HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 076 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, October 17, 2017

Chair

Mr. Dan Ruimy

Standing Committee on Industry, Science and Technology

Tuesday, October 17, 2017

● (1105)

[*English*]

The Chair (Mr. Dan Ruimy (Pitt Meadows—Maple Ridge, Lib.)): Good morning, everybody. We're a couple of minutes behind. We're going to just jump right into it today.

We are continuing with our study on what I am going to call CASL, Canada's anti-spam legislation, today.

Today, we have, as individuals, Michael Fekete, partner at Osler, Hoskin & Harcourt LLP; Michael Geist, Canada research chair in Internet and e-commerce law, faculty of law, University of Ottawa; and Adam Kardash, counsel, Interactive Advertising Bureau of Canada.

Representing organizations, we have from the Information Technology Association of Canada, David Messer, vice-president, policy, and finally, from Rogers Communications Inc., Deborah Evans, associate chief privacy officer.

Thank you all very much for coming today. We have a busy day with lots of witnesses. You'll each have about eight minutes to present and then we'll get into our lines of questions.

We're going to get started with Mr. Fekete.

Mr. Michael Fekete (Partner, Osler, Hoskin & Harcourt LLP, As an Individual): Thank you very much.

I'd like to start by thanking everyone for inviting us to speak on what I think is a very important issue.

I'm the co-chair of the technology group at Osler, Hoskin & Harcourt, and we advise a broad range of clients, from start-up technology companies to some of the largest companies in the world. What we've seen with CASL is legislation that has really challenged us, both in terms of advising clients and in terms of having clients who want to comply with the law but who truly have difficulty understanding what's required and fitting what the law prescribes into a business reality.

My perspective is that, although very well intentioned, CASL is flawed. That really stems from the fact that it's overly complex, very prescriptive, and very broad. I think it's really important to point out that it undercuts some other very important public policy objectives. I'll name just a few.

CASL has increased cybersecurity risks because it places restrictions on when updates and patches can be installed to fix security issues and vulnerabilities.

Also, it has unlevelled the playing field among Canadian businesses, including many of the technology companies that we're looking to support and to see become global players, because it creates a regulatory burden that competitors in other markets don't face.

We see this in the installation of computer programs. If you set up operations in Canada, you need to comply globally with the rules in CASL in terms of any installations you might send to your users or install base, whereas if you're in the United States or another jurisdiction, it's only the installations made on computers in Canada that need to comply.

This isn't a trivial point. The rules with respect to computer programs are quite complex, and they're unique. They're very much made-in-Canada rules that are not reflected in the laws of other jurisdictions.

I think it's fair to say that CASL creates unnecessary red tape and compliance costs. At a time when we're looking to see how red tape can be reduced, you could say that CASL goes in the opposite direction. It's really the small businesses that bear the brunt of this red tape, in that they have difficulty understanding what the law requires, and they're having difficulty using the most efficient means of communicating—which is electronically—with their customers.

There's also a question as to whether CASL is constitutional. There's no question that it impinges upon free speech. The questions a court would ask are whether the restrictions are proportional to the harm, and whether the restrictions minimally impact on the right of free speech enshrined in the charter.

I think that when we look at CASL's regulatory reach and prescriptive rules, we can say that full compliance becomes next to impossible. There's no shortage of circumstances in which you can say that it doesn't make sense to comply with the rules in the context of day-to-day business operations.

I think this is exemplified most strongly in the computer program provisions. I'm a technology lawyer. I work very closely with technology companies that are trying to comply with the rules. Again, these are unique rules. No other country has adopted rules as broad as the ones found in CASL, or as prescriptive.

The real question is this. When these rules were conceived, it was really in a world of laptops and hand-held devices, but we've moved to a world where the Internet of things is the buzzword. We have devices that are permeating all of our different day-to-day interactions. Many of these devices do not have user interfaces through which you can request consent. Many of the manufacturers of devices, whether they be automobiles, fridges, or TVs, do not have a direct relationship with consumers, and that makes the request for consent challenging.

I can provide a few other examples of where CASL creates just really practical problems. The question is whether it's sensical to require companies that sell online exclusively—they're online businesses—to provide an unsubscribe mechanism in the transactional messages they send to consumers. You're confirming a transaction that you've just completed and you must, under the rules in CASL, include an unsubscribe mechanism.

Essentially, that leads to confusion for the lawyers, the companies, and consumers. I'm providing this example because it highlights how prescriptive CASL is and the way that prescriptive rules, however well-intended, don't necessarily have the intended effect.

We can look at text messaging, in which we have a very limited number of characters available to us. Because CASL prescribes exactly that contact information, identity information, and an unsubscribe mechanism need to be provided, you're really not left with anything to communicate to consumers vis-à-vis text messaging.

It's also important to ask how effective CASL has been at addressing spam, spyware, and other online threats. The truth is that we have very little empirical information, so there's very little that we can point to in terms of statistics to show the impact. A 2015 report published by the security firm Cloudmark is often cited. It did an analysis of email traffic in Canada following the coming into force of CASL. Interestingly, it showed that there was a reduction, but the reduction was largely due to decreased use of messaging by legitimate companies. I don't think that was the intent of the legislation. We're trying to encourage digital activities, not reduce them.

What other things can we say about effectiveness? We know that phishing emails remain very prevalent and the related cybersecurity concerns are growing, and growing for good reason, because this has become an epidemic. So we know that CASL hasn't been effective at preventing those types of risks. We also know that enforcement by the CRTC has largely been against legitimate companies rather than against the bad actors, the fraudsters.

We can then ask ourselves how we got here, with well-intentioned legislation that has had a questionable impact on fighting the harmful spyware and spam that the legislation was really intending to address. I think we can look back and say that there was broad three-party support for the legislation. There was largely support from industry, from civil society, and from academia, since fighting spam and spyware is a critical objective. However, I think we can also be truthful and say that it hasn't been a success. There has been a chorus of complaints about the complexity and the prescriptiveness, and about how it doesn't work in practice. We want legislation that encourages participation in commercial activity, and we can't say that CASL has facilitated that.

The opportunity today is for all three parties and all stakeholders to work together and to identify fixes. I'm going to identify four fixes very quickly.

First, the regulatory reach of CASL needs to be narrowed. We need to focus on harmful spam and spyware, and we need to be very clear that this is the intent and purpose.

Second, we need to ensure that there's a meaningful implied-consent exception. Rather than having a prescriptive rule, which is the way it's expressed today, we need to introduce flexibility. As with our federal privacy legislation, PIPEDA, we need an approach to applied consent that's based on a contextual assessment of whether it's reasonable. This will in no way undermine the efforts to fight the harmful stuff. Rather, it will introduce the flexibility that business needs.

Third, we need to reduce the prescriptiveness. There is too much in the way of prescriptive rules for what we can clarify through general principles.

Fourth, with respect to the private right of action, rather than having standing to sue left with anyone who receives a message that doesn't comply, we should provide the companies that are in a position to go after the bad actors the opportunity to supplement the efforts of the CRTC and place standing to sue in their hands.

Thank you for your time. I look forward to receiving any questions.

● (1110)

The Chair: Thank you very much.

We're going to move on to Mr. Kardash for eight minutes.

Mr. Adam Kardash (Counsel, Interactive Advertising Bureau of Canada, As an Individual): Thank you.

Good morning, everyone. First of all, I would like to thank you, Mr. Chair and members of the committee, for the opportunity to speak with you today.

My name is Adam Kardash and I am here on behalf of IAB Canada, a not-for-profit association dedicated exclusively to the development and promotion of the rapidly growing digital marketing and advertising sector in Canada.

IAB Canada represents over 250 of Canada's best-known and most respected stakeholders in the digital advertising and marketing sector, including advertisers, agencies, digital publishers, social media platforms, and ad networks. Our members include numerous small and medium-size enterprises.

To put it simply, CASL requires significant amendment, so the work of this committee is very important to IAB Canada, as CASL impacts every one of IAB Canada's members. Our trade association has been closely and actively involved with CASL for years, including through formal submissions on CASL regulations and meetings with government officials, and through hosting CRTC information sessions for our members.

My brief introductory comments this morning are based on my experience as counsel to the IAB as well as my personal capacity as the head of Osler, Hoskin & Harcourt's national privacy law practice. Our team, together with our firm's technology practice, led by Mr. Fekete, has dealt with hundreds of mandates involving CASL across all sectors, in particular the digital marketing and advertising sector.

The main theme of my comments this morning is that while CASL was intended to build trust in the digital ecosystem by deterring spam, malware, and other nefarious activity, there is widespread acknowledgement that there are serious and fundamental issues with CASL's regulatory framework that need to be carefully considered and appropriately addressed, mainly by significant amendments to the statute.

We're offering the following three recommendations for the committee's consideration with regard to the changes necessary to CASL's statutory regime.

First, we urge that the committee, in its review of the act, focus on narrowing the incredibly broad scope of CASL's application. In our view the expansive scope CASL's framework is fundamentally flawed. Instead of just targeting nefarious activities, CASL is structured to regulate virtually all electronic messaging activity. CASL could be effective if it applied only to bad actors or egregious activities, as opposed to regulating wholly legitimate messaging activities that nobody considers unwanted, let alone spam.

By way of just one example, consider that CASL doesn't just regulate marketing and promotional messages. Rather, the statute, as my colleague Mr. Fekete just mentioned, applies even to certain administrative or transactional messages that provide solely factual information about an account, a product recall, or even safety. Stunningly, CASL requires that such messages contain an unsubscribe or opt-out mechanism. This is totally confusing for consumers and businesses. Nobody would ever consider these types of messages to be spam, yet companies that don't offer an unsubscribe option for these types of administrative messages would be technically violating the statute.

CASL definitely needs to be amended to expressly exclude these and other wholly legitimate types of electronic messages from the CASL regulatory regime. CASL's broad scope has resulted in an incredibly and unnecessarily complicated statutory regime, as legitimate electronic messages are subject to the consent, notice, and unsubscribe requirements and penalties under the statute unless they expressly fall within one of the several highly technical exceptions set out in the regulations.

From our day-to-day experience, it can be a very time-consuming, complicated exercise, and, for small businesses especially, an expensive undertaking to interpret and navigate CASL's provisions in this regard.

Moreover, in terms of scope, while the display of online advertisements is not subject to CASL as the display of an ad is not sent to an electronic address, statutory clarity of the scope of application in this regard is critically required. CASL simply cannot apply to the display of online advertising, because it would be practically impossible for organizations involved in the online advertising ecosystem to comply with the act's prescriptive requirements.

In our view, without question, the scope of CASL needs to be clarified and could be appropriately narrowed without imperiling CASL's intended goal of fostering trust.

Second, we urge the committee to recommend the elimination of unduly prescriptive and technical requirements in CASL that are either ambiguous or, often, very impractical to implement and totally unnecessary in order to achieve the policy objectives of the statute.

● (1115)

One example for the committee is that when an organization is seeking express consent, CASL requires organizations to provide a whole bunch of specific and detailed contact information and a statement about how individuals can withdraw their consent at any time.

This may sound like a totally innocuous requirement, but these requirements are more strict than what's required for a valid express consent under privacy legislation and they pose very practical compliance challenges when, for instance, companies seek a valid express consent over the phone or in person, such as at a retail store when you're just trying to get out of the checkout line.

These and other unnecessary notice requirements need to be removed from the statute. They don't benefit consumers, and there's no reason why a company should be exposed to regulatory enforcement, let alone class action litigation, for failure to comply with a technical requirement by providing a statement that says you can withdraw your consent at any time. It makes no sense. These are technical and wholly immaterial violations of the statute as currently constructed.

We urge the committee to recommend that any consideration of the issues raised by CASL be done through the application of CASL's provisions to very specific-use case scenarios.

We cannot overstate the significance of this suggestion. If you examine the actual impact of CASL on legitimate, daily, electronic messaging activity, you—and not just you but also ISED—will see through real-life examples on a case-by-case basis that there will be a drastic need to address a myriad of very impractical, ambiguous, technical, and unnecessary provisions. Over and over again the application of case studies sheds light on this.

Third, we want to make a specific recommendation regarding the private right of action. As was anyone who has actually spent time trying to comply or to help companies comply with CASL, IAB Canada members were very grateful for the deferral of the private right of action coming into force.

In short, CASL in its current form with the PRA, the private right of action, is a perfect cocktail for unnecessary litigation. CASL's overly expansive breadth of application, prescriptive technical requirements, ambiguous drafting, and the right to sue with no proof of harm would have set the stage for plaintiffs' counsel to commence a stream of class action litigation, including meritless and frivolous class action lawsuits. There's a payday for plaintiffs' counsel in such class action activity.

IAB Canada is strongly urging the committee to carefully review the private right of action, including narrowing the PRA as a remedy only in circumstances involving bad actors and particularly nefarious and egregious violations of the act.

I'll conclude my introductory comments at this time. On behalf of IAB Canada, I thank you again for inviting me here this morning. I would be pleased to answer any of your questions.

● (1120)

The Chair: Excellent. Thank you very much.

We're going to move to Mr. Geist.

You have eight minutes.

Dr. Michael Geist (Canada Research Chair in Internet and E-commerce Law, Faculty of Law, University of Ottawa, As an Individual): Thanks very much.

Good morning. My name is Michael Geist. I'm a law professor at the University of Ottawa, where I hold the Canada research chair in Internet and e-commerce law. I served as a member of the national task force on spam and appeared before this committee in the development of CASL. As always, I appear in a personal capacity, representing only my own views.

The hallmark of fraudulent spam, from get-rich-quick schemes to body-part enlargement promises, is that while it contains something that seems unlikely, people still often want to believe the claims. Over the last several years we've experienced something similar with respect to anti-spam legislation, in which the claims of doom often just don't add up.

A perfect example is the frequent suggestion that somehow the neighbourhood lemonade stand would be affected by CASL. Now, stop and think about this for just a moment. Politicians admittedly might be an exception to this, but how many of us have email addresses for all of our neighbours? How many would think to actually not only collect all of those email addresses, but then email the entire neighbourhood about a lemonade stand? Like spam, it takes a claim with a kernel of truth—the need for consent to send commercial messages—and then moves into a world of fantasy. Long-standing scare tactics, ones that pre-date even the drafting of the legislation, are not the way to assess this law.

In my view, there are really three questions that lie at the heart of the assessment of CASL: Is there a harm or risk that needs to be addressed? Does CASL help solve the problem? And even if the answers to one and two are yes, is the law still too onerous?

Let me try to answer all three.

First, is there a harm or risk to be addressed? I think the answer to that is obvious: absolutely. Let me point to three examples. First, malware, spyware, and phishing attempts have emerged as exceptionally important cybersecurity issues and they are caught squarely by CASL. Today these efforts may be state-sponsored or simply criminal. Consider the impact of phishing attempts in the last U.S. election that successfully gained access to thousands of emails at the DNC and may have helped change the course of U.S. political history; or the massive malware cases such as WannaCry, which have affected millions, caused millions or even billions in damages, and put hospital and banking systems at risk. We need effective laws to counter these threats, and they are unquestionably part of CASL's ambit.

Second, I think we all recognize the importance of e-commerce. The success of e-commerce depends on trust, trust that our information will be used appropriately, and trust that online sellers will deliver what is promised. The concerns associated with fraudulent spam extend beyond just the losses that can occur from those individual messages. They undermine the potential success of all e-commerce activities by undermining trust more broadly.

Third, the public is increasingly aware and, I would argue, concerned with their privacy and the use of personal information. Our major trading partners, particularly the EU, have tried to address these concerns through tough new laws. CASL isn't separate and apart from PIPEDA; it is a foundational part of the legislative response to the risks of misuse of our personal information. At its heart is the need for informed consent, a standard the establishment of which is long overdue.

Now, does it work? I would start by saying I wish we had more data. I think the failure to collect extensive data is a serious mistake by officials who should have been working with the spam research centre, Internet providers, email service providers, and law enforcement to collect data. The need for more data provides a reminder that the work of policy-makers doesn't end just because the legislative process concludes. There are, however, several studies and reports that provide valuable data on the impact of CASL.

The committee already heard from Mr. Fekete about the 2015 Cloudmark study, which found significant declines in spam, with 29% less email in Canadian inboxes, and a 37% reduction in spam originating from Canada. I'd be happy to debate and explain why that's actually a good thing.

Further, one of the core concerns about Canada's anti-spam framework before CASL was our inability to co-operate actively with global enforcement actions. Our task force heard that without a comparative spam law, Canada risked becoming a spam haven, without the legal ability to assist partner countries in investigations and enforcement. CASL has unquestionably addressed this issue, ensuring that Canada is no longer an island in the fight against spam. We have international enforcement agreements with four countries, and MOUs with 12 agencies in eight countries. But perhaps most telling—and I don't believe the committee has heard about this yet—is the ROKSO list, the register of known spamming organizations, which is maintained by an organization known as Spamhaus. The ROKSO list identifies the top 100 spamming organizations, which are responsible for 80% of the spam worldwide. I have to tell you that the existence of this kind of list came as a surprise to me and to many other spam task force members, as it confirmed, surprisingly I think, that we actually know where the leading spammers are.

Further, we learned that Canada was a notable home for these spamming organizations.

● (1125)

When CASL took effect in 2014, Canada was home to a disproportionate number of spamming organizations, with seven of the top 100 spamming organizations in the world located in Canada. Today, three years later, there are only two remaining. There may be several factors behind the decline in the top spamming organizations in Canada, but the existence of a tough anti-spam law with real penalties is surely one of them.

This data confirms CASL's effectiveness, and in this regard it should be emphasized that the goal of the law was never to eliminate all spam from our inboxes. No law can do that, just as no technology can eliminate spam or fully protect us from malware, spyware, and phishing. Rather, the goal was to reduce the spam that originates in Canada with the hope that other countries would do their part. In that regard, the law has been a success.

Finally, is the law overbroad? I have to say that CASL complaints have always struck me as a bit odd. The complaints typically focus on the many exceptions in the law, claiming they are too narrow, restrictive, or difficult to interpret. The real narrowness has often come from the interpretations that have been provided.

Consider the issue of charities. ISED Minister Navdeep Bains stated the following in the press release announcing the decision to delay the private right of action: “Canadian businesses, charities and non-profit groups should not have to bear the burden of unnecessary red tape and costs to comply with the legislation.” But the CASL regulations state that section 6 of the act does not apply to a commercial electronic message sent by or on behalf of a registered charity, which has as its primary purpose raising funds for the charity. In other words, charities already enjoy a broad exemption under the law.

Similarly, the committee has already heard from others about the supposed need for a business-to-business exception, yet the law already states that this section does not apply to a commercial electronic message sent to a person engaged in a commercial activity consisting solely of an inquiry or application related to that activity. That exempts legitimate business-to-business commercial electronic messages.

I'd say that even this focus on exceptions is misplaced. Businesses rely on exceptions where they don't want to comply with the foundational obligation that is in the law: consent. The law is clear: if you get informed consent, there is no need to go searching for an exception to apply to your activities. When you hear complaints about narrow exceptions or calls for more, that complaint is fundamentally about the ability to use that personal information without informed consent by leveraging an exception. I'd say that's bad policy and bad for privacy.

To conclude, these remarks aren't meant to suggest we can't do better. We need better data; we need better awareness of the Spam Reporting Centre; we need the agencies to engage more directly with businesses about the true requirements of the law; and we need better enforcement, including the private right of action. I would also suggest that we need a strong anti-spam law with real penalties that is based on informed consent to deal with a very real threat. That law is CASL.

I look forward to your questions.

● (1130)

The Chair: Thank you very much.

We're going to move on to Mr. Messer.

Mr. David Messer (Vice-President, Policy, Information Technology Association of Canada): Thank you, Mr. Chair and committee, for having me here today.

I'm here on behalf of the Information Technology Association of Canada. ITAC is the national voice of Canada's information and communications technology sector. There are over 37,000 ICT firms in Canada, employing almost 600,000 Canadians.

The ICT industry is uniquely positioned to provide comments on CASL. The industry includes telecommunications, online, and IT companies that are both on the front line fighting against spam and spyware and dependent on electronic messaging and the installation of computer programs as core elements of their businesses.

While the legislation under review is commonly referred to as CASL, or Canada's Anti-Spam Legislation, it's important to consider the full objectives, as stated in section 3, which are:

> to promote the efficiency and adaptability of the Canadian economy by regulating commercial conduct that discourages the use of electronic means to carry out commercial activities, because that conduct

(a) impairs the availability, reliability, efficiency and optimal use of electronic means...

(b) imposes additional costs on businesses and consumers;

(c) compromises privacy and the security of confidential information; and

(d) undermines the confidence of Canadians in the use of electronic means of communication to carry out their commercial activities

While spam is part of it, the central goal of the legislation is really to promote and grow the digital economy and to encourage businesses and consumers to embrace electronic means of communication and commerce.

The idea is to clear the pipes of junk so it's easier and safer for everyone. The interests of the ICT industry are very much aligned with these public policy goals. However, to date, there is little objective evidence that CASL has led to either a decline in malicious forms of spam or an increase in confidence in electronic commerce. We do know that phishing, ransomware, and other cyber-threats remain very prevalent and we know that enforcement of CASL by the CRTC has largely been against legitimate companies, with an absence of targeted enforcement against true malicious spammers or other bad actors. We also know that CASL has imposed substantial administrative costs on businesses across the country.

CASL is complex and confusing, with highly prescriptive rules, heavy fines, and aggressive enforcement by the CRTC. Organizations of all sizes need to devote considerable resources to understanding the rules and maintaining compliance. It is so complex that CASL consulting has become an industry unto itself, which is certainly an unintended consequence of the legislation.

Confusion breeds risk aversion, and the experience of our members has been that CASL discourages Canadian businesses from innovating or adopting new technologies. Enforcement actions by the CRTC only exacerbate this aversion, which creates a chill in the industry without providing useful guidance so that other companies can avoid the same mistakes.

In addition, the often overlooked computer program provisions have created risks to consumers by inhibiting companies from installing updates to protect against emerging cybersecurity threats. While the regulations include limited deemed consent exceptions, they do not go far enough, and ultimately they undermine the legislation's objective of making consumers more secure.

The software provisions are especially unworkable when we consider the quickly emerging Internet of things, as Michael mentioned. Many software-controlled devices coming into our homes and workplaces have no user interfaces, and the global companies that design and sell them often have no direct relationship with the consumer, which makes CASL compliance extremely difficult.

To address CASL's unintended consequences and to help it meet its stated objectives, ITAC proposes five themes to guide amendments.

First, the justification for CASL has been articulated as targeting damaging and deceptive spam, spyware, malicious code, and other threats. Amending CASL so that it targets only these harmful activities would go a long way to addressing CASL's unintended consequences. This can be accomplished by narrowing the definitions of three terms: computer program, commercial electronic message, and electronic address. In ITAC's written submission, we will include outlines of specific proposals regarding how we think these definitions should be narrowed.

Second, the circumstances in which express consent is not required should be expanded. CASL combines prescriptive express-consent rules with narrowly drafted exceptions. This combination creates complexity and rigidity that make compliance exceptionally difficult and costly when compared to compliance with anti-spam laws in other jurisdictions, such as the United States or Australia. Amending CASL to include an implied-consent principle, similar to Canada's privacy law, PIPEDA, would help to remove the unnecessary regulatory burden created by CASL.

● (1135)

Third, we should make CASL less complex and rigid. Canadian businesses should not require a lawyer to determine whether they're in compliance with CASL. CASL's overly prescriptive rules, including the rules governing requests for consent and the content of messages, should be replaced with general principles, similar to Canada's privacy law. By following the approach found in PIPEDA, businesses will be free to innovate in how they communicate specific information to consumers, and the CRTC, the Office of the Privacy Commissioner, and the Competition Bureau will have room and flexibility to provide guidance.

Fourth, CASL should be amended so that businesses in Canada are on a level playing field with competitors in other jurisdictions. The computer program provision in CASL should not apply, for instance, to programs installed on devices in another jurisdiction if the installation does not violate the law in that jurisdiction. Further, the red tape and regulatory burden caused by CASL's prescriptive rules should be minimized and, where appropriate, harmonized across borders.

Last, as mentioned previously, the private right of action, which combines broad standing to sue and statutory damages, creates the perfect conditions for frivolous class actions against legitimate businesses. Minister Bains was wise to defer its implementation earlier this summer. To avoid the significant costs to both the court system and industry, the private right of action should be repealed, or at the very least restricted to have standing only for organizations like networks and ISPs who bear the direct costs of spam, spyware, and other online threats.

Thank you. I look forward to your questions.

The Chair: Thank you very much.

Finally, we have Ms. Evans from Rogers.

Ms. Deborah Evans (Associate Chief Privacy Officer, Rogers Communications Inc.): Thank you, Mr. Chair.

I am Deborah Evans, associate chief privacy officer for Rogers Communications. I welcome the opportunity to appear before the committee and provide input into the review of Canada's anti-spam legislation.

CASL has increased consumer protection but it is not perfect. This review provides a valuable opportunity to ensure that the legislation can give greater certainty to consumers and businesses interpreting CASL.

When we reflect on the last three years, there are certain provisions that could benefit from further clarification. Specifically, there are three areas in which Rogers would like to see changes: improving enforcement and ensuring proportionality of administrative monetary penalties, reducing the ambiguity with regard to content and wording of the act, and eliminating the private right of action.

The current structure of CASL empowers the CRTC to enforce compliance through a range of remedies, including the use of AMPs. While we acknowledge that there are benefits to enforcement through the use of AMPs in more egregious cases, the current process has not been without difficulties. For example, all companies in both private and public sectors are faced with unintended information system errors. When consumers are impacted, they notify companies directly in the majority of cases, but they also go to the CRTC's spam reporting centre.

During this committee review, we have heard that warning letters are often issued for violations requiring corrective action. This was not the experience of Rogers when faced with a CASL investigation. We were given no warning at all.

Rogers is an established Canadian business with systems and processes in place to ensure that we comply with all applicable laws and regulations. Nonetheless, we were investigated and signed an undertaking that involved a significant payment. This undertaking was required despite Rogers having identified and resolved the minor issues impacting our customers prior to the investigation. Under CASL, we were not afforded an early resolution process prior to investigation and penalty, unlike similar processes of the Privacy Commissioner, the Advertising Standards Council, and the Canadian Transportation Agency.

When enforcing penalties, the CRTC considers the history of violation and the ability to pay when determining an AMP. We recommend that this approach be revised, and that penalties be linked to the severity of the infringement, not the ability to pay. In the case of the first violation, where an organization's act of non-compliance is an unintended information system error, the CRTC should always issue a warning letter or citation. This would be a more appropriate way to tackle infringements that are inadvertent.

If there are subsequent violations, there should be an established framework to determine the level of fine based on the proportionality of the violation. AMPs would then increase with the magnitude and frequency of the infringement. For example, a deliberate malware dissemination would warrant a much higher penalty than would sending a CEM that omits a required field. For every subsequent violation of the same nature, the fines would grow in severity. The large majority of Canadian companies want to comply with the legislation. Unfortunately, due to uncertainty in the wording of the act, many Canadian businesses have employed an overly cautious approach to communicating with their customers in order to avoid being subject to enforcement activities. This is compounded by uncertainty regarding the application of AMPs, and the high punitive nature of the maximum fine.

In reviewing the act, and based on Rogers' experience, there is an opportunity to provide clear guidance and to remove ambiguous wording. We have heard witness presentations during this review, which have outlined concerns with the lack of clarity in the definition of a CEM and computer programs. We support these positions. As well, there are other areas where the act could provide more clarity for businesses. For example, the current wording in subsection 6(6), states that notification-type emails, such as messages to tell you that your mobile device is roaming, are exempt from consent requirements. However, such messages must include an unsubscribe mechanism. There is no reason why legislation created to regulate electronic commercial activity should be applied to non-commercial messages. These types of notification messages do not fall within the statutory definition of a CEM and should not be subject to consent or message form requirements.

We recommend removing subsection 6(6) from the legislation to limit the scope of CASL to commercial electronic messaging only. As well, guidance material from the CRTC should be produced to give greater certainty as to what types of messages are not CEMs. Additionally, the current definition of electronic address should be updated. We are in the age of new technologies and digital advancements. The overly broad definition has added an additional layer of complexity for Canadian businesses.

We recommend providing a clear and specific definition of electronic address. In particular, the reference to “any similar account” should be removed. As well, we recommend issuing guidance material indicating what is excluded from this definition.

● (1140)

We support the decision by Minister Bains to suspend the PRA. It is unnecessary and does not represent a proportionate response to the stated objective of CASL, namely increased consumer protection. The three agencies responsible for enforcing CASL provide sufficient protections for consumers. The PRA allows any person affected by an alleged infringement to sue for actual damages of up to $1 million per violation with no requirement to demonstrate harm.

Currently, the PRA has the potential to create an environment that encourages consumers to pursue Canadian businesses that may have experienced an unintended informational system error rather than targeting deliberate spammers, many of which operate outside of Canada. Rogers supports eliminating the PRA from CASL. It creates an environment for frivolous lawsuits and is not an efficient use of Canadian courts.

As the committee has heard, most Canadian businesses want to comply with CASL. Well-intentioned companies should not be associated with those that are deliberately and maliciously ignoring the act. If the PRA is to continue, the government must ensure that it is specific enough to target those intentionally acting outside the legislation.

In summary, we propose the following: that first-time offenders be issued a warning letter if the violation was the result of an unintentional error; that penalties be based on a framework of proportionality in which fines increase with the severity and frequency of the infringement; that subsection 6(6) be removed to limit the scope of CASL's commercial electronic messaging; that the definition of electronic address be updated to remove the reference to any similar account; and that the PRA be removed since it is unnecessary.

Thank you for the opportunity to participate in this review. I'm happy to answer any questions.

The Chair: Thank you all very much.

We're going to move right into questioning, starting with Mr. Jowhari.

You have seven minutes.

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

I'll be sharing my time with MP Longfield.

Good morning and welcome. It's good to see some familiar faces.

My riding of Richmond Hill holds about 8,000 small businesses. The majority of them have about four to five people. They use electronic means to reach out to their client base. Some of them do business with each other, so they use B2B. One of the areas they're focusing on is building their skill set to become more innovators, based on and aligned with the agenda.

I understand that aside from the fact that the scope is very complex and very broad, you've come back and you've said that the consent issue remains—the definition of the consent and how it's expressed, how it's requested, and how it has been received.

Also, I understand PRA, but a number of you touched on the fact that the current CASL inhibits innovation. It blocks innovation. Specifically, you talked about IoT and you talked about AI. So, in the about a minute and a half that I left, can any of you touch on which specific areas of IoT are blocking innovation and how they are doing that? That's really important to small businesses in my riding.

David, do you want to go ahead?

● (1145)

Mr. David Messer: Sure. I can start on that at least. From speaking to companies in our association, small and very large, I would say it inhibits innovation because it's confusing, and people don't know what to do. So you have a great idea and then you go and say, “Oh, can we do this?” But the requirements are so complex and there are so many exemptions and small requirements here and there that companies don't know what to do.

For instance, I was speaking to a very large company yesterday. They wanted to send out a text message to their clients about the wildfires out west, saying “if you send us a number back with this hashtag we will match your donation.” They wanted to do this very quickly to get donations to the Red Cross, but they got stuck internally because everyone said, “Wait—does this fall under CASL or does this not? If we include a hashtag that mentions—”

Mr. Majid Jowhari: Help me understand how that inhibits innovation.

Mr. David Messer: It makes companies less likely to take innovative steps and to change the way they're doing business. It makes them stop and think, and it makes them shy away from innovative activities.

The Chair: Mr. Geist.

Dr. Michael Geist: If anything, when we're talking about something like IoT, that's an area in which we particularly need stronger privacy rules and clear knowledge of how our information is being used. Let's recognize what that is.

If we're talking about giving companies the right to listen in through our televisions or through our smart fridges or our coffee makers or whatever it happens to be, the notion that somehow we need greater flexibility and consent.... Let's understand that for years we had that flexibility and consent under law, and that was effectively code for consumers agreeing to things they were not aware they were actually agreeing to.

If we want to see innovation and consumer acceptance of these kinds of new technologies, consumers need to know when their information is being collected and how it's being used, and the messages that go back and forth are part of that.

Mr. Majid Jowhari: It's part of the education. It's not an inhibitor.

Dr. Michael Geist: No, it's not an inhibitor.

Mr. Majid Jowhari: Thank you.

I'd like to share the rest of my time with you.

Mr. Lloyd Longfield (Guelph, Lib.): Thank you. That's very generous.

Thank you, all. We're getting a very good range of opinions; and of course, when we're working on our report, it's good to have balance.

I want to focus on the technical part of whether we need legislation or whether technology has solutions that could do what we're trying to do through legislation.

Mr. Messer, your group is working in technology. Could you talk about how it has progressed, either in Canada or globally, in terms of blocking spam or unwanted messages?

Mr. David Messer: Certainly.

Most of us can tell from our own inboxes that spam filters and cybersecurity mechanisms put in place by ISPs and by email providers and email programs have gotten much better, certainly over the past decade. These are only improving as technologies such as AI feed into cybersecurity. Moving forward, they will advance and our inboxes will be safer before we even get there.

Mr. Lloyd Longfield: Right.

Ms. Evans, on the ISPs front, one thing we talked about as a group before we started this study was the changes in communications, the new technologies. Texting isn't new, but it's relatively new. I've just counted 25 text messages from different U.S. addresses coming to my parliamentary cellphone. I know that I don't have constituents in the United States, and I don't want those messages. Do we have some way to handle text messages through our ISPs and to block them? They certainly couldn't prosecute them.

Ms. Deborah Evans: Certainly. Many ISP and telecommunication service providers do have spam filters on their network to try to identify keywords that will block out spam. Obviously the system isn't perfect, and spammers who are deliberately trying to reach you to do nefarious things are quick to act and get around that.

In a similar example, not related to CASL but to spoofing of telephone calls, we put in a fix to eliminate a telephone number that someone has been spoofing. The spammers know and they've moved on to another one. They're quick acting, and we're just keeping pace with them.

Mr. Lloyd Longfield: Commercially, to compete against other ISPs, you have to be ahead of the game as well.

Ms. Deborah Evans: We have to do our best to keep our customers happy.

Mr. Lloyd Longfield: It makes me wonder who's supplying my cellphone here.

Mr. Fekete, I'm running really short on time, so I'm just going to use my time to say thank you for getting the balance. As a former president of a chamber of commerce, I'm left back where I was a few years ago, wondering about the efficacy of this whole exercise that we're in the middle of right now.

Thank you.

● (1150)

The Chair: Thank you.

[*Translation*]

Mr. Bernier, you have seven minutes.

[*English*]

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

My first question is for David Messer.

You said on your website that your organization championed the development of a robust, sustainable digital economy in Canada. Is the creation of a robust, sustainable digital economy in Canada possible under the current legislation?

Mr. David Messer: If we want our digital economy to grow and be stronger, we need to make it better aligned with our competitors. As Michael noted, Canada's software provisions are an outlier compared to those of the rest of the world. The requirements in CASL are completely different from the requirements in CAN-SPAM, the U.S. legislation, which is much more principles-based.

If we want to build a strong and robust digital economy, we need to be engaging with the world and not inhibiting our companies by putting in unnecessarily strenuous requirements; and we need to be working through organizations such as the OECD, APEC, and the G20 to develop interoperability where we can, because the ICT industry really is the most globalized industry in the world.

Hon. Maxime Bernier: Do you want to add something?

Dr. Michael Geist: I'd note that CAN-SPAM in the United States is aptly named, because you can SPAM.

The reality is that the task force had the opportunity to look at some of those other laws. The idea that Canada should emulate a law that is universally regarded as entirely ineffective strikes me as problematic.

If anything, what we are seeing is jurisdictions moving towards stronger rules. Australia, for example, saw the spam problem that was happening locally and adopted the strongest anti-spam rules at the time. It found that, within short order, much as we've experienced with the reduction in major anti-spamming organizations, they left Australia because the penalties were so high that the risk changed their analysis of whether it made sense.

If we're thinking about whether these kinds of rules are getting tougher, just take a look at what's taking place in the European Union with the GDPR, which has far tougher privacy rules that are applied not just in the EU but around the world.

Mr. David Messer: I'm not saying Canada should have the weakest rules or go to the lowest common denominator at all. We should find ways to work with our allies and other countries to develop interoperability so Canadian businesses are not unnecessarily hampered.

Hon. Maxime Bernier: Michael.

Mr. Michael Fekete: Certainly. I want to agree with Michael that we need strong privacy rules that govern the collection of information, and we have a federal privacy statute that sets a very strong standard in terms of how to do that based on principles and a flexible approach with strong guidance provided by our commissioner.

When we think about the computer program provisions, Michael is right to say there are times when personal information is collected, but that's where PIPEDA applies already. There are many times when updates to computer programs do not result in collection of personal information. In those instances, you have to comply with very prescriptive rules that don't match the rules in any other jurisdiction. If you want to focus on where Canada is hamstringing innovation in Canadian business, you can look very closely at the computer program rules and ask yourself why no other country has copied our approach.

Hon. Maxime Bernier: I have a question for Ms. Evans.

Do you have any idea of the costs Rogers must pay for being compliant? What is the cost of the employees and the database? Can you explain what you are doing to be fully in compliance with the legislation?

Ms. Deborah Evans: We have a very robust compliance program that follows the guidance that has come from the CRTC.

With regard to employees, we have embedded a culture of CASL compliance in all employees who have are responsible for sending commercial electronic messages. Those employees are required to know what they have to do to comply with the law. They get robust annual training on how to comply with the law. We have tool kits available to them and job aids to help them.

We have a centralized database. We have an online preference centre for our customers to go in and self-manage their communications from us according to types of communications and lines of business. I couldn't put a dollar figure on specific costs, but it is something that's embedded in the corporate culture.

● (1155)

Hon. Maxime Bernier: Thank you.

I want to share my time. We still have three minutes.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Thank you, everybody, for coming today and to your staff who are here for helping to prepare for today. I know it's a lot of work.

I want to just clarify a few things. We had before us some presentations from a number of individuals in the lead-up and preparation for this. I will read you just a couple here.

From the Canadian Chamber of Commerce, Mr. Scott Smith indicated in his presentation that "...in 2008 92.6% of global email traffic was spam. By 2015 that number had declined to 54%."

We had another presentation from Mr. Lawford from the Public Interest Advocacy Centre. He said that, "One report from...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 period immediately after CASL came into full force on July 1, 2014."

A number of you said that it hasn't had any effect on this issue. Can you point us to any reports or statistics that show that?

Dr. Michael Geist: I'll just reiterate my opening remarks. I don't think there is anything more telling, to be honest, than knowing that Canada was once truly a haven for large spamming organizations responsible collectively for more than 80% of the spam generated worldwide, with a disproportionate number of those organizations hosted in Canada. Today we can't say that anymore. The decline from seven of those organizations two days before CASL took effect in 2014 to only two organizations today—and that's still two too many—speaks volumes about how the law intended to try to address the amount of spam being generated in Canada and sent either to Canadians or around the world and how it has clearly had an impact in reducing the number of those organizations situated here in Canada.

The Chair: Thank you very much.

Mr. Masse, you have seven minutes.

Mr. Brian Masse (Windsor West, NDP): Thank you, Mr. Chair.

Thank you for being here.

I represent many businesses in my community that do not want to have innovation stymied by unnecessary maintenance of emails they do not want, viruses, and other scams that occupy their time, especially when they don't have IT people on staff and have to rely on subscribers. I also come with a different perspective. I mentioned this last time, and I'll mention it every time: I view it as a privilege that this type of advertising appears on something you pay for, something you maintain, something on which you pay for the data downloaded to you. To email me advertising is a privilege, not a right.

With regard to Rogers, if I'm correct, it was a problem with the "unsubscribe" that led to that, and it turned out to be something that others were involved in.

Can you give me an example of that? How could it be done to allow for a quicker resolution? There are others such as Compu-Finder that were fined as well, but they were well-known spammers going back to 2008. What can you say about the two different cases? There are others that have been fined, like Plentyoffish, which is an online dating site that bogs down business. These are the types of problems we're facing.

Ms. Deborah Evans: From our perspective and our investigation, we had an issue for a short time on our business-to-business publishing side, where an “unsubscribe” was not functioning as we had intended. We had put in place robust processes prior to deploying the email regarding how we compile our lists—the form, the content, everything to comply with the legislation. We sent out some communications. Unfortunately, it didn't operate as we'd intended. We heard from some of our customers, and we immediately looked into the issue. We resolved it in a matter of days of it having been brought to our attention. It's not in our best interests to be out of compliance with the law. We want to be seen as good corporate citizens—not as a company in the same boat as Compu-Finder, which, as you pointed out, has been a known spammer forever. We're a well-intentioned, established business.

● (1200)

Mr. Brian Masse: I agree. What was striking in some of this was the in-between time of those who are doing it but not using it as a loss leader. There has been a lot of discussion on this.

Mr. Geist, maybe you can talk about ROKSO a little bit, because in the past, spam has been a loss leader for business, a small spam investment sending out millions, if not multi-millions, of dollars in emails. All you have to do is get back one. I think all members of Parliament get calls about the fake CRA scams that prey on seniors. This deplorable practice is only getting worse. It's done not only by telephone but also through spam.

That was a big part of the discussion about what we're doing internationally on this, and I have made a request for a witness from Interpol in the future, but could you please go into a little more detail about ROKSO?

Dr. Michael Geist: One of the most surprising things is that the large spamming organizations operate with impunity and very often in the open, something one wouldn't expect. One of the reasons they do this has to do with the lax laws that exist in many countries. It's recognized that one of the only ways to deal with some of those large players is through tough anti-spam laws. We've seen a couple of countries, Australia and now Canada, that have been able to effectively drive some of those organizations out by passing some tough laws.

At the heart of the problem is the risk equation. If you are a spammer, you are in a sense off-loading just about all the costs onto consumers. We pay for all of this, and I would argue that legitimate businesses, large and small, pay too, because people's trust in the system is undermined by all of this. What we need is an effective system that will benefit large and small businesses alike, while increasing the costs for some of the scammers out there, so that they either leave the jurisdiction or stop what they're doing.

I find it somewhat discouraging when we hear people coming before committee saying that what we really need is to reduce the tools we have to enforce this law. Private right of action is a good illustration of this. You can't say, on the one hand, that the rules are too tough from an enforcement perspective and that we need ways to sort this out, and then say, on the other hand, that everything is going really well so we don't need a private right of action.

PRAs have been used in other jurisdictions and they can be used effectively.

Mr. Brian Masse: Mr. Kardash, do you and Mr. Fekete work at the same—

Mr. Adam Kardash: Yes, we're at the same law firm, but I'm also counsel to the Interactive Advertising Bureau of Canada.

Mr. Brian Masse: I'm just looking for clarification, because we're provided 20 minutes. I don't know which—

Mr. Adam Kardash: We're different organizations.

Mr. Brian Masse: Thank you. Please, both of you, split the remaining time.

Mr. Adam Kardash: Mr. Geist's comments focus fundamentally, and correctly so, on bad actors. The issue we're raising is not with respect to bad actors. No one likes spam, certainly none of our members. We can speak about our client base. None of them like spam. It's extraordinarily costly for business. Bad actors should be appropriately punished. That's not the issue, which is what's fundamentally raised. We're talking about a legislative scheme that applies to all legitimate activity. That is a problem compounded not only by sheer scope but also by very complex prescriptive rules that, when you look at real life examples, don't make sense for small business.

We agree that if there's a bad actor, such as those spammers that are now gone from this country, the punishment they would get through a very focused private right of action or another remedy makes sense. What we're talking about and what our members are concerned about is the expansive scope of a legislative regime that applies to everything. Through a very complicated scenario, you're effectively playing Whac-A-Mole when trying to understand the legislative scheme, because it says everything is covered except for things that aren't.

Mr. Brian Masse: That's where we differ. I still believe it's a privilege for you to send information, to use my cost to send that information, versus for me to request it. It would be similar to my walking into a store, and having a chance to pick up its flyer when I enter versus somebody forcing me to take it and me having to pay for that flyer as I enter the store. That's my view. If it is hard work, we can ask how we can make it better. However, I come from the basis that it is a privilege for you to be able to send me things when I haven't asked for them and they're unsolicited.

● (1205)

The Chair: We're over our time, and perhaps we can ask further questions.

We're going to move on to Mr. Baylis.

You have seven minutes.

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Ms. Evans, you gave an interesting suggestion about subsection 6(6), to reduce it to strictly commercial electronic messaging, and you gave the example of a notification for roaming. Theoretically, right now you have to have this full set of prescribed data inside of that to unsubscribe from the roaming message. Is that correct?

Ms. Deborah Evans: That's correct.

Mr. Frank Baylis: A number of people have brought up this point. I'll start with Mr. Fekete. You said a similar thing, that an update patch would also need to have an unsubscribe mechanism.

Mr. Michael Fekete: I didn't say that, but you're right. The rules prescribed by the CRTC indicate that in any request for consent, you must state that a person will have the opportunity to withdraw consent.

Mr. Frank Baylis: If we were to implement the suggestion from Ms. Evans, which is that subsection 6(6) should apply only to commercial messaging and therefore an update or a patch would not be commercial messaging, would that address this issue?

Mr. Michael Fekete: Subsection 6(6) does not deal with a computer program. It deals exclusively with electronic messaging.

Mr. Frank Baylis: Okay. Go ahead.

Ms. Deborah Evans: I can give you other examples: a safety recall message or a notification saying your bill is now available.

Mr. Frank Baylis: If we were to start with subsection 6(6)—and that's if we were to tackle a number of things—that would address your updates and your roaming, but it doesn't tackle the computer software part, which is patches. We'll come to you in a minute, Mr. Messer. Obviously the legislation is not designed or was not intended to stop someone from having a patch or an update. You're saying it's too prescriptive. How would we deal with that in the legislation specifically?

Mr. Michael Fekete: I think we need to look at what our international trading partners do. They don't regulate all computer program installations. They regulate malware and spyware. There are unintended consequences of having an overly broad approach, and those are the consequences that I fear are undermining the innovation.

Mr. Frank Baylis: So it's not the electronic messaging part but rather the part about tackling computer programming that is wrapping up and capturing your updates, and that needs to be targeted strictly to malware. Is that what you're saying?

Mr. Michael Fekete: Other jurisdictions regulate malware and spyware, as they should and as we need to, but they don't go and regulate all other messages. They certainly regulate collection of information, personal information using computer programs, as we have with PIPEDA and as we will continue to need to do. We go that much further than anybody else does.

Mr. Frank Baylis: By going further, we're capturing things we don't actually want to capture.

Mr. Michael Fekete: A decision was made to regulate the installation of all computer programs except for those specifically exempted by regulation.

Mr. Frank Baylis: And you'd like to turn it the other way around.

Mr. Michael Fekete: I'd turn it the other way around, and focus on the bad stuff.

Mr. Frank Baylis: Mr. Kardash, you mentioned administrative messaging. Would that be captured, either through section 6.6 or—

Mr. Adam Kardash: Yes, section 6.6 is exactly what I was referring to.

Mr. Frank Baylis: —with the administrative messaging. That would be captured if we were to implement something like what Ms. Evans is suggesting.

Mr. Adam Kardash: Yes, expressly exclude the messages contemplated in section 6.6 from the definition of commercial electronic messages.

Mr. Frank Baylis: That would capture that part.

Mr. Adam Kardash: Yes.

Mr. Frank Baylis: You also touched on something else. You mentioned online advertising like Facebook. If I'm on Facebook, I get ads coming up. I didn't understand what your point was there.

Mr. Adam Kardash: CASL applies to the sending of commercial electronic messages to electronic addresses. The definition of electronic addresses expressly contemplates email accounts and instant messaging accounts and telephone accounts.

Mr. Frank Baylis: If I go on Facebook, it knows where I've been and what I'm up to, and it messages me. It displays—

● (1210)

Mr. Adam Kardash: It's a display, yes; it's not sent. It's completely outside the ambit of the legislation.

Mr. Frank Baylis: It's not within the legislation.

Mr. Adam Kardash: There were comments unfortunately made by the CRTC and in the RIAS statement by what was then Industry Canada about the potential application to IP addresses, which is not, in our view, there, and you cannot have this legislative scheme apply.

Mr. Frank Baylis: It doesn't apply, but you're concerned that we might try to apply it?

Mr. Adam Kardash: We need scope of clarity.

Mr. Frank Baylis: That's on the address.

Mr. Adam Kardash: It was a similar point made—

Mr. Frank Baylis: Theoretically, right now, we could include the IP address as an email address. Is that my personal address?

Mr. Adam Kardash: That would be devastatingly bad, yes.

Mr. Frank Baylis: It's unclear whether that's being done right now.

Mr. Adam Kardash: Well, it wasn't unclear until statements were made by the CRTC and in the RIAS about the potential concept of electronic addresses applying to IP addresses. That's totally outside the scope of this.

Mr. Frank Baylis: It was just something that came up like electronic addresses applying to IP addresses, but it's not actually in the legislation right now.

Mr. Adam Kardash: No.

Mr. Frank Baylis: And you're saying we can't go in that direction.

Mr. Adam Kardash: That's right, 100% correct.

Mr. Frank Baylis: Understood.

We heard about implied consent, and, Mr. Messer, you also touched on that. A lot of software within the Internet of things, but there's no way for me to go in and say I consent. Things are happening.

If we were to tackle what Mr. Fekete is suggesting vis-à-vis programs, would that take away the concern you have with regard to implied consent, in terms of updating, and the Internet of things, and all of those kinds of things that have to happen? There's nowhere I get a flashing light that says, “Hey, do you agree to do something?”

Mr. David Messer: Yes. On a number of Internet of things-types of devices, implied consent is really the only way.

Mr. Frank Baylis: If we were to write the computer programming legislation specifically tackling malware and spyware, would we still need to write something about implied consent, or would that deal with the issue?

Mr. David Messer: Implied consent as a principle would be good to put in the legislation more generally, as it is in PIPEDA, because having it will make the legislation more flexible and more nimble. The CRTC will be able to issue guidance, and companies will be able to ask questions.

Mr. Frank Baylis: Even if we narrow the electronic messaging and the computer, we should still consider implied consent, because we don't know what's coming down the pipe. There might be areas in which we need to have implied consent so that things can go along.

Mr. David Messer: Exactly. It will provide more flexibility. It will make it easier for companies to ask questions, and to learn from each other.

The Chair: Thank you very much.

Mr. Jeneroux, go ahead for five minutes.

Mr. Matt Jeneroux: Thank you.

I do want to come back to my previous line of questioning, but before I do that, I want to follow up on some of Mr. Baylis's questioning.

In terms of social media, if a company messages me directly through a direct message on a, let's say, Twitter account or Instagram account, that should be...that's not allowed, or there should be an unsubscribe function to that.

However, where's the line currently drawn in terms of having individuals reach out to us, I guess, essentially on behalf of a company? If someone messages me on my Twitter account, we haven't engaged in a transactional history of any sort. Now suddenly, they're messaging saying I should pay more attention to something on behalf of their organization.

Where's that line? I'm probably looking at you two gentlemen, particularly, to answer some of that.

Mr. Adam Kardash: You're speaking about a case scenario in which a company goes on, or an individual....

Mr. Matt Jeneroux: I mean an individual on behalf of a company. I don't want to choose any of you here at the table. Let's say a cellular phone provider reaches out on Twitter and Instagram and says, “This is a great deal. You should pay attention to this deal.”

Mr. Adam Kardash: I'll just speak generally. The act contemplates various circumstances in which you'll have authority to reach out. The entity in question could have gotten express consent under the act. There are very prescriptive requirements to do so, as I mentioned before, but they could rely on express consent. Or there are a series of implied consent provisions, which are very detailed, and which say, for instance, that if you made a purchase within the last two years, you're able to reach out and do so; or if you have a written contract, for the duration of that contract and two years thereafter you can reach out. So assuming it's a commercial kind of message—

● (1215)

Mr. Matt Jeneroux: There would have to be an exemption—

Mr. Adam Kardash: Now, depending on the message—and this illustrates the complexity—either subsection 6(6) might apply or one of several exemptions could apply. It depends on the very specific context.

Mr. Matt Jeneroux: Sorry, but we hate dealing with hypotheticals in our world.

Actually, Mr. Geist, I'm going to move on, if that's okay, because I do want to get some other feedback on my initial question with regard to providing proof on the other side of it. I read out some statistics that show that other people have been in front of us and have indicated that the amount of spam has gone down. A number of you have made presentations saying this legislation has had no effect on spam. I'm just hoping you can point to some of that.

I know, Mr. Fekete, you were hoping to answer last time.

Mr. Michael Fekete: I think the problem is, as Mr. Geist has mentioned, we really don't have enough information. We have some statistics that are quite old, from 2015, to suggest there's been a reduction in overall messaging, including of legitimate messages. To Mr. Masse's comment, the question we have to ask ourselves from a policy standpoint is how we ensure that it is a privilege to use electronic means to communicate, much as it is a privilege to collect, use, and disclose personal information. It's not a right. It has to be, however, through a balanced framework. What I am personally suggesting is that the framework as reflected in CASL doesn't strike the appropriate balance, and that there's an opportunity for all stakeholders and all parties to work together to get the balance right.

Mr. Matt Jeneroux: Are there any other comments on that?

You had your chance already, Mr. Geist. Do you want to go back again? If you have something to say, go for it.

Dr. Michael Geist: I just note—and it's come up now a couple of times—that there's this notion that there are the really bad actors, the spamming organizations, and everyone is in agreement that we have to target them; and then there's an attempt to characterize all the other businesses as not being bad actors. I don't doubt for a moment that Rogers, my carrier, is not a bad actor, but I will say that if you are sending me messages when you have not obtained my consent that is a bad act. I think we have to recognize that there are lots of legitimate businesses that may even still want to comply but that are, I would argue, misusing our personal information without obtaining appropriate consent. That's a bad act, and that's what the law's designed to target. If we contemplate moving back to implied consent, then we're right back to where we started from. The task force looked at whether or not PIPEDA was effective in dealing with spam, and the conclusion was that it was not. One of the core reasons was that implied consent just doesn't work in this context. It will be obvious to all of you, given the number of times, I'm sure, you've received messages from a legitimate business while you can't for the life of you understand why you're getting this message. The reason is that these businesses often rely on implied consent to be able to send out those messages.

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

Ms. Ng, you have five minutes.

Ms. Mary Ng (Markham—Thornhill, Lib.): Thank you.

Please help me with some clarification here. We heard from Desjardins at our last meeting that, overall, the provision to be able to provide safety notifications is inhibited by CASL. You at Rogers are saying a similar thing. To protect your consumers, you want to be able to give them notices of roaming, etc. And yet we'll hear from people who do in fact get those messages. Then we heard from Mr. Geist that somehow there is not an interpretation or an appropriate interpretation of CASL, and yet companies can indeed do that to help protect consumers, and yet companies are interpreting it too narrowly. Can both of you talk about that? There seems to be some incongruity here. Is it in the application, or what is it?

Ms. Deborah Evans: Sure. I'll start that off for you. Thank you.

I think what we're seeing is that there is subsection section 6(6), which we spoke about, which says that in these scenarios, you can send the messages to the customers. You don't need consent to send the messages, but they must follow the form and content of CASL requirements, so they must have an unsubscribe mechanism.

My point is that certain messages we will send to our customers either because we're required by law to send them or because it's the good customer experience. For example, if you need to know something from us, we'll send it. To put the unsubscribe at the bottom gives the wrong impression; it creates confusion for consumers. When I'm required to send you a message and I put in the unsubscribe, and then you click on it, you think you're unsubscribing. But really, are you unsubscribing? I'm still going to send you the message, because I'm required to send the message. It creates confusion.

I've heard from other businesses that they just don't send those types of messages because they're not sure how to do that. Maybe they've resorted to other means of contacting their customers, such as direct telephone calls or direct mail. I would argue that's a negative impact and an inadvertent, unintended consequence.

Regarding public safety messages, there's an exemption in CASL that will allow messages to be sent for public safety reasons, but there's confusion created by the requirement to have an unsubscribe in a message that the business is still going to send the customer because they're required to send it or it's.... For example, you need to tell the customer if they signed up for online billing that their bill is available for them to look at. How are they going to know their bill is available otherwise? If they're unsubscribing from it, and then you send them the next month's bill, that's where the problem is created.

● (1220)

Ms. Mary Ng: Mr. Geist.

Dr. Michael Geist: You asked how we can have this confusion. I think we've seen it happen on this panel just in the last number of minutes.

The panel was asked a question that I thought Mr. Kardash effectively responded to with the use of a case from Mr. Jeneroux. He started by saying that if you have explicit consent, you can go ahead and do this, and then he proceeded to talk about the various exceptions.

The problem is that we get bogged down in the various instances of how you can do this if you don't get someone's consent. The starting point again and again in many of these instances is to get consent. If we're talking about something different, not about the ability to message but instead this potential for confusion with an unsubscribe, surely that's an issue that can be fixed for a public safety message. It's not that we can't send it, but there's an unsubscribe issue. That is a far cry from the doomsday scenarios this committee has been hearing about in the last number of hearings, moving from "Can you please fix an unsubscribe mechanism in a public safety message?" to somehow that e-commerce is going to stop in Canada if this law continues.

Ms. Mary Ng: Thank you for that.

I'm going to continue on this. We have heard a lot from the business community. My riding has a lot of technology companies and a lot of start-ups, so we certainly want to make sure the legislation does the one part, which is to get out the bad actors and make sure there is indeed consumer protection for many of our vulnerable people, including our seniors, who now are using more and more electronic communications. We need to be able to balance the consumer protection with the ease of doing business and the ease of innovating.

Mr. Geist, do you have a recommendation as to how to do that? We're genuinely hearing from people and from businesses that say the cost of complying is a challenge and the ability to innovate is a challenge. Help us with some practical solutions that we could consider, because I think that's the job of this committee ultimately.

The Chair: Unfortunately, we're really over time.

Perhaps we can come back to that question.

Mr. Eglinski, you have five minutes.

Mr. Jim Eglinski (Yellowhead, CPC): Thank you. I'd like to thank the witnesses for coming out today.

I was sitting here listening to the witnesses that we had at the previous meeting, and we've listened to you. We definitely have a lot of controversy going on between the groups of people who are appearing as witnesses. A lot of you are saying it's not working. Others are saying it is working. There's little information showing that it's actually working. We're hearing that.

I had a meeting last week in my riding, dealing with tax reform, a round table discussion with about the same group of people we have here, business people. After we had finished our discussion, I turned to the group of businessmen and asked how many of them know about CASL. They said, "What the hell are you talking about, Jim?" There was only one who understood the dynamics of what we're talking about here today. He spends a lot of time on his computer, makes a living off his computer.

I'll throw this to Mr. Messer. What can we do to educate the small businesses out there? The big businesses sitting here today are telling us it's a big problem. Yet when I talk to a group of businessmen, about the same number we have here, they say, "I don't see no goddamn problem. We don't even know about it." I think we have a problem, because they should know about it.

I wonder if you would answer that, please.

● (1225)

Mr. David Messer: I think the first point is that we need to simplify the law. We need to make more clear what it applies to and to make it more flexible and adaptive, so that you can explain it to a business and they'll understand it and say, "Oh, this what I need to do to comply."

As people on the panel have been mentioning, part of the problem is that there is a range of things that are exempt or not exempt, and in some circumstances they work, but in some they don't. This is why businesses, large and small, need lawyers and consultants: to tell them how to comply.

It's no surprise that a lot of people fall asleep when they start hearing about it or ignore it if they don't have to pay attention to it, because people who do have to pay attention to it are—rightly—very confused by it. I think the first thing needs to be simplifying it and making it easier to comply with.

After that, of course, the CRTC needs to become a partner in this. They need to reach out to business.

Mr. Jim Eglinski: Thank you.

Mr. Geist, you mentioned something earlier which I took note of. When we brought out this legislation, we had seven major spammers in Canada, and immediately five of them headed south, or north, east, west, or whatever. We don't care where they are. But we still have two. Why do we still have two? Why aren't we dealing with them?

Dr. Michael Geist: I agree with that. I agree with the premise of the question, and I think it's a question best posed to the enforcement agencies as to why they haven't targeted those—

Mr. Jim Eglinski: Okay. Talking about enforcement, we had a witness here last session who said that the CRTC was fairly lenient