



HOUSE OF COMMONS  
CHAMBRE DES COMMUNES  
CANADA

# **Standing Committee on Industry, Science and Technology**

---

INDU • NUMBER 075 • 1st SESSION • 42nd PARLIAMENT

---

**EVIDENCE**

**Thursday, October 5, 2017**

—  
**Chair**

**Mr. Dan Ruimy**



## Standing Committee on Industry, Science and Technology

Thursday, October 5, 2017

• (1100)

[English]

**The Chair (Mr. Dan Ruimy (Pitt Meadows—Maple Ridge, Lib.)):** Welcome, everybody, to meeting number 75 of the Standing Committee on Industry, Science and Technology.

Pursuant to the order of reference of Wednesday, June 14, 2017, we are looking at the Canadian anti-spam legislation, CASL.

Today, we have Scott Smith, director of intellectual property and innovation policy at the Canadian Chamber of Commerce.

From the Desjardins Group, we have Ms. Diallo, senior legal counsel, as well as Natalie Brown, director.

From the Public Interest Advocacy Centre, we have Alysia Lau, external counsel for regulatory and public policy, and John Lawford, executive director and general counsel.

As an individual, we have Barry Sookman, partner with McCarthy Tétrault.

We are going to jump right into it. You will each have eight minutes to do your presentation.

We are going to start with Mr. Smith.

**Mr. Scott Smith (Director, Intellectual Property and Innovation Policy, Canadian Chamber of Commerce):** Thank you so much, and my thanks to members of the committee for having me here today. It's good to see you all again.

I'm here representing the Canadian Chamber of Commerce. I think you all know who we are. We represent a network of 450 chambers of commerce across the country, boards of trade, and over 200,000 businesses of all sizes, in all sectors, and in all regions. We're the largest business organization in the country. We also represent over 100 sector associations, so by extension we basically represent the views of the business community in Canada.

Since 1925 the Canadian Chamber of Commerce has connected businesses of all sizes, from all sectors, and from all regions, in pursuing public policies that will foster a strong, competitive economic environment that benefits business, communities, and families.

In 2014, making those connections became a little more complicated. I'll start by saying that none of the organizations I represent like spam. No one does, unless of course you're a spammer. If you regard spam as a massive intrusion of unwanted bulk email

advertising sent into your inbox by nefarious criminals lurking on the Internet, then 10 years ago spam was a big problem. According to Trustwave, which is a global services company, in 2008 92.6% of global email traffic was spam. By 2015 that number had declined to 54%. In 2016 it was back up to 59%. But here's the catch. In 2008 much of the unwanted messaging was reaching your inbox; by 2016 it wasn't.

Trustwave is measuring the volume of traffic entering their servers and comparing spam to legitimate messages. The spam that's filtered out never reaches you. In fact, the ISPs managing all of your email accounts have gone to great lengths and expense to build filters with sophisticated algorithms that achieve a 99% success rate in eliminating spam.

The real problem now is cybersecurity. According to Fung Global Retail and Technology, and IBM X-Force, the total amount of spam found with ransomware attachments in 2015 was 1%; in 2016 that number jumped to 43%. The bad guys found a new platform.

While there are tools in CASL that would be useful in going after these bad guys, the breathtaking scope of CASL clutters the digital landscape and distracts enforcement efforts away from the problems that really matter. The trouble is that CASL does not define spam as a massive intrusion of unwanted bulk email. The law applies to everyone. It applies to multinational companies, small businesses, trade associations, charities, and individuals, and it captures single messages from one individual to another. While the private right-of-action provisions in CASL have been delayed from coming into force, the provisions still represent a significant risk to the business community down the road, assuming that they do come into force at some time.

The law regulates electronic commerce by restricting the use of electronic communications media to send commercial electronic messages. In effect, the law requires the consent of a recipient to send an email, text, instant message, or any other form of electronic message unless the sender has a narrowly defined pre-existing relationship. The law does not permit the sending of an electronic message in order to obtain that consent, so if you want to email somebody to talk about a business venture, even if it's one-on-one you can't send an email asking them to meet you for coffee.

In essence, CASL places unreasonable limits on free speech, it stifles innovation, and it puts the competitiveness of Canadian business at risk. On February 19, 2016, the *National Post* published an article saying that Canadians could no longer appear on *Jeopardy!* The *Jeopardy!* organization couldn't send a note to prospective contestants because they were fearful of violating CASL. It's a glib example, but it's illustrative of the challenges that organizations face when attempting to do business in this country. The law has been in force for about three years now, and I still get frequent calls from businesses outside of Canada asking what CASL is all about. More often than not, the choice of these businesses is to avoid the Canadian marketplace, after they find out the rules.

• (1105)

We released a survey about CASL earlier this week. It will be in the field for a few more weeks. I'll paraphrase from one of the comments we've received back so far.

Prospecting for new business is very difficult. It is almost impossible to track how long you can rely on implied consent for a lead and how you can contact them. The record-keeping required is also very challenging. You need a screenshot of where the email address or contact info was published, and you need to know when. There is no one-size-fits-all, off-the-shelf technology solution to track records of consent. It means we must make a huge technology investment. This particular company says they've done a lot to become CASL-compliant, including investing in the technology and legal advice, and from a marketing perspective, they believe that they are onside. The challenge is the sales team, as they feel very uncomfortable with where they stand in terms of documenting, contacting, and prospecting for new clients.

I'll get into a few specifics. Organizations are struggling with CASL compliance in the following areas.

First, they are struggling with the definition of commercial electronic messages, CEM, which is exceptionally vague, and could inadvertently cover many messages that are not commercial advertisements or promotion of a commercial product or service.

Second, CASL does not permit the installation of a computer program without obtaining express consent. We believe this will have, or has had, unforeseen, negative impacts on consumers given the fact that data analytics is now a massive global innovation opportunity that's likely being darkened in Canada because of CASL.

Third, the information requirements for acquiring express consent are onerous, as the system asks for a voice recording, for instance, for verbal consent, and this will need to be stored, tracked, and managed over time.

Fourth, managing the deadlines around implied consent is too difficult. There was an effort to make things more efficient by allowing certain types of implied consent, but that implied consent expires. The reality is, when you have multiple levels of messages going through the system and consent is going through third parties, managing unsubscribes is very difficult.

Fifth, many of the exceptions are too vague. For instance, in section 3(d) of the CRTC regulation, it states that:

Section 6 of the Act does not apply to a commercial electronic message... (d) that is sent and received on an electronic messaging service if the information and unsubscribe mechanism that are required under subsection 6(2) of the Act are conspicuously published and readily available on the user interface through which the message is accessed, and the person to whom the message is sent consents to receive it either expressly or by implication.

Most small businesses won't even read that.

Sixth, the record-keeping standard is difficult to achieve. According to regulators, consent can be achieved not only by digital or written format, but also through voice. However, section 13 puts the onus on the sender to prove consent. This has created a predicament for businesses. Even if they acquire valid consent, they will be unable to document it in a sufficient way, forcing them to abandon the message in the first place.

Seventh, the private right of action, which I've mentioned, is still a concern among businesses. The likelihood of a business being drawn into a class action lawsuit, even if they are in full compliance, would be a significant burden on that business.

Eighth, there is an issue related to vicarious liability. Section 53 creates potential personal liability for officers and directors of corporations that violate CASL where due diligence is the only defence. We view this as extreme.

Finally, there is an issue related to proportionality. The punishments don't fit the crime. Compliance agreements that have been implemented by the CRTC to this point have imposed massive penalties on legitimate companies that had minor errors in their attempts to achieve compliance. Instead of following along with the due diligence argument when companies were attempting to do the right thing, the CRTC fined them hundreds of thousands of dollars. The same is true in the case of very small companies that had infractions. Yes, they were out of compliance, but a \$15,000 fine? This is a very significant amount of money for a small company.

I will wrap this up.

The government's objective in bringing this legislation was to “deter spam and other damaging and deceptive electronic threats such as identity theft, phishing”, and it “helps protect Canadians while ensuring that businesses can continue to compete in the global marketplace.” I would argue that CASL has not met that objective.

Disproportionate compliance spending hurts the Canadian economy. Businesses could be spending this money on innovation, hiring, marketing, and expansion, and I would urge this committee to take a stand on this legislation and make recommendations for a significant overhaul that will meet the objective of promoting a framework of effective electronic commerce in this country.

Thank you very much.

• (1110)

**The Chair:** Thank you very much.

We're going to move to the Desjardins Group with Ms. Diallo.

You have eight minutes.

**Ms. Aisha Fournier Diallo (Senior Legal Counsel, Desjardins Group):** Thank you, Mr. Chair.

[*Translation*]

Honourable members, on behalf of the Desjardins Group, thank you for inviting us to testify before your committee.

I am pleased to be here today to talk about something as important as the review of Canada's anti-spam legislation, that I will call CASL. It is an important piece of legislation for our industry, and it has a considerable impact on how we communicate with our members and clients.

As the Chair said, my name is Aïsha Fournier Diallo. I am senior legal counsel with the Desjardins Group, more specifically with its subsidiaries in property and casualty insurance that do business across Canada. My job is to support the validation of the legal risks associated with Canada's anti-spam legislation. Naturally, we are called upon to interpret the legislation every day.

Let me introduce Natalie Brown. She is the director of the caisse network and she leads a team that deals with credit card services, payments and litigation.

[*English*]

Although my remarks will be mostly in French, we will be happy to answer your questions in both languages.

[*Translation*]

First, I will say a quick word about the Desjardins Group because I would like to move on to CASL.

It was here, in Ottawa, that the idea for the Desjardins Group was born. Right next door, across the road, Alphonse Desjardins was a *Hansard* reporter for more than 25 years. After a debate on loan sharking, he got the idea to found a co-operative financial group that would address the needs of smaller depositors.

Today, 117 years later, the Desjardins Group is the largest co-operative financial group in Canada, and the 6th largest in the world, with assets of over \$270 billion.

