng: Thank you.

I'm going to the CBA with the same question.

Give us your thinking about how this committee should consider private right of action, and how to allow for the teeth while balancing legitimate businesses being able to operate and not encouraging litigious action.

Ms. Suzanne Morin: The very fact that you're asking those questions is really the first step. As Mr. Schwartzman explained, even when CASL was being debated before committee, back when it was introduced, definitely one of the comments about it made by the business and legal profession was that it was too broad, that it went way beyond what we were seeing across the border, and also what we thought was necessary, which was to allow those who were suffering the harm, if you like, the network providers.... While the CBA doesn't have an explicit provision as to exactly what it should be, you need to look at it, and you need to make sure that you look at it in the context of existing CASL and any changes that you might make. But narrowing it down to those service providers who are actually suffering harm and actually have the ability to go after some of those more nefarious players sounds like a possible, reasonable approach.

● (1230)

Ms. Mary Ng: Well, I'm not hearing that PRA should be eliminated. I'm hearing that PRA should be focused so that we could actually get at the bad actors. Is that a view shared by you as well, Mr. Vernhout, in your organization?

Mr. Matthew Vernhout: Absolutely. As a consumer who receives large volumes of spam, certainly I've had a personal interest in being able to go after that, but in turn, if my network provider and my email provider had the tools to go forward on my behalf, or on behalf of fellow consumers using their domains, I certainly think that would be a valuable tool. We did see under CAN-SPAM that organizations like Facebook have effectively used CAN-SPAM on their own to protect their network and protect their users. In fact, they did have a settlement against a gentleman in Montreal that resulted in, I believe, a $1-billion violation under the California anti-spam act and CAN-SPAM, which was later upheld by the Quebec courts, because his initial response was that if he lived in Canada, CAN-SPAM didn't apply. Then they went after him civilly and were able to get the Quebec courts to honour that judgment.

Ms. Mary Ng: Okay.

The Chair: You still have a minute left.

Ms. Mary Ng: Do you want to go? I've actually done my piece.

Mr. Frank Baylis: Sure.

I'll go to you, Mr. Schwartzman.

In line with what Ms. Morin said, when it comes to messaging, we've heard from people saying that some of the electronic messaging has too broad a definition and it denies certain companies the right to do updates that are necessary or there are certain things, like the Internet of things, where they can't get explicit consent to do an update. Would you agree with that?

Do you see a value in defining what those electronic messages are, more in line with what was suggested by Ms. Morin?

Mr. Neil Schwartzman: The IoT software update issue has been misstated a little bit to this committee and perhaps misunderstood more generally. Once you install a piece of software and they throw up the terms of service to a net user, they also accept, if the terms of service are written correctly, the ability of the software publisher to update the software.

Mr. Frank Baylis: Would it hurt us to make that clear in the legislation?

The Chair: We're going to have to move on, but very quickly—

Mr. Neil Schwartzman: It would not hurt us. It would benefit us and IoT is a lurking giant that should scare us all.

The Chair: Thank you.

We're going to move to Mr. Jeneroux.

You have seven minutes.

Mr. Matt Jeneroux: Perfect. Thank you, Mr. Chair.

Thank you all for being here today.

Ms. Morin and Ms. Carter, I want to pick up on something that you brought up during your presentation. I think it was you, Ms. Morin, who talked about small businesses and their—I'm trying to refrain from using the words “ability to pay” because I feel that's part of the act and I don't intend to associate the question to that part of the act. Could you give us some tangible examples of what has been done in the past that has made it difficult for these businesses? Is it an IT system that they have to pay for? Is it more staff? Could you go into a bit more detail on what you spoke about earlier?

Ms. Suzanne Morin: Sure. Thanks for the question.

From a large business perspective, you gather the resources and you do what you need to do to comply. As someone who has worked on implementing CASL internally at a few organizations, but also in working with external counsel and my colleagues in other companies, and the discussion we have at the CBA across the different sections as well, it is truly amazing the amount of time spent, and org charts and step-by-steps that you have to develop in order to make sure that you're actually complying with all the different pieces because it is unnecessarily complex. You shouldn't need a lawyer to implement CASL, and unfortunately, you do. When you think of a small enterprise where they have a few employees, or larger ones—and you heard from the Canadian Marketing Association, an organization which in about 2025 may have spent upwards of $40,000—it's mind-boggling.

Once again, the idea is not to get rid of CASL, but rather to have it focus on what it should be focusing on. For small and medium-sized enterprises to be sending electronic communications to their customers or trying to do prospects, even before CASL came around, people used to insist on consent. However, it's all the little things you need to do to ensure that you have complied that bogs everybody down and it's the fallout from the non-compliant element. If it were more akin to PIPEDA, on which we heard from Commissioner Therrien before, it's a complaints-based model. If you make a mistake or you have a judgment call that you make that's not quite agreed to by everybody else, you have an opportunity as an organization to make it right without necessarily seeing yourself subject to a very formal investigation or fines.

Unfortunately, in the way it's been enforced here in Canada by the CRTC, it has had a chilling effect. You don't want to be that organization that then has to have a settlement agreement or notice of violation.

● (1235)

Mr. Matt Jeneroux: Right.

Mr. Vernhout, I'll come to you because I can see you getting a little bit agitated by some of that. I just want to narrow it down because there are definitely views and opinions, at the end of the table here, where Mr. Vernhout says that people say it's not as hard as what they thought it was.

What I'm hoping to get from you, Ms. Morin, is some of those examples that we can tangibly see that—the $40,000 was a great amount that was brought up by the Canadian Marketing Association. Is that an outlier in this? Is that the norm? Again, I'm trying to get a sense of what you think.

Ms. Suzanne Morin: To your question, if the $40,000 that the Canadian Marketing Association...which would be a trade association really trying to do the right thing, you can't just really wing it, because if you do, then you're subject to potentially being found to be not compliant. If the CRTC were to send back to individual organizations right away any complaint that they got, that would be an opportunity for organizations, small and large alike, to see what changes they need to make.

There are some things that a small organization would have to deal with. Once they got over how broad the definition is, they would have to look at the unsubscribe requirements. No one has an issue with unsubscribing, but we also have to add some of the managing consents, separate consents, for all the different elements. With the record-keeping obligations, which are fairly onerous, you have to be able to show at every instance which consent you're relying on and how you obtained it. There's the way they have to manage their lists. Once you have an existing business relationship, you leave.... I'm sending you emails for two years, but then after that, I have to stop because the law says to. It's all these little artificial things that get in the way of just everyday, appropriate business practices.

Those are some of the elements that small and medium-sized enterprises in particular would have to deal with.

Mr. Matt Jeneroux: Mr. Vernhout.

Mr. Matthew Vernhout: A lot of the compliance efforts and a lot of the consulting that I've seen done really focus on education. Sure, you need someone who understands the law, you need maybe a legal opinion on a few business practices, but there are lots of solutions, many free, many paid for. Obviously if you pay, you get better service and support to manage consent tracking, daytime tracking, even to manage the idea of taking screen shots at the point of data collection and tracking what forms look like. There are solutions out there. Not all of them are onerous to use; not all of them are expensive to use, either.

Is $40,000 for an organization a lot of money to comply? Honestly, I don't necessarily think it is for most mid-sized businesses. Smaller businesses, sure, but smaller businesses also tend to have very small email lists and they may very well know every person who's on their list, so they're not going to be necessarily looking at.... They know where their consumers come from. They have transaction purchase data; they have that history. It's just organizing it in a way that makes it accessible and easy to understand.

There was a question earlier in the panel around six-month implied consent versus two-year implied consent. All of those things are built into marketing automation platforms now. You can track the date the consumer subscribed. You can assign a flag to them to say this is a six-month implied consent, this is a two-year implied consent, an express consent. You can build the logic right into the marketing platforms that will either suppress those users when they've reached their end-of-life cycle or will notify those users, or build some sort of communication plan proactively into reaching those consumers before they reach their expiry.

The Chair: Thank you very much. Excellent.

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

● (1240)

Mr. Brian Masse: Thank you, Mr. Chair.

It's hard to believe how we got along in our economy without unsolicited email. I guess I take a different perspective. I get unsolicited advertising at my doorstep at my house. It goes in my mailbox and I can decide then to put it in the recycle bin. I suppose I've lost time doing that and I also suppose that I'm paying as a consumer and a taxpayer because I have to have that go to the landfill. A difference is that with my electronic device, as a consumer, that's a privilege that I actually can get that because I pay for the device, I pay for the constant servicing of it. Also, we can't forget the mere fact that one little unsuspicious email or unsolicited information could lead to a virus, a privacy breach. It could lead to exposure of your device now being basically a bot for spyware. It could be quite a cost for yourself and your family to recover that device. You have a whole series of things that could be affected. In fact, if you have to fix those things, it can cost you hundreds, if not thousands of dollars.

One thing that I think has been forgotten about is the third party spammers and the firms in the industry that are related to that. Mr. Vernhout, could you maybe highlight a bit about the third party industry that's created from just basically sending people information that's unsolicited?

Mr. Matthew Vernhout: Sure. There are the right ways to do third party communications and there are the wrong ways to do third party communications. CASL actually allows for both, unfortunately.

The right way that typical people will look at doing third party communications in regard to even the idea of list rental is similar to the idea of taking out a full-page ad in a newspaper. I will give you my advertisement, you will send it to your communication list because you have the proper consents and can manage the unsubscribes. I don't see any of the addresses until people choose to either take my offer or engage and give me some type of consent directly. That's the right way to do third party communications.

The other way really comes down to the idea of, “I have a list. Here you go. Please feel free to send it based on our contractual agreement.” That industry, right after CASL came into force, was studied by an organization in Toronto. They said the available number of lists to be used that way in Canada went from 400 to 14 because none of them had proper consent prior to CASL. When they were reviewed against CASL, that industry basically disappeared, actually probably accounting for a significant amount of unsolicited email communication also disappearing.

Mr. Brian Masse: There's a cost to all of this too on the other side.

Mr. Schwartzman, we haven't had a lot of testimony about this yet, but you mentioned our role with the rest of the world and with others catching up, to some degree, to some of this. I think that in the future for privacy, security, and other things, we should be looking at this to be built inside trade agreements. That's where I think we should be going if we want true efficiency.

You noted in your presentation where the OECD or others are going in international agreements. Can you highlight that a bit? I think it's important to define that we fixed Canada's being somewhat of an outlier, to at least no longer having that reputation. It was described as an outlier and a bastion for spammers.

Mr. Neil Schwartzman: That was one of my talking points, that we were the last country in the G8 to adopt an anti-spam law. It's embarrassing that some would like to do away with the law. It's an excellent law, and it's one that is respected as the best in the world among my colleagues.

Absolutely it could do with some adjustments, but in terms of the GDPR which is coming into effect May 25, 2018, we are about to encounter a degree of onerousness in data integrity that the world hasn't seen before, and that's a good thing.

The GDPR builds on the European privacy directive, which has been around for about a decade, with no teeth, with no ability to take punitive action. The GDPR gives countries the ability to force companies back into compliance, to respect the individual's right to say no, to be forgotten, to be left alone by marketers, or to willingly give that data to them and enjoy the benefits.

One thing that's very important is that the difference from the junk mail or the bulk mail that ends up on your doorstep is the marketer pays to get it there. They pay Canada Post to bring it to you. They pay for the printing. They pay for everything. Spammers do not. The recipients end up paying for that.

I'll talk about a small company here in Ottawa: striker.ottawa.on.ca was their domain. It's a consulting company that, for some reason, ended up on the spammer lists, and now they get one million spam a day. They've been driven out of business using that domain. There's not enough spam filtering in the world to compensate for that kind of flood.

We need to be a leader, and we are absolutely positioned to be such. I think it would be a matter of pride for everybody in this room that we can maintain parity with the EU.

● (1245)

Mr. Brian Masse: Ms. Morin, this is meant with all due respect, but with regard to CASL itself, it almost sounds as if we need a “CASL for Dummies” book to help clarify some of these things. All of us want to get rid of all that stuff. The whole point is to be more efficient.

I'm a Detroit Lions season ticket holder, so I get the Lions' email. Now I think I've signed something, because now canada.nfl.com starts coming to me without my consent, so I'm pretty sure they're connected through the NFL or whatever. I probably assented to it. There's a direct process for me to at least follow through with that, but it is taking up space.

Would a hard clarification so that everybody understood the rule book on CASL be a big step forward at this point? They're plain and simple, black and white, and then go from there. We're going to have another review of this legislation in the future as well.

The Chair: Sorry. We're going to move on.

Mr. Brian Masse: Okay. That's rhetorical, apparently.

Voices: Oh, oh!

The Chair: I'm trying to get everybody in.

Mr. Sheehan, you have seven minutes.

Mr. Terry Sheehan: It's a good segue to where I was going to begin.

Earlier I asked a question to our presenters from the Privacy Commissioner of Canada. In the presentation they mentioned some outreach and educational activities. I don't know if you were here or heard it. If you did, that's good. I would like your comments on that piece about their direction. Will that help bring some clarity? We heard earlier in testimony that there's a dispute whether or not a businesswoman can send an email to a businesswoman to go for coffee. Some say yes and some say no. Please comment on that, and then I have some further questions.

Ms. Suzanne Morin: As Commissioner Therrien explained, there is no doubt they have a very narrow and small piece of CASL that they implement, so obviously any sort of outreach they can do to clarify so that there is no inadvertent.... Being offside of those provisions would be helpful, but if we slide to the rest of CASL, which is where you're hearing a lot of the concern that we are expressing here today and from others who have come before us, yes, there have been a lot of people out on the road trying to explain CASL, but the guidance that organizations have been provided has not been sufficient to remove the fear and the chilling effect that being inadvertently non-compliant could result in something fairly onerous for your organization. That applies to large organizations, small and medium-sized enterprises, and charities as well. So yes, we are all for it, and we think any legislation needs it, so we definitely think there needs to be more, and it needs to be very focused.

We also need to get a message, separate from any changes to CASL, because we've made recommendations about some changes we might want to CASL. There needs to be a message about what the approach to enforcement is going to be. If you are an organization that is trying to do the right thing, "It's okay, don't worry, we can work with you to get you onside" is not the messaging they're getting, so they're spending a lot of money unnecessarily. They're developing a lot of processes that maybe they don't.... There is confusion, also, for individuals who are receiving these messages simply because of the way CASL has been structured.

You heard from Mr. Sookman, and Mr. Elder as well, that when you have a statute that prohibits everything unless it's permitted through exceptions and exemptions, you're offside if you can't fit yourself within those narrow exceptions.

That's some of what our members are struggling with when they are helping their organizations or advising organizations, big and small alike, and not-for-profits as well. That's what we're struggling with. We just want to get to a place where business can operate. We're not talking about the bad spammers here. We want to continue that. This is just about legitimate business trying to do the right thing, so more guidance would be great, but some changes to CASL as well.

● (1250)

Mr. Terry Sheehan: Just on that, then, there are little things we've heard in testimony, too. We heard from Rogers about how they want to have the ability to send a message that you're about to roam in an area outside of their zone. What kind of exceptions or changes could we put into CASL that would allow that legitimacy to go on?

As well, when I think of updates that are sent to you, which you're currently involved with, how exactly do we deal with the Internet of things for particular updates that companies want to be sent?

I'll start with Neil on some of those comments.

Mr. Neil Schwartzman: Let's make no mistake. Legitimate companies spam, too. They do, all the time. Matt and I have been doing it for 20 years. The amount of non-compliance among legitimate companies is high. CASL has put a stop to that.

On Internet of things updates, I think we could talk for hours, if you want to go to lunch. Your light bulbs should scare you. They really should. The amount of destruction that is happening as a result of IoT and the inability—not by law, but by connectivity—to update this stuff, I think absolutely should be a subject of investigation by this committee. I'd be happy to elucidate to that end.

We keep hearing about charities, but charities are specifically exempt under CASL. I don't understand what the onerous thing is. We keep hearing about the chilling effects of CASL. I don't understand how.... We have data that shows that there is more mail being delivered to Canadian consumers. It is being more effectively delivered, and our economy is growing, yet there is a chilling effect. I'm not feeling the cold; I'm actually quite warm right now.

You have to understand, in terms of the way ISPs work, we get complaints. Consumers hit, "this is spam", "this is spam", and "this is spam". We put a block up in front of, let's say, one of Matt's clients because Matt helps them to send.... They have to come to us with proof that they had permission to send anyway, so what CASL is asking for is exactly the same proof that is demanded of senders every single day of the week. If they don't have proof that you signed up to his list, I'd block them permanently so they don't get to send mail to Bell Canada or Rogers—the ISP side, not the marketing side—or any other network operator in the world. That happens every single day. It's been normal, standard operating procedure for decades.

Mr. Terry Sheehan: Thank you very much for that testimony. Obviously you guys are allowed to put into writing any further thoughts that you have on some of the questions that we don't have time to go to lunch on.

Frank, do you have anything further?

Mr. Frank Baylis: I have just a quick question on charities, because it's differing in what Mr. Schwartzman and Ms. Morin said. You say it does have an effect. Maybe you could explain that as you see it.

Ms. Suzanne Morin: It's how one interprets the exceptions. To the extent that the charity is not engaging in a commercial electronic activity, that part of the business is exempt, but then every once in a while they're going to creep into soliciting money. They're going to creep into things, and with the way the language is.... Again, you prohibit everything, and unless you fit within one of the exceptions, you find yourself in this spot, as a charity, where you're not quite sure if you can send out that commercial electronic message, and if you are going to send it, then you need to make sure you meet all of these different obligations. Making it very simple for a charity would go a long way to making it easier for them.

Mr. Frank Baylis: Can you respond to that?

Mr. Matthew Vernhout: Sure. I consulted with the Heart and Stroke Foundation. It is a former client of mine. They had no problems figuring out what part of their email programs were deemed to be fundraising messages, which are the messages that are exempt, and their commercial activity such as their lottery. They were able to absolutely separate those and treat them differently with regard to the activities of the business.

● (1255)

Mr. Frank Baylis: Can you explain it to me, then?

Mr. Matthew Vernhout: When they look at soliciting money in regard to their research and their programs, they are undertaking fundraising activities. In their view, and some of the other opinions they received, activities such as a lottery is a game of chance; therefore, it is not a fundraiser. It results in funds being raised for their organization, but because it is a game of chance it looks—

Mr. Frank Baylis: If I just ask, straight up to give me money, that's okay, but if I have a lottery or some fun way of trying to get money out of you, that's not okay. What about—

Mr. Matthew Vernhout: There are multiple interpretations.

Mr. Frank Baylis: What about "Come to my gala" or "Buy a ticket to my gala"? Would that be okay or not okay?

Mr. Matthew Vernhout: If the purpose of the gala is fundraising versus simply to host an event, then yes, if the funds are being used toward a goal or activity with a purpose. Simply buying a ticket to an event would be a commercial activity, however.

Mr. Frank Baylis: If it's "come to the event" and then extra dollars going to fundraising, I'm cool. Is that it?

Mr. Matthew Vernhout: I would say that would be open to interpretation, potentially by the CRTC.

Unfortunately, when I've asked them specifically about this as well, their answer tends to be that it's a case-by-case example when they look at the activities and the end goals, which I know is not necessarily the answer anyone wants to hear, but when you look at this as being a fundraising event versus being an event—

Mr. Frank Baylis: What's a charity doing other than fundraising?

Mr. Matthew Vernhout: A lot of funds get driven toward payroll and non-charitable activities as well. I suppose it depends on the activity of the charity.

Mr. Frank Baylis: I guess I'm out of time.

Ms. Suzanne Morin: If I could add quickly—

The Chair: Very quickly.

Ms. Suzanne Morin: The definition of "charity" and "not-for-profit" is not the same under CASL as it is under the Income Tax Act, so one opportunity, and it's in our submission, is to sort of make them the same. That may eliminate some of the confusion. The fact that we're here, and we can't even agree, and you can't understand shows the position that these charities find themselves in.

The Chair: I see a consensus of heads nodding, which is probably a good thing.

Mr. Neil Schwartzman: Yes.

The Chair: On that note, I want to thank our guests for coming in. It's been another great panel, which has taken us to a place where we better understand what's going on.

Thank you again for coming.

For the rest of us, this is just a reminder that on Thursday we have witnesses, and in the last 15 minutes we're going into committee business to discuss one of the motions. Then on Tuesday, 31 October, we'll have the Competition Bureau and the Office of Consumer Affairs, who are likely to be our final witnesses.

Thank you all. It's been a great day. Go out and play in the rain.

The committee is adjourned.