Our close to 1,100 caisses and financial centres in Quebec and Ontario, together with our online platforms and subsidiaries from coast to coast, serve over seven million members and clients. It should be noted that a third of our service centres are located in less densely populated areas.

From heritage to insurance management, including business services, the group employs just under 48,000 employees and 5,000 managers.

That said, I would like to say what a pleasure it is to be among you today, honourable members, to share with you my point of view.

I came to Desjardins as a lawyer in 2013, about one year before the legislation came into force. I was able to witness the impact it had on what we do and how we communicate with our members and clients.

People's expectations towards communications have changed. Our modes of communication have also changed. Clients expect us to reach out to them in the most natural and effective way possible. You have to put yourself in the shoes of the consumer, which we do every

day since we are in contact with them. They want emails and texts, and are looking for an easy way to connect with us.

This is why organizations should be able to communicate with their clients and their members without having to constantly worry about whether they are violating a section of Canada's anti-spam legislation. With every message we send, we have to ask: does my email or text comply with the law? Is it a commercial electronic message, a CEM? Do I have the necessary valid consent to send it? Is it excluded under the legislation? Is the prescribed information included in the email?

Imagine having to do this every single time you send an email to a member or client.

In the past, the government said, "Canadians deserve an effective law that protects them from spam and other electronic threats that lead to harassment, identity theft and fraud." As Mr. Smith said, no one is against this. However, the law is far too broad.

People, like ourselves for instance, who work everyday with this legislation while trying to support our business operations have been anxiously waiting for this review. We hope that the government will take advantage of this opportunity to undertake an in-depth review of this legislation so that it may achieve its goal, while at the same time finding a balance that will allow organizations that have legitimate reasons to communicate with their clients to do so without fear and with the benefit of more streamlined legislation.

● (1115)

[*English*]

CASL is one of the most restrictive pieces of anti-spam legislation in the world. It was a great idea, protecting Canadians from spam. No one likes spam. But in our view, there has been a chilling effect on marketing and business communications, primarily for four reasons: the lack of clarity and the interpretive issues that exist in the act that require either clarification or amendments to the law; the fact that it is an opt-in consent model piece of legislation, meaning that you need an express or implied consent to send commercial electronic messages; the incredibly steep administrative penalties that the CRTC can impose for violations of the act; and the possibility of lawsuits from consumers through the private right of action.

The interpretive issues and lack of clarity make it difficult for lawyers like us to provide firm advice to their clients and for clients to be confident that they are in compliance with the law. There is no room for error under CASL, and all are extremely cautious, therefore missing opportunities to communicate with the clients for legitimate reasons, particularly in the one-on-one context. It should be easy for small businesses and larger ones to understand CASL and to apply it.

[*Translation*]

I am going to give an overview of the major interpretive issues we have faced these past few years, and we will provide you with a brief explaining them in greater detail, because there are quite a few.

First of all, the definition of a "commercial electronic message" is so broad that it includes practically any commercial message, even if the message is sent to a client with whom we have a perfectly legitimate commercial relationship.

As I said earlier, with every message, its content and the context in which it is sent have to be considered. You need to be aware of things like hyperlinks in the emails, clickable logos, in short, anything that could be seen as promoting the image of whoever is sending the email, and that includes a lot of things. For example, the fraud prevention email we would like to send to our members and clients could be considered a CEM because of the hyperlinks it includes. If a hyperlink leads to our website where our products and services are advertised, we have to ask whether it compromises the email by turning it into a CEM, which is prohibited.

The fact that our clients have to consult us before they send an email to their clientele with every new initiative and new campaign or innovation complicates things a great deal. We need more clarity to make sure that the nature of the messages we send, like the fraud prevention email, cannot be misinterpreted, even if they include hyperlinks, logos or elements that promote the Desjardins Group.

We feel it necessary to clarify the definition of CEM and to relate it back to the legislation's original purpose, which is to protect consumers from spam and the electronic threats that could lead to harassment, identity theft and fraud. Essentially, we need the assumption to be that Canadian companies have no ill intent when they communicate with their clients, and focus rather on the truly problematic communications.

I am now going to talk to you about the notion of consent and related provisions. As you know, the law requires express and implicit consent. Some of the provisions around implicit consent are a bit murky, and as a large financial group, we need to know who can benefit from this consent. Therefore, we recommend an opt-out option, that way, we would administer an unsubscribe mechanism instead of getting bogged down with consent management.

There is still one more area I want to cover. Earlier, Mr. Smith mentioned that subsection 6(6) is unclear. Indeed, some emails that shouldn't even qualify as CEMs are prohibited under this subsection.

Finally, I would like to mention the private right of action provision. We are very happy that it was suspended and we think it should be completely struck from the act. As a regulatory body, the CRTC can interpret the act. We believe that it is better to defer to such a body on matters of interpretation instead of overwhelming the courts.

● (1120)

I would like to thank you once again for inviting us to testify today. I sincerely believe it is possible to find a balance that would allow organizations to communicate more freely with their clients while at the same time protecting the interests of Canadians.

**The Chair:** Thank you.

[*English*]

We're going to move now to the Public Interest Advocacy Centre.

Mr. Lawford, the floor is yours.

**Mr. John Lawford (Executive Director and General Counsel, Public Interest Advocacy Centre):** Thank you, Mr. Chair.

The Public Interest Advocacy Centre, or PIAC, is a national, non-profit organization and registered charity that provides legal and

research services on behalf of consumer interests, and in particular, vulnerable consumer interests, concerning the provision of important public services.

PIAC has been active on the spam file since before the anti-spam task force was constituted in 2004. We testified before this committee in relation to then Bill C-27 in 2009 in support of the legislation. We supported the legislation as passed in 2010.

Our message today is simple. Canadians benefit from some of the world's strongest protections against spam. Canada's anti-spam legislation generally keeps business from sending spam unless the recipient has provided express prior consent and can easily unsubscribe. This is the great Canadian innovation. Trust consumers and citizens to control their privacy in the marketplace not marketers.

Has CASL been working for consumers? Currently, the CRTC is receiving about 5,000 complaints a week about email marketers not respecting CASL. One report from spring 2015 found outgoing spam volumes from Canada dropped 37% and overall email volume, spam and legitimate email, received by Canadians also dropped about 30% in the immediate period after CASL came into full force on July 1, 2014.

Since then Canadians have enjoyed the control of their email and other electronic communications by giving their consent to email, texts, and other electronic messages only to those companies with which they deal and by being able to unsubscribe from any email list that they wish.

Companies can still reach Canadians via email. There is no commercial email ban. Consumers buying products and services or who reach out to the company in question can expect two years of emails before the existing business relationship is deemed stale and the emails must stop. While consumers have a valid contract with a company, emails are allowed during the contract and for two years after that contract ends, unless of course the consumer unsubscribes on the handy link on each of these emails.

If a company does not follow these simple rules that put consumers in control, consumers can report the spam by completing a complaint form at [fightspam.ca](http://fightspam.ca). As mentioned, up to 5,000 consumers a week file complaints.

Spam still wastes consumers' time and reduces their confidence in electronic commerce, as it continues to deliver not only irrelevant, unrequested marketing but also deceptive and fraudulent messages and malware. What is different now is that the CRTC, Competition Bureau, and Privacy Commissioner of Canada can pursue companies for doing all these things.

Alysia.

• (1125)

**Ms. Alysia Lau (External Counsel, Regulatory and Public Policy, Public Interest Advocacy Centre):** Enforcement of CASL relies on a spectrum approach. The CRTC, which is the main enforcer, issues information on compliance, educates business associations, and then if there are problems, issues warnings, reprimands, seeks voluntary consent orders, and finally if necessary issues administrative monetary penalties, or AMPs.

In PIAC's view, contrary to the opinion of some of the other parties here today, CRTC enforcement of CASL has been very generous to offenders and in some cases, nearly to the point of being weak. Companies are given many chances to change their practices. When more stringent sanctions are required, AMPs are often set at well less than the maximum possible due to the consideration of many mitigating factors, which are outlined in CASL. I will add here that of the undertakings published on the CRTC website, only two exceed \$100,000. Those are for Rogers Media and Porter Airlines, which are not your typical or your average small businesses. Yet the CRTC does have the authority to impose an AMP of up to \$10 million per violation for corporations. Finally, all offenders are permitted to challenge AMPs before the CRTC, which can reduce, and has reduced, the recommended AMP.

The committee should also note that the government has apparently indefinitely suspended the bringing into force of the private right of action in CASL, which would have allowed consumers to sue particularly recalcitrant or aggressive spammers. Marketers, and in particular those marketers that act responsibly while attempting to adhere to CASL, therefore face little prospect of any significant AMPs or other sanctions.

**Mr. John Lawford:** We therefore find it disingenuous that representatives of companies and marketers are here today to say the CASL is somehow bad for consumers and commerce. Instead, we believe CASL is bringing some control to consumers in their electronic interactions with marketers and that consumers in control are more confident and better consumers. That should help commerce.

Instead, marketers are here to defend stale lists and lazy marketing. CASL sets reasonable limits on the contact that marketers can have with consumers without first asking consumers for permission to continue to market to them. That's all it does. It does not sabotage legitimate commercial relationships between consumers and companies.

Were CASL to be repealed or the consent requirements flipped to require consumers to opt out of marketing as before, then CASL would truly be useless. We would return to the days before the anti-spam task force and consumers' feelings of helplessness in the face of ever-increasing spam volumes. CASL now is working fine. We suggest you leave CASL alone.

If one thing has not been done right since CASL was introduced, it has been insufficient information gathering. Since CASL does not require spam volume to be reported by ISPs, although they may report it to the CRTC, Competition Bureau, or Privacy Commissioner, nor by the spam reporting centre, and CASL does not require that any of this information be made public or provided to Parliament directly, we are here today largely in the dark regarding evidence of the effect of CASL on spam and other electronic messaging. This committee could recommend a more robust and public spam reporting mechanism that would allow all parties and academic researchers to evaluate the effect of CASL upon objective evidence. That at present is sorely lacking.

PIAC thanks the committee, and we welcome any questions you might have.

• (1130)

**The Chair:** Thank you very much.

Finally, we're going to move to Mr. Sookman.

**Mr. Barry Sookman (Partner, McCarthy Tétrault, As an Individual):** I thank the committee for inviting me here today. What you are doing is very important. CASL is flawed and needs re-examination.

I am a senior partner with McCarthy Tétrault. I am also an adjunct professor of intellectual property law, and I am on the advisory boards of the Macdonald-Laurier Institute and CIGI. I am here today in my personal capacity.

I have been closely involved in CASL for many years. I appeared before this committee when it first examined CASL, and I pointed out that CASL was so flawed that it would, among other things, literally have made browsing on the Internet illegal.

I worked with officials trying to fix CASL at the committee stage. I was extensively involved in the regulatory process, the first and second consultations on the regulations. I made a personal submission to the committee.

I have been extensively involved in advising clients from all sectors of the economy, including large and small businesses, charities, the educational sector and other not-for-profits, the media, and software companies on how to comply with CASL.

I know what's happening on the ground and the impacts CASL is having.

CASL is, and is seen as, complex, disproportionate, and wrongly focused. To be frank, it is ridiculed by many organizations. It is particularly onerous for small businesses.

CASL's overbreadth makes communicating over networks illegal or legally uncertain in countless situations that Parliament could never have intended.

Let me give you a few examples. Take a start-up business that wants to use a public trade directory to email prospective customers and investors. This is most likely illegal under CASL, and it especially hurts small businesses trying to grow and develop new markets. To take another example, a person leaves his or her former employer to start a business or join another business and wants to email former clients, patients, customers, or former colleagues to let them know. Or the person wants to email an old schoolmate the person used to be good friends with. That is illegal under CASL in many cases.

It also deprives individuals of the valuable connections they have, which are important to their livelihoods, and it deprives recipients of information they would want to know. I would want to know if my doctor moved.

Say a charity or not-for-profit wants to continue sending newsletters to someone it has been sending them to even before CASL became law. If the newsletter is funded in part by the inclusion of only one ad, say, a vision correction device ad in a newsletter sent out by the CNIB, the charity likely has to cut off the recipient unless it can find a donation by the person in last two years or a record of obtaining express consent. Records weren't kept before CASL came into being. This deprives individuals, including the most vulnerable, from receiving information they want and need. It is also illegal under CASL to send an email asking people if they want to continue to receive emails, including from the CNIB.

Organizations want to send out Christmas cards to current and former clients, customers, and colleagues. They want to include a corporate logo and tag line promoting the organization. These items by themselves may make these cards CEMs, because they promote their businesses. If the recipients haven't expressly consented to receiving CEMs and haven't done business with the organization in the last two years, the cards likely cannot be sent. So much for Christmas cheer and keeping in touch.

A new online newspaper wants to send trial copies to members of the public. In the physical world, a publisher could leave complimentary copies in mailboxes. It's illegal online if the paper includes a single ad or if it asks people if they want to subscribe. This is especially unfortunate as it hampers establishing new media, something we need to foster in this world of fake news, as a healthy press is critical to our democracy.

There is a business-to-business exception in CASL. It has a number of conditions. It applies to organizations but not to individuals carrying on business as sole proprietorships. CASL operates in a discriminatory way for no good reason—in this case, discriminating and hurting small businesses.

• (1135)

CASL makes it illegal for a child to email neighbours promoting his or her lemonade stand, to ask if they want a babysitter, or to ask if they can mow their grass to earn a little school money. Its breadth is not subject to any de minimis or reasonable limitation. Do you want your kids not to be able to promote their lemonade stands?

A person wants to send a CEM using an SMS. Even if the person has consent to send the message, the person can't legally do it because the character limits don't enable people to include all of the

identification and unsubscribe information the CRTC regulations prescribe. The person might try to comply by including a hyperlink in the message to a website, but if the person doesn't have a website—which not every young small business has—and can't find a tool that lets them shorten the hyperlink, they effectively can't use SMS messages. CASL effectively impedes the use of the modern messaging systems it purports to regulate.

These problems all flow from CASL's flawed structure, which prohibits a broad range of communications subject to a limited number of exceptions. The computer program provisions also have many difficulties.

What's happened in the real world and not the theoretical world of those people who conceived of CASL? CASL has had no material impact on the purveyors of damaging and deceptive spam, spyware, malware, and other related network threats, which were the stated objectives of CASL. As a practical matter, the burdens fall on legitimate businesses. Many businesses have invested and continue to expend resources to comply with CASL, and it's not easy for the reasons Natalie Brown explained. Use of electronic messaging is chilled, because organizations don't know if they can send messages, and they are very concerned about the excessive AMPs that can be levied.

What should this committee do?

My most important recommendation for this committee is to assess all the provisions of CASL against the government's justification for it. CASL was repeatedly represented during the legislative process and the regulatory process as a law targeting the most damaging and offensive type of spam and malware, yet these prohibitions target ordinary commercial electronic messages and computer programs that have nothing to do whatsoever with malware.

Given that CASL impairs freedoms of expression in Internet communication, I urge this committee to recommend that CASL be recalibrated to what it was really intended to do, and that is to deal with the really bad actors.

I'll just say one more point because I realize, Mr. Chairman, that you have already given me a substantial indulgence, which I appreciate. If CASL were recalibrated, the CRTC could reallocate resources to deal with the real problems Canadians have. We have a real problem with cybersecurity and a real problem with malware. That should be the focus, not legitimate businesses like Desjardins that want to continue to communicate with their customers.

Thank you, Mr. Chairman.

• (1140)

**The Chair:** Thank you very much.

We definitely have a lot of information to go through today, so we are going to jump right to questions.

Mr. Jowhari, you have seven minutes.

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

Good morning to all of you. Thank you for coming.

This is a very important piece of legislation to me, because in my riding of Richmond Hill we have over 7,000 small businesses. The majority of them have one to four employees, and they use the Internet extensively to be able to promote their products and services. They don't have the budget to be able to hire a large marketing company. Therefore, this legislation directly impacts a large portion of the businesses in my riding.

Having said that, I just want to quickly highlight the area of interest I want to explore with each one of you.

Mr. Smith, you touched on cybersecurity, consent, PRA, and proportionality. I really want to start with cybersecurity with you. I have a question for each one, so if you could limit your comments on cybersecurity to about a minute, I would really appreciate it.

Can you expand the area of concern? You touched on it, and then you went to other areas such as consent. What's the concern with cybersecurity, and what's a recommendation?

**Mr. Scott Smith:** The concern around cybersecurity is that most of the messages that contain things like ransomware.... That's the big thing that we are hearing about right now. All of these breach.... There is personal information being stolen, and identity theft issues, but the big one is around ransomware, and it's going after businesses. From our perspective, that's the big concern.

I'd give you a statistic on the volume of messages that now have ransomware attached to them. They are coming from other countries; they aren't coming from Canada. The reality is that the anti-spam legislation is never going to touch or solve that problem by going after businesses in Canada. For the most part, they are not coming from here.

**Mr. Majid Jowhari:** Who is ransomware going after, specifically? We know it's coming from outside Canada. Which target audience is it going after?

**Mr. Scott Smith:** It's going after anybody who can pay.

**Mr. Majid Jowhari:** I have a large number of senior people in my riding, and they are getting attacked by these types of ransom emails. Is this something that we should be focusing on?

**Mr. Scott Smith:** Absolutely. There are a number of things that can be done to solve that, but not necessarily through legislation. There is education, an awareness challenge, and I think there is a certification option out there now that businesses could undertake, which would help prevent some of the attacks they are experiencing.

**Mr. Majid Jowhari:** Ms. Diallo, you specifically talked about lack of clarity, the consent model being very complicated, steep penalties, and the PRA. I want to go back to the lack of clarity. I know Mr. Sookman is saying, basically, that we should just wipe the whole thing and start again, but if you could help us.... Which area of the legislation do you feel needs the highest level of clarity?

**Ms. Aisha Fournier Diallo:** The first one is definitely the definition of CEM. It's too broad: any message that "encourage[s] participation in a commercial activity", including promoting the image of a person. That's much too broad. That would definitely be the first one.

**Ms. Natalie Brown (Director, Desjardins Group):** I would like to add to that. An email that facilitates, completes, or confirms a commercial transaction is deemed to be a CEM. I can give you two examples of emails that are sent in the context of sound business practices and that would fall under that definition.

We are an issuer of credit cards. If I want to alert by SMS the owner of the credit card that they are approaching their credit limit, or even surpassing it, I can't send it because it might be a CEM. As a co-operative, I want to warn my cardholder. That's a good, sound business practice.

Another one is under new technologies. I want to be able to offer electronic signature at a distance, and I want to send a password for the electronic signing session to my client, but the transaction hasn't been completed yet, and that's a CEM. It's much too broad.

**Mr. Majid Jowhari:** Perfect.

I'm going to go to Mr. Lawford. In your recommendations, you mentioned that one of the areas you are concerned about is insufficient data. Can you specifically tell us what data are missing, what data we should be collecting, and what the focus of that data should be?

• (1145)

**Mr. John Lawford:** There are a few spam studies out there, from the Netherlands and other places, where they've set up spam traps. There are emails that have never been used by anyone for anything, but researchers set them up, and they end up trapping only spam because they have never been used for legitimate email. The spam reporting centre doesn't quite work that way. It gets emails forwarded by Canadians who think something is spam. Then there is a third source, which is just ISP spam volumes, which I think Mr. Sookman told us about, where a lot of it is caught already.

There needs to be more coordination work at the CRTC enforcement end, to work with academics, ISPs, and their own enforcement people to give us a coherent picture. At the moment, a lot of it is presented in a very restrictive way, if you will, from CRTC. We have little scraps, but we don't have an overall picture.

It's hard for us to say.... For example, today I would have loved to come and say that since CASL, the volume of spam that consumers receive has gone down 35%. I can't say that. I don't know. It's hard to prove a negative.

**Mr. Majid Jowhari:** Thank you.

I have less than 45 seconds left, and I wanted to ask you a lot of questions. You specifically said, "complex, disproportionate, and wrongly focused", and a number of other things. I want to talk about "disproportionate". Can you expand on what you meant by that?

**Mr. Barry Sookman:** I'm glad to do it, and if I can in 10 of my seconds, I want to deal with the cybersecurity issue, because CASL makes it very difficult to combat the problems facing Canadians. Unless you're a telecommunications service provider you can't install computer programs that would combat a cybersecurity threat without express consent, and if you're a software provider, it's also illegal to transmit updates that would protect systems used by Canadians. So CASL could really be improved in that area to let companies protect their consumers.

**The Chair:** Thank you. I'm sorry, we're out of time.

**Mr. Majid Jowhari:** That's okay. That was a great clarification. Thank you, Mr. Chair.

[Translation]

**The Chair:** Mr. Bernier, you have seven minutes.

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

My first question is for Mr. Smith.

[English]

You said there's a lot of spam but the question is how much of this spam is coming to our inboxes? You were saying maybe 99% is not. Can you explain?

**Mr. Scott Smith:** The intent of that comment was to demonstrate that having CASL in place really hasn't had an impact on the volume of spam coming to your inbox. The ISPs are managing that for you. There's a technical solution to dealing with most of the spam that comes through right now, and companies like Microsoft and Google and others that are managing your email accounts for you are filtering out most of the spam that comes through the system. They're the ones spending the money to make that happen.

**Hon. Maxime Bernier:** So that's why the question is on cybersecurity now. If the private sector is successful in finding ways to prevent consumers from receiving spam, I don't think we need anti-spam legislation. The private sector is giving that to consumers.

But I'm very concerned, Mr. Sookman, what you said about cybersecurity; that this legislation is not helping. Can you explain it a bit more?

**Mr. Barry Sookman:** You're exactly right. The legislation, as the goals were articulated, was to help protect consumers against malware, spyware, phishing, and to the extent that it covers that, those goals are appropriate and CASL does address that. The problem is that by expanding the ambit of CASL, the focus is not on addressing the real problems. So we have the CRTC going after a company because they've failed to have an unsubscribe, or there was a bounce-back, and they didn't give effect to it, when they could be spending their technical resources in trying to protect Canadians against cybersecurity.

My point is that the act is too broad and it's unfocused and it's leading to unfocused enforcement by the CRTC.

On the computer program side, the prohibitions against installing computer programs make it illegal to do things that Parliament would absolutely want legitimate organizations like Microsoft and other big software companies to do. I lobbied very hard for that in the regulations, and we ended up with a very narrow regulation that

recognizes the problem but only if you're in a specific category. If you're in any other business, you can't protect your customers. We have to fix that.

• (1150)

**Hon. Maxime Bernier:** Can you tell me a little more about the exemption in the law that we are adding right now? You stated that adding exemptions in legislation illustrates that the legislation may have flaws. Could you elaborate on that, because as you know, we can extend the exemption, or if we have exemptions, it's because the legislation is not working. What is your view?

**Mr. Barry Sookman:** You ask a very good question.

There are two kinds of ways in which the problems with CASL can be addressed.

One is legislative, like the private right of action. Only Parliament can address that because it's in the legislation, and at some point, it has to come into force or be killed or amended.

Two, the Governor in Council has a very broad regulatory authority, and many of the problems Canadians have occur because during the regulatory process there was—I think—a too narrow approach in what the exemptions should be, and when you have a structure that says that everything's illegal unless it falls within an exemption, you have a problem. Imagine a criminal law that prevented you from going out at night except if you were going to work or school or coming to the committee. You're bound to miss some, and that means a lot of things are going to be illegal until the regulatory process can catch up.

So the approach that the Governor in Council should have taken, in my respectful view, is to have had very generous exemptions so the act would apply to things that really counted, but it wouldn't discriminate against small business. There was no need, for example, for this law to apply to businesses, to business communications, at all, because they don't want it, they don't need it, and they see it as stifling innovation.

One thing this committee could recommend is that the Governor in Council re-review the regulations so that some of these things that are blatantly causing problems can be fixed.

**Hon. Maxime Bernier:** About the exemption, as you know, in the legislation we politicians have an exemption. We're not under that legislation. I don't think it's fair. We are asking for the civil society to follow that legislation and for us it's not important. I think that if we are serious about it, we politicians must be under the legislation. If not, just repeal that law. What do you think?

**Mr. Barry Sookman:** You're exactly right, but if you actually look at that exemption, it applies to federal and provincial members who are applying. If you were, for example, trying to run for the leadership of a party, you'd be caught by CASL. But if you're running for municipal or regional government, you don't have the exemption so it discriminates very much in terms of the level of democracy that is protected.

I agree, nobody should have it...but in my view all politicians need to have it. It's essential for democracy that people who are running for office can reach out to potential constituents to be able to communicate their messages. It doesn't matter if it's federal or municipal, they should all be covered.

**Hon. Maxime Bernier:** That's a good point, I think we should keep that in mind.

I had that experience. I was running for the leadership of my party, and I was able to reach 65,000 people by email who were very happy to receive my email because they believed in the same values that I believe in. I was able to do that. But if I were in a non-profit organization, I wouldn't be able to explain my position and what I want to do.

I think the position of this committee must be to be sure that the politicians are under the legislation. If we're not ready to be under that legislation, we must repeal that legislation.

**Mr. Barry Sookman:** Technically, even one running for the head of a party does not have the exemption.

**Hon. Maxime Bernier:** It's all about fairness, and that's important.

**The Chair:** Thank you very much.

We're going to move to Mr. Masse.

**Mr. Brian Masse (Windsor West, NDP):** I would add that it might be debatable whether receiving a message from Mr. Bernier would be spam or not, but I'll leave that for others to decide.

**Voices:** Oh, oh!

**Mr. Brian Masse:** Before I get into comments, I was here for the original anti-spam legislation, and I think it's important to put some contextual element as to why it came about. I missed last week, but what I'm receiving here, at least the impression, is that this came out of left field, but that's not the case.

In 2004 there was, under the Martin administration, a national spam task force that went across this country and heard from businesses and from consumers and so forth, and they reported back unanimously to Parliament to act, because Canada was one of the few G7 nations without anti-spam legislation. We were the source daily of nine billion pieces of spam. In fact, countries that were comparable to Canada at that time were Nigeria, and other places like that.

Technology obviously has evolved, and I put forward the recommendation to review after three years. It was Conservative legislation that was put in place here. I'm glad that it is getting a review because a lot of things have changed. There have been some business elements that have changed with this, but also too, I think it's important that the cybersecurity element is looked at.

I see it differently in terms of approaching and how we got to this point. I see it as, I pay for this device. I pay for the ongoing service for the device. I pay for the use of it, and the maintenance, and if it gets infected by somebody sending something that I didn't want, or I didn't ask for, I have to be the person who loses my privacy, and has to pay for the cleanup. Sometimes the devices are damaged physically or damaged through the software. I have to pay for the

servicing, all those different things. I believe it's a privilege to send me marketing or consumer information. If I'm a customer of my bank, Canada Trust or something else, it's their privilege, it's not their right, to send me something.

I approach it from that perspective because it was also an economic issue. The mere fact that we had so many people trapped going through so many emails...and we all know in our offices what we receive. I come from the day, sadly enough, where your fax machine used to spit out the equal of that, and some people now say what's a fax machine?

My first question would be to Mr. Smith. One thing I have heard across the board here is the lack of understanding of rules. One thing I do like is a rules-based system of understanding exactly what is required and how. You read a good segment there with regard to that communication. If right now, we weren't to change anything with regard to the responsibilities or roles, how do you think that it could actually be condensed or what type of a playbook could be created to actually narrow it down so it's easier for businesses to really understand? We really want to get to the worst of the worst. Can that be done?

• (1155)

**Mr. Scott Smith:** I'll address a couple of your points in my response.

You're correct with regard to the spam task force, and I believe that even the Chamber of Commerce at one point was certainly in support of anti-spam legislation. That's a case of "be careful what you wish for" because we ended up with a piece of legislation that is breathtakingly large in scope. It covers basically every message that you could conceive of. If it's coming from a business, there is a likelihood that it is going to have some commercial content on it. Even if it's just in the signature block of a message, it has a link to a website, and suddenly that has become a commercial electronic message.

Our concern is about the scope, and narrowing the scope would solve a lot of problems. Taking one-on-one emails out of the equation, taking business-to-business emails out of the equation, would solve a lot of the problems.

I think most businesses that do email marketing or any kind of electronic commerce recognize the value of having an unsubscribe mechanism. There is no argument about that. If somebody doesn't want to receive messages, the businesses I deal with won't send any to them.

You heard from others today about the opt-in versus the opt-out. In the U.S. they have an opt-out system that works for the most part. It's not perfect, and I don't think we'll ever get to perfect, but I think the preference of business here would be to have a mechanism that allows them to communicate with their customers that first time in order to have the opportunity to opt out.

**Mr. Brian Masse:** That would be a clearer definition in terms of why you would be in and out of it.

My concern about that, though, is that if you don't opt out then you can have all kinds of different spam, and you could recirculate that and so forth, so there is an argument there. I think it's worthy, though, to examine the potential. I have some really big concerns about it.

Let's say, for example, my bank sends me an advertisement that I have to click off. It's similar to spam in mine. Let's say that it's TD Bank. If I go to my TD site, it asks me a million times if I want to receive a product, and before I get to my banking, I have to click to get rid of it.

I've paid with my time for that, and I've paid for the data consumption of that ad. I've paid for all of those things to get something I don't want. I could easily read and find out about their products as a customer. What gives them the right to have me bear a cost for that in terms of time and financial data management that I have to make a decision on something I haven't asked for? Shouldn't they have to pay for that if they're actually going to be using my system and my time since I haven't asked for that?

• (1200)

**Mr. Scott Smith:** I think most companies have a management system where you can subscribe or unsubscribe from various components of their messages, or you can unsubscribe from everything, and it's simple, one click. If that doesn't work for you and you continue to get messages, you have a complaint option, or you can just block the sender.

**Mr. Brian Masse:** That could also just be my ignorance, as a customer of TD Bank, so I'll have to look into that.

I have limited time, so I'll go to—

**Ms. Natalie Brown:** If you want to come to Desjardins, we have that service.

**Voices:** Oh, oh!

**Mr. Brian Masse:** With regard to the payday loans, I'm not sure you want me spending time on that issue right now.

Quickly, Mr. Lawford, with regard to this, if we just repeal everything now, what do you expect is going to happen?

**Mr. John Lawford:** The spam volume for Canadians will go up. What Canadians consider to be spam are messages that they don't want to receive, that are unsolicited. What this act does is flip it around. You have to ask consumers first. That's the point.

What they would start getting is unsolicited messages, and they would have no clue why they're on this list or why they're getting these messages. We'll just go right back to that.

**The Chair:** All right, thank you very much.

We're going to move to Mr. Longfield.

You have seven minutes.

**Mr. Lloyd Longfield (Guelph, Lib.):** Thanks, Mr. Chair.

I'm going to split my time with Mr. Lametti, who let me know he has a question he'd like to ask.

I was president of the chamber of commerce in Guelph when this legislation came forward. We had about 900 members, 100 of which

were non-profits. There were about 3,500 businesses, and 800 non-profit organizations in Guelph.

As a chamber, we tried to reach everybody, whether they were a member or not. Then, all of a sudden, we couldn't update the business community on business matters, federally, provincially, or municipally.

I'm looking to Mr. Smith on where the chamber network is at. I know in your testimony you talked about some of the chambers. Have they been involved with any of the complaints against businesses within their organizations that are spamming each other?

**Mr. Scott Smith:** I can't necessarily speak to whether they have been involved with members who have been spamming each other. I'm not aware of too many businesses that are complaining about spam. Most of the complaints that go through the complaint centre are coming from individuals who may or may not understand what the rules are about. If they get a message, they may be just complaining about getting a message without going through the unsubscribe process.

If there's a complaint, the reality is that it doesn't mean that there's a violation. To the point about understanding the statistics, that might be something you would be interested in, regarding how many of the complaints are actually valid.

To your point about not-for-profits and the ability to communicate with business, the chambers across the country were heavily involved in the discussion during the time when the regulations were being considered. We had a number of chambers that had written to their local member of Parliament concerned about how things were going to proceed. Then there was the follow-up on how to comply. That was a major effort on our part.

**Mr. Lloyd Longfield:** I was in one of those chambers. As we were trying to go through all the hurdles of implementing with all the small businesses, my members got a message from the Conservative Party of Canada and they said, "Why can they do this?", which goes back to Mr. Bernier's point, that politicians were exempt. It was kind of rubbing salt on the wound of some businesses that were pretty upset about regulations and then finding out that political parties didn't have to comply with their own regulations. That's just a general comment.

I want to come back to the proportionality question that Mr. Jowhari had. In just a short period, could we have a summary from Mr. Sookman on proportionality and whether this legislation is equitable?

•(1205)

**Mr. Barry Sookman:** I want to start by saying that I don't think it's unreasonable to protect consumers. I don't think it's unreasonable to have regulations affecting business that are necessary to protect consumers. At the end of the day, it's all about a balance. It's about a balance and ensuring that the goals are clear and the goals don't go farther than are needed and impose burdens that can't be justified by the incremental benefit to consumers. It's all a balance.

When you look at this legislation, since the definition of CEM is so broad, it's not capturing the kinds of things that are of concern. It captures the malware that might come in an email message, but it covers a whole lot of other things that are not necessary.

Regarding the consents, businesses in Canada all comply with PIPEDA. PIPEDA has a very stringent new requirement for expressed consent, but this legislation requires every business, every charity, and every non-profit in the country to now comply with two disparate regimes with consent...for two different systems. There's no need to have overlapping and different systems that businesses have to comply with. Even where PIPEDA has an opt-in, there is no way that a foreign spammer that is sending these kinds of malware has any consent under any system.

**Mr. Lloyd Longfield:** The foreign component is one that's a concern that I'm sure we'll be dealing with in our subsequent meetings as well.

I promised Mr. Lametti some time. We have just over a minute.

**The Chair:** You have two minutes.

**Mr. David Lametti:** Thank you, Lloyd.

I would like to ask a general question to Mr. Lawford and Mr. Sookman. Has the level of consumer sophistication changed since the legislation was originally passed and if so, how does that impact the balance to where we should be pitching any reform to the legislation?

**Mr. John Lawford:** I think CASL lined up consumer expectation with the law. Prior to this time, consumers wanted to have control. They thought that they should only get emails that they've consented to. Now, the law lines up with that. That's really my only way to answer your question.

If it's changed back to opt-out, people will think they have control and they won't. Their spam volumes will go back up and they'll start getting problems. That's the only way I can express my answer.

**Mr. Barry Sookman:** It's a good question, Mr. Lametti.

I'd have to say that it's hard to know. There's the good and there's the bad. Consumers obviously don't want to get this malicious type of spam. They may think CASL is the reason why they're not getting as much. Of course, the answer is that it's nothing to do with CASL. It's everything to do with the spam filters that the ISPs have.

Then you have other consumers who aren't getting the kinds of messages that they want. Like the people in the charities or like messages that educational institutions are sending to solicit students to join their programs. They may not know why they're not getting these messages. In some cases, they get dropped from the list and they wonder. In other cases, they don't know.

**Mr. David Lametti:** Thank you.

**The Chair:** You have about 20 seconds left.

**Mr. Lloyd Longfield:** To the group from Desjardins, the technical solutions are there. Are you relying on technical solutions as a company, or are you relying on legislation?

**Ms. Natalie Brown:** We're relying, in part, on technical solutions. The problem is that they're extremely expensive and, given all the different levels of exceptions and delays, they are almost impossible to manage.

I would like to address your point on disproportionality very quickly. I've had to face many boards at Desjardins, with great arguments to defend that something is not SEM. In those situations, given the number of sanctions and given the personal liability, we've had very strong cases that were completely denied just because they weren't willing to take that amount of risk. It's disproportional.

**Mr. Lloyd Longfield:** Thank you.

**The Chair:** We're going to move to Mr. Eglinski. You have five minutes.

**Mr. Jim Eglinski (Yellowhead, CPC):** I'd like to thank all the witnesses for coming out today and supplying us with this evidence and information.

Mr. Lawford, you're well outgunned today, but you brought Alysia with you, so you're a little balanced.

•(1210)

**Mr. John Lawford:** It helps.

**Mr. Jim Eglinski:** I'm finding a lot of contradictory information coming from the business side and from Mr. Sookman and Mr. Lawford. My questions are going to focus on Mr. Sookman and Mr. Lawford.

Mr. Sookman, a lot of your examples were theoretical. You mentioned charity newsletters. Then you mentioned Christmas cards being a targeted practice, a child with her little lemonade stand, and babysitting. Can you give me examples where that happened?

**Mr. Barry Sookman:** You're quite right about the lemonade stand. The reason I raise it is that it appears to me that everyone in the committee will understand that if a piece of legislation stops a kid from trying to get a babysitting job or operating a lemonade stand, there's something wrong with the legislation. That's the example, but it applies across the board. It's not just the kid with the lemonade stand. It's small businesses and sole proprietorships. It's everyone who's caught by the breadth of this legislation.

That example may be theoretical, but I can tell you that it's the kind of thing Canadians are concerned about. I have small businesses that come to me, start-up businesses, and they say, "We need to do x and y." It's not theoretical to them. It's real-world trying to build their businesses.

**Mr. Jim Eglinski:** I can understand that.

**Mr. Barry Sookman:** I tell them what they can do and can't do, and they say, "I can't do that. I cannot do that. I only have so many people, so many employees. Don't tell me I have to have a regime like Desjardins has to operate a small business."

**Mr. Jim Eglinski:** Mr. Lawford, you mentioned that the CRTC has been fairly light in its enforcement programs. There were three questions I asked Mr. Sookman. Have you known of any of those types of situations, where they've gone after people for these minor things? You can put an umbrella over everything, and you can say everybody's going to be dealt with the same way, but I don't believe that's happening, from what I learned from your evidence.

**Mr. John Lawford:** No, our view is that with the enforcement spectrum the CRTC is already using, they don't waste their time on very small situations. They look for patterns of behaviour, very egregious spamming episodes, ones where the company is completely recalcitrant and doesn't respond to entreaties or notices from the commission, before they get to fining them. They have cut down at least one AMP substantially before.

We're not talking about lemonade stands. We're talking about big businesses, large retailers, large banks, and large telecom companies that send millions of emails a day. What is happening is that the law is restricting that to a list that only has express consent or implied consent if you're already buying a product or service. That naturally limits the lists. It naturally limits trying to get new customers if you have not built up your own leads. The decision was made to put consumers in control from 2014 on. We think it's the right decision, because if there are many people competing to get your attention, that spam builds up, and the only way to counter it is to put consent on the consumer side rather than on the business side.

**Mr. Jim Eglinski:** I have a question for Mr. Smith.

What do you see as the most important part that we should be focusing on here? I can agree with you that we need to upgrade this policy and look at it, but what do you think is the most important thing to look at today?

**Mr. Scott Smith:** It was said earlier today. It's the scope of what exactly a CEM is. Narrow the scope. Give a definition, and allow business to conduct business. The business-to-business communication really needs to be pulled out of it.

**The Chair:** We're going to move to Mr. Sheehan.

You have five minutes.

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

There have been some very thought-provoking presentations. I'm glad we are reviewing this legislation, because we had a discussion as to whether or not we should. I'm glad we're doing this.

In particular, both Mr. Lawford and Mr. Masse mentioned the task force created in 2004 to take a look at the anti-spamming legislation.

If you all recall, there was another thing that was developed in 2004: TheFacebook, which became Facebook.

This piece of legislation is to regulate certain activities and discourage a reliance on electronic means of carrying out commercial activities. Fast forward to now with Facebook, Snapchat, Instagram, and all these new ways we're connecting with each other. How will this piece of legislation need to be amended to deal with social media?

• (1215)

**Mr. John Lawford:** Mr. Smith already provided you the answer. There is a CRTC regulation that allows closed-loop social networks: if they post the information about how contacts will be exchanged on the site, they're pretty much exempt from this. At the moment, they're not really covered when you're within Facebook. I believe that's why you're not getting Facebook appearing before you here to say this thing is impeding their business.

I know this because we fought against it. We went to the folks at Industry Canada at the time and said we think there should be some kind of control from this act within Facebook and these other platforms, and they said no. At the moment, it's pretty much fair game as long as they post the rules.

**Mr. Terry Sheehan:** Yes, because Facebook is developing exponentially as a marketer's opportunity. We all use it, even politicians, but the business community and chambers of commerce are using Facebook more and more to communicate with their members. It's getting more complex as it goes from just family and friends looking up an old high school buddy, to really developing your business.

I'm not sure what we should or should not be looking at as it relates to Facebook, because people are still getting unsolicited emails, in particular young people like my daughter. It seems generational. The generation of young people really aren't too concerned about all this sharing, in my opinion. It's anecdotal, yet someone like my father, who is a senior citizen, is very concerned. Some of them are clicking on various messages, whether it's Facebook or emails. They're getting those blue screens of death, if you will. That is a concern.

Another thing I wanted to ask about was particular exceptions related to small business. From the Chamber of Commerce, Scott Smith, do you have a number of chamber members who have been hit with this piece of legislation that you would know of through your surveys and could provide to us?

**Mr. Scott Smith:** I don't know if anybody has actually been hit with it. The question is more that they're unclear as to what applies. If you look at one of the small business exceptions, you're supposed to be able to send notices that are warranty related, related to a transaction, or required for legal or juridical obligations. At the same time, there's a regulation in there that says you have to add the unsubscribe mechanism in all the prescribed information. It should either be exempt or not. It's kind of halfway, which makes everybody question if it's a CEM. We don't actually know.

What ends up happening is they end up contacting their customers in other ways. They'll either phone them, or they'll put out an advertisement of some kind, or they'll contact them in a different way. They'll say, "We don't know what to do here, so we're not going to use that exemption."

**Mr. Terry Sheehan:** It's interesting. At our last meeting where we dealt with this, the CRTC mentioned they have opened about a million cases. In those cases, generally they send a letter. I suppose a letter could be snail mail or electronic—I didn't ask that—but it's sort of a cease and desist, like "Don't do that".

The question is: is that an effective form for dealing with people who are issued these things, or is it an educational thing from the federal government, where basically both the consumer and the person sending the spam aren't aware of it, and they make a mistake, and then they don't do it again?

**The Chair:** Just like that, you're out of time.

We're going to Mr. Maguire. You have five minutes.

• (1220)

**Mr. Larry Maguire (Brandon—Souris, CPC):** I want to thank all the presenters for their presentations today as well.

This is most interesting. I'm not a regular member of the committee, so I've found the discussions, examples, and so on pretty interesting so far. I appreciate seeing that my Liberal colleagues appeared to be concerned about the small businesses, but I notice that none of them wanted to extend the discussions around the concerns of small business that we've had, that being the one of corporate tax grabs.

But we're not here to discuss that today, so I'll move on.

**Voices:** Oh, oh!

**Mr. Larry Maguire:** I have a question for Mr. Lawford.

I just want to say, don't you think calling small businesses lazy, like you inferred in your presentation, is a little over the top? It sounds to me like the Prime Minister's comments about small businesses during the election when he said that people form small businesses to avoid paying taxes.

Given the concerns expressed by the other panellists, including one that represents all of these small businesses in Canada, do you think the concerns of the CASL that are being expressed are without base?

**Mr. John Lawford:** I didn't say that small business owners are lazy. They certainly aren't. I said that business practices where you are not getting consumers' consent post the law are lazy, and using old lists or buying lists that have no relation to your consumer base is a prohibitive practice, and that's what's lazy.

What should be the optimal environment, privacy versus business, is really at the base of your question, I think. The difficulty always faced when you're a legislator is trying to balance that public interest as expressed by different groups, and so business is quite right to say they want to just do business and we can trust them. The trouble is that we had 10 years of getting to this law, and it was pretty obvious you couldn't trust business because of the group send, if you will. There were so many businesses trying to reach people that the

overall tsunami effect on consumers was just too much. When it gets malware and other bad payloads mixed in with unsolicited commercial messages, it's a stew that's just impossible for the consumer to manage at the consumer end.

I didn't mean to imply that commerce is bad, as I said. We think that, if consumers are in control, they'll receive the messages they want, they'll buy the products they want, and two years after a contract ends is a pretty long tail to be able to continue to try to entice that customer back to do business with you.

**Ms. Alysia Lau:** If I may, I'll just add that the CRTC is also not just sitting on their hands and scrolling through emails and saying, "Oh, there's no unsubscribe button here, let's go after that company". All of their investigations are triggered by complaints, so these are Canadians who are taking advantage of the current regime and are filing submissions and complaints saying, "Hey, I got this. I didn't want it," or, "It was misleading; it was deceptive. Could you look into this?"

**Mr. Barry Sookman:** Mr. Maguire, could I respond to that question as well?

**Mr. Larry Maguire:** Yes, I would be happy to have you respond to that.

**Mr. Barry Sookman:** Very briefly, the problem for small business—and for large businesses, but for small business—is that this law is too complex. You have a law that's very difficult to read. You have two sets of regulations, and because of all the difficulty, you have a RIAS that is probably longer than every RIAS in history. You have guidelines from the CRTC. Every time I sit down I have to reread it because it's so hard to keep in your head because it's not logical.

I've been in rooms where businesses have tried to figure it all out, similar to the representative from Desjardins. You have 25 people in a room, including five lawyers, going through every kind of email that's sent and trying to figure out if it's a CEM, trying to figure out how you get consent, and trying to figure out if you have the right unsubscribe. It takes that many people to try to figure it out, and you still can't get it right. To impose that on a small business, where it's not understandable.... These small businesses are not securities lawyers or tax lawyers, and this legislation is that complicated. Leaving aside just how onerous it is to comply, which I've dealt with and others have dealt with already, it's so complex that the average small business cannot figure out what they need to do.

**Mr. Larry Maguire:** I appreciate that.

This question is for Ms. Brown and Ms. Diallo—and for Mr. Smith too, if he wishes.

You mentioned, Ms. Diallo, that you had three or four things we could look at, but I believe you indicated that some of them should be totally withdrawn. Or perhaps I will ask you that: are there some that should be?

• (1225)

**The Chair:** Be very brief, please.

**Ms. Aïsha Fournier Diallo:** I think I was referring to the private right of action.

**Mr. Larry Maguire:** Yes.

**Ms. Aïsha Fournier Diallo:** That for sure should be completely pulled from the law, in our opinion.

**Ms. Natalie Brown:** The CRTC is sufficient.

**Mr. Larry Maguire:** Thank you.

**The Chair:** Ms. Ng, you have five minutes.

**Ms. Mary Ng (Markham—Thornhill, Lib.):** Thank you very much. That was really informative.

My riding is probably not that different from those of some of my colleagues'. It's a mix of start-ups, technology companies, large organizations, Canadian headquarters for multinationals, and then people—seniors, consumers, and just people. I've heard a lot here, and I'm wondering if we could talk about that balance.

The work that we need to be doing as a committee, in looking at this legislation, is to really examine how we might improve it so that we can actually get to the objectives that are intended. We heard about cybersecurity. We heard about the increase in malware. That is, of course, alarming, but we also want to make sure that there isn't a legislative regime that will chill the effect of good business practices, good competition, and the ease with which businesses do what they need to do, which increasingly now is digital and electronic.

Mr. Lawford and Ms. Lau, there is some suggestion by others here to narrow the scope of definition of a CEM, and to therefore be more focused, alleviating some of the unnecessary obligations we've heard of in the legislation for small business owners and perhaps for start-ups. What do you think? Could that work?

**Mr. John Lawford:** We believe that the regulations in place and the exceptions referred to—warranty and that type of thing for contacting customers in the flow of a business relationship—are presently wide enough. If there are additional factors that have to be thought of, then doing that through a regulation is something that could be done quickly and easily. I don't believe you need to change the act or reverse the consent obligation on the consumer so that they have to opt out.

My concern is that small items will be blown up to completely change this act, and consumers then will bear the burden or the costs of pushing away spam, whereas we've decided to try to make the regime the other way. I'm not opposed to legitimate business concerns with compliance. The act has only been in place for three years. It's possible that there are some unintended consequences, but again, that would normally be done in the regulations, not by changing the act.

**Ms. Mary Ng:** Okay.

Mr. Sookman, you talked about how one of the unintended consequences of the legislation, particularly around cybersecurity, is the inability to help companies help create a greater digital environment in view of cybersecurity. In your view, or anyone's view, what could help in terms of any modifications to CASL that could actually help us do that better, and therefore protect consumers and people?

**Mr. Barry Sookman:** Those are good questions. If I could, I would like to spend just a minute on the question you addressed to Mr. Lawford.

One way of assessing the legislation is by comparing it to international norms. It was represented to this committee back when CASL was being reviewed that this legislation was the same as what was in Australia, the same as what was in New Zealand; that was incorrect. Although the law was somewhat modelled after that, the definition of CEM in those countries was closed, not open-ended, and the consents were not only expressed consents but included inferred consents without narrow, closed categories. If you look at international norms, even the closest norm we were trying to model was not in line with international standards. It was ratcheted up to make it even more of a straitjacket.

To get to your question, I think that is something somebody should really look at. In terms of cybersecurity, this is a problem with third parties inserting computer programs into systems and thereby hijacking systems, turning them into botnets or acquiring information, including—if you look at 142 million individuals' recent information in the Equifax case—2.5 million more. These are the kinds of things that the legislation does target, except that it doesn't permit the installation of programs where needed to combat cybersecurity.

I've always thought that, in addition to that, the legislation should actually permit the installation of counter-cybersecurity programs on the target that is attacking, in order to protect Canadians. I've also thought, as well, that ISPs should have the power to block foreign spamming sites and foreign malicious sites, to protect Canadians. It would be sort of an umbrella, if you will, to protect Canadians at large, as opposed to every ISP doing it or every organization doing it.

There's a lot that this committee could do, both with CASL and otherwise, to protect Canadians on cybersecurity.

• (1230)

**The Chair:** Thank you very much.

Mr. Masse, you have two minutes.

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

Mr. Sookman, you mentioned the CNIB in your remarks. I'm a former board of directors member for the CNIB. Can you specifically give me that? How exactly, and what case are you're referring to?

**Mr. Barry Sookman:** I'm giving you an example of a situation where a charity like the CNIB—

**Mr. Brian Masse:** Okay, so it was just an example.

**Mr. Barry Sookman:** I'm giving you an example.

**Mr. Brian Masse:** I just want to clarify that for the record, because I think it's something that the CNIB doesn't need to be dragged into individually as a brand—

**Mr. Barry Sookman:** But I have—

**Mr. Brian Masse:** I would move my questions to Mr. Lawford and Ms. Lau.

When we looked at the legislation in the past, there were bot spams, zombie computers, and a whole series of things that were done at that time. In fact, we had the first Facebooks at that time. We had to rely on U.S. prosecution at that time. If we reverse this and take that empowerment from the CRTC, do we then have to rely upon other prosecution for fines and penalties? What happens then?

**Mr. John Lawford:** At the moment, the CRTC is working hard with other jurisdictions to try to cross-pursue, if you will, spammers on both sides. If the legislation is changed significantly to do with insulation of programs, they'll just have that many fewer tools to go after people pushing malware in Canada. It takes time for the enforcement authorities to work up their connections with foreign counterparts. They're concluding an MOU, as I understand it, and starting new work on that. It's going to take some time, but weakening the act won't help them with that goal.

**Mr. Brian Masse:** Do I have any time left?

**The Chair:** You have about 15 seconds.

**Mr. Brian Masse:** Ms. Brown, do you have 10 seconds of Desjardins positive stuff we could...?

**Ms. Natalie Brown:** How could we narrow the—

**Mr. Brian Masse:** Really quickly, would efficient, more well spelled-out rules be an important step forward so that it wouldn't take a big meeting to figure out the rules?

**Ms. Natalie Brown:** Absolutely, narrow the scope. There's an exemption in the law, which is a partial exemption that allows us to send without consent but requires us to have "unsubscribe". All of those definitions should not fall under the definition of CEM.

**Mr. Brian Masse:** Beat 'em up.

**Ms. Natalie Brown:** Beat 'em up.

**The Chair:** Thank you.

We still have more time for questions. We're going to do one each around the table for seven minutes.

Lloyd, I believe it is you first, and you'll share your time with Eva.  
[Translation]

**Mrs. Eva Nassif (Vimy, Lib.):** Thank you, Mr. Chair.

I am new to this committee. I am replacing my colleague Frank Baylis.

I would like to thank our six witnesses for their presentations, all of which were quite informative.

Ma question is for Mr. Sookman. I am the member for Vimy, a riding in downtown Laval that's home to many small and medium-sized businesses.

Not only did you mention that CASL should not target our SMEs, you went even further.

In your post dated June 7, 2017, you said, "You should instantly sense something is wrong with a law if it could make kids promoting lemonade stands to their neighbours or trying to get a babysitting job, or a person recommending a dentist to an acquaintance, illegal." However, the exemptions provided for in CASL and its regulations—family relationships, personal relationships and recommendations—would potentially apply to each of those cases.

In your opinion, should we broaden the scope of the exemptions provided for by the act and its regulations? Further, should we include new exemptions from the act's prohibitions?

• (1235)

[English]

**Mr. Barry Sookman:** Thank you very much for the question. Being from Montreal, I appreciate the question in French, although I cannot respond in French because my French is too rusty.

**Mrs. Eva Nassif:** You can answer in English.

**Mr. Barry Sookman:** With regard to your astute question about whether the exemptions apply or not, the problem is that there was a regulatory process that could have led to the exemptions applying.

There's an exemption for personal relationships. Personal relationship as it's defined as an exemption, a message from one person to another, is so narrowly confined that it really is someone who has an existing relationship and, pretty much, is exchanging views as a best friend. It doesn't include a situation where a person who lives on the same street sends a message to the friend's mother, for example. It's too narrow. It could easily have been broadened.

The family relationship doesn't permit the sending of CEMs to grandparents or cousins. It could easily have been broadened. A lot of these examples... I did this one on whether you could actually recommend a dentist over Christmas. It just occurred to me. Could I actually recommend a dentist to somebody? Under the law as it appeared, it was impossible. It made me think it made no sense.

That is the kind of thing that could be addressed if the GIC regulations were revised. They could have a de minimis exception. They could more broadly define what is a personal relationship or a family relationship to take those kinds of situations, which should never be illegal, out of play.

[Translation]

**Ms. Natalie Brown:** I would add that we should keep in mind that the general rules of statutory interpretation call for a restrictive interpretation of these exemptions. In other words, despite the provided exemptions, we often end up having to stick to a restrictive interpretation, even when the intent is broader.

**Mrs. Eva Nassif:** Thank you.

[English]

**Mr. Lloyd Longfield:** For the record, I'd just like to ask the Canadian Chamber of Commerce a question.

When you have the survey results, could those come in to the clerk so that we can use them as part of our study?

With regard to Australia's CEM definitions or others that might have been used in the previous study, maybe Mr. Sookman could send those in so that we can see some best practice examples of CEM definitions. That would be very helpful.

**Mr. Barry Sookman:** I'd be glad to do that. There is one other thing this committee might want to see. There is a charter challenge of CASL before the CRTC, and that charter challenge very explicitly identifies, both in the submissions and in the expert reports that were filed for the applicant, some of the problems with CASL.

If this committee would like me to file those materials, I'd be glad to provide them to the committee.

**Mr. Lloyd Longfield:** Thank you. We're learning from you, so we really appreciate your coming in and doing that and offering that.

Ms. Brown, let's go to the other side of things and think of vulnerable Canadians—seniors, people who can be targeted by commercial enterprises—and how they might be protected from being targeted. We have a lot of stories in the media about shopping channels and things that really go after seniors' savings.

Is there any way that we could address seniors and vulnerable Canadians, and still protect business-to-business communications?

**Ms. Natalie Brown:** I can speak only for our business, and seniors are a large part of our business in Quebec.

Don't forget that we're under a tremendous amount of regulation. Our regulatory authority is the AMF, which checks for sound practices. We're under the Consumer Protection Act. There are various ways to protect seniors. Mr. Sookman mentioned personal information protection. We have all sorts of consents in place under those laws, and there are various other protections under consumer personal protection that protect seniors very well.

• (1240)

**Mr. Lloyd Longfield:** Thank you.

I'll share the rest of my time with my colleagues across the way.  
[Translation]

**The Chair:** Mr. Bernier, You have seven and a half minutes.

**Hon. Maxime Bernier:** Thank you.

My question is for the officials from the Desjardins Group.

You mentioned that there is a need for data and to maintain a database in order to show compliance. In your estimation, what are the costs incurred by the Desjardins Group in order to comply with CASL? How many employees do you have in each of Desjardins' networks working on this?

I imagine that you are currently doing your best to be in compliance. Do you think that small companies have the same resources as Desjardins to ensure compliance?

**Ms. Natalie Brown:** First, on the issue of the cost of compliance, we will have to forward you that information at a later date. We never bothered to establish a grand total.

Furthermore, having chaired the Desjardins Group's anti-spam committee, as Aïsha is doing now, I can tell you that we are talking about several dozen employees, since we have to include every branch, every caisse and every aspect of compliance, from legal

affairs to operational risk. I will forward you this information as well.

On your second question, now, as to whether smaller companies can bear these kinds of costs, I would have to say that it would be unrealistic to think so. The Desjardins Group is a massive company, and even despite that, we feel the burden is much too heavy to bear. I think that more than answers the question.

**Ms. Aïsha Fournier Diallo:** We need to remember that every email and every piece of electronic communication we send is subject to the law. We need to ask the question every single time.

We need to ensure that everything is ready so that our 48,000 employees and 5,000 managers know what to do. It is not difficult to imagine how a small business might not have the resources to validate all that.

**Hon. Maxime Bernier:** Thank you.

It would be useful for the committee to have that information on the number of people that ensure compliance with the act in the various departments and on the cost of ensuring compliance.

**Ms. Natalie Brown:** Of course.

**Hon. Maxime Bernier:** Thank you.

[English]

I have another question for Mr. Smith about individuals... Canadians who are having issues understanding this legislation. Can you explain a little bit more about this?

**Mr. Scott Smith:** There are individuals within businesses who are having trouble understanding it. Mr. Sookman described this fairly explicitly in a previous question, but essentially, you have multiple layers of text that you need to be able to follow. The act is very prescriptive, so you need to follow it very closely. Then you need to follow the regulations that came through Industry Canada. You need to pay attention to the CRTC regulations, to what the Competition Bureau has put out in terms of guidance, and to what the Office of the Privacy Commissioner has put out in guidance. You need to read the regulatory impact statement to get some understanding or context of why the law is there in the first place. Then you need to read the guidance from the CRTC, which in many cases hasn't been that helpful, because it doesn't give you a lot of guidance.

The problem is that the CRTC is both the enforcement agency and the guidance agency. The challenge for businesses in going back to the CRTC for guidance is that as soon as they open the door to say they have a problem, it opens the door to an investigation.

From a business person's perspective, if you are a small business and you have four or five employees, you as the business owner are likely the person who's going to be responsible for figuring out how to comply with this at the same time as running your business and dealing with all the other regulations that come across your plate.

When we're saying they're having difficulty complying... They're having difficulty understanding the definition of a CEM, why they can't send a message to their neighbouring business saying, "Let's go for coffee." They don't understand it.

**Hon. Maxime Bernier:** What about Canadian consumers? As you know, there are a lot of complaints at the CRTC. We had a civil servant before us a couple of days ago.

You said before that you think maybe they are not real complaints. Can you explain a bit more about that?

**Mr. Scott Smith:** What I suggested there is, just because there's a complaint, it doesn't necessarily mean there has been a violation. We don't know what those complaints actually look like. Maybe there should be some type of reporting back from the CRTC where these complaints are valid or these complaints are not valid. We don't understand that right now.

From our perspective, our businesses want to protect their own customers. They want to protect consumers, and there are ways of doing that.

There was a code of practice developed long before CASL came into play. That code of practice dealt with things such as making sure you are active on activating unsubscribes, for instance, or how the wording in the unsubscribes should be characterized. Most of the businesses I deal with were compliant with that code of practice.

•(1245)

**Hon. Maxime Bernier:** Thank you.

Jim, you can take my time.

**Mr. Jim Eglinski:** Thank you.

Mr. Sookman, during your presentation you talked about more generous recommendations. I would like to get a little clarification, because Mr. Lawford stated that he thought the CRTC was fairly lenient. I know as a former policeman that if I had allowed everybody to go down the highway 15 kilometres over, as they probably do on Highway 401 here, everybody would go 124 kilometres an hour, and after a little while the speed limit would be set at that.

Would there not be a tendency for people to push the system? Can you tell me where you were going with that statement?

**Mr. Barry Sookman:** That's a very good question. I did a very extensive blog post in terms of what I thought the structure should be for considering regulations.

In my view, it starts from looking at the structure of the act. The structure of the act prohibits a large swath of activities. You may not communicate electronically something that's in a category that's very broad, and then it has a very close list of exceptions. Recognizing that this impacts free speech, and commercial speech, is exceptionally important for Canadians, because free speech lets Canadians have information they need to make better choices. It also promotes competition in the marketplace.

Recognizing the value of commercial speech and that it is protected by the charter, and recognizing the structure of CASL, my point—when I talked about generous regulations—was not loopholes. My recommendation was, having regard to the way in which

the legislation is structured, one had to recognize that there were going to be a myriad of situations that could never have been contemplated when you ban, take a "ban all" approach.

That's why my recommendation was, in the case of doubt, we should not be trying to prohibit things that could in fact be advantageous and needed by Canadians. That doesn't mean in any sense of the word that we should have regulations that would permit malicious computer programs to be disseminated or the things that the government said they were really concerned about.

When I say generous, the regulations should have been viewed having regard to the freedoms that Canadians are entitled to and that are necessary for the proper operation of a competitive marketplace.

**Mr. Jim Eglinski:** Thank you.

Thank you, Chair, for being generous with his time.

**The Chair:** No problem.

We're going to move to Mr. Masse, for seven minutes.

**Mr. Brian Masse:** I'll ask everybody to respond to this.

We had a recent stay of part of the legislation for individuals. Whether you're an individual and a private citizen or you're a business owner, there was recourse.

In your opinion, what recourse is there for people? If I go out and spend my money to buy a device, some of them up to \$1,000, I'm going to pay fees of \$50 to \$75 a month for it. It's going to affect the way I interact with my family and with my business and it can have other consequences on my privacy. It can have other consequences in terms of how I maintain contacts for emergencies, and so forth. I've chosen this as my primary communication device.

What recourse is there, then, in terms of what has been stayed? Whether you agree or disagree with the private thing, why should there be a reduction of that privilege to protect oneself in terms of the argument? Why either reduce the protections or not allow that for private citizens? What gives somebody the right to unsolicitedly use my investment, my time, and my materials, and expose me to privacy concerns without being requested to do so?

I'll start with Ms. Brown.

• (1250)

**Ms. Natalie Brown:** Of course, if we could have the privilege to have you as a customer, the purpose we aim for with the emails we want to send.... Obviously some are commercial, obviously some may be useful to alert you to fraud, to transactions that are being done in your account, if they're more commercial in marketing. My point as a business owner is to send you the most personalized, useful information that's targeted to your needs. And by doing that, I believe we're saving you some time by sending you information that you want.

**Mr. Brian Masse:** Your business might be doing that, but if I haven't solicited that relationship with you, if we get rid of what we're doing here, it just comes in as it used to, through bots and through phishing and other things. That's my concern.

Once we've engaged in that relationship with Desjardins—and thank you for the work they do, I'm not trying to pick on you by any means—and in fairness to my bank, they give good service when I go in there. As a customer I hate some of the things they do. But that's my choice at the end of the day. My concern is that a consumer can eventually choose that, and I do that. I accept the fact that my bank takes advantage of my data and sends me unsolicited information that I pay for. I have that choice.

**Ms. Natalie Brown:** Under the current regulation, that can still be sent because technically the bank has your implied consent. So those emails you're talking about are permitted today.

**Mr. Brian Masse:** But there's control in that. If somebody does it right now and it causes me a virus, I can go to the CRTC and demand recourse, and now we've had a stay as part of the legislation to protect you on that.

**Ms. Natalie Brown:** I think the objectives of the law are exactly those that you mentioned, and with good clear definitions, that could still be attained.

**Mr. Brian Masse:** Thank you.

I'll let people carry on.

**Mr. Scott Smith:** I think we need to be careful about conflating different types of messages. I don't think any of us would argue that it is important to manage emails that come through with malicious intent. So if there are ransomware attachments, if it's being sent through a botnet and it's attacking your system, it makes sense to have some legislation in place that allows enforcement agencies to deal with that. I think what we're talking about is messages that customers want. From a business-to-business perspective, there needs to be a certain amount of freedom to be able to conduct that business, to be able to prospect. If specific bulk emails are going to advertise a broad cross-section of people who may or may not have an interest, that's a different story.

**Mr. Brian Masse:** Mr. Sookman.

**Mr. Barry Sookman:** You asked a good question. First,, the fact that the CRTC is there and prosecutes and publicizes prosecution does have some impact on behaviour. Contrary to what my friend said, I think some of their fines have been very high relative to the alleged infraction. Specifically on your question about the PRA, which is a good one, I don't have a problem with a private right of action in a calibrated piece of legislation. If the private right of action was effective against the people who were providing the malware,

the spyware, the phishing problems—the real bad actors everyone agrees on, assuming you can find them and go after them—I have no objection to that. Nor do I have an objection to letting ISPs, which are bearing the brunt of dealing with this, have a right of action against the people who are the purveyors of the 99%. The problem I have is that when you have a piece of legislation that's extremely onerous, that's ambiguous, and we have the potential for class actions, we're creating a monster that is going to be very expensive for Canadians to address.

I applaud the government to have suspended the PRA while this committee does the work it needs to do. If, at the end of the day, the recommendation is to recalibrate the loss but it targets the things that it truly was intended to target and it has a PRA, so be it. Throw the book at these bad guys. I don't think anyone around the table disagrees with that.

• (1255)

**Mr. John Lawford:** I think we agree with you that consumers should have control, and that's what you're talking about. I own the device and I pay for the connectivity. That's the way the act is set up now. If it turns to opt out, consumers lose control. What you're going to get, if you lose control, is unsolicited commercial email. There's not only bad spam and malware, if you want to talk about illegal. There is also unwanted, unsolicited, commercial email, and the act covers that as well. That's an element of control that chafes against the thought that businesses should be able to contact people out of the blue. We support the control of consumers in that.

As for the private rate of action, it would have been a complementary aspect because, as I said in our remarks, a recalcitrant or aggressive spammer, somebody who's been told to stop over and over again, clearly fined in the past and continues to do so, or who is a hard-core spammer, needs to have the threat of millions of dollars outside of the administrative regime because some of those just can't be handled by the administrative regime. We've seen people set up shop in Canada who are very hard core.

I'll just end there.

**The Chair:** Thank you very much.

We have about two minutes left.

Ms. Ng.

**Ms. Mary Ng:** I'll make this really quick.

I think it was never the intention of the legislation to not enable good business practices. I think it was never the intent to not encourage start-ups to be able to start and be successful or to be so cumbersome to small businesses that it impairs the ability to operate. I certainly think that the intent of the legislation was to deal with a real issue at hand, and indeed, it needs to continue protecting consumers and achieve that balance.

We have work to do as a committee. What would be enormously helpful is if the witnesses across the table would be able to, with that view in mind, send submissions to us because we're not going to have time to do this verbally. Maybe you can provide submissions about the solutions in addition to what you've already said, because obviously we have that. There may be practical solutions that we should be looking at that we can be focused on so we don't throw the baby out with the bathwater but really do something here as a committee to address the very bad and have the tools to do that. We

could manage the way that we protect consumers without having a chilling effect on overall competitiveness, because that's not what we want.

I think that where you could be the most helpful to us—and we're going to ask this of everyone—is to give us those ideas. I think government and this committee would welcome that.

**The Chair:** Thank you very much.

That was a really great session. There are lots of things for us to consider. I'm glad that we had the two opposing views here today. It really opens it up for where we need to go.

I'd like to thank everybody for their comments and their presentations. It will be an interesting study.

This meeting is adjourned.

---





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

---

### SPEAKER'S PERMISSION

---

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

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

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

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

---

Also available on the House of Commons website at the following address: <http://www.ourcommons.ca>

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

---

### PERMISSION DU PRÉSIDENT

---

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

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

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

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

---

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : <http://www.noscommunes.ca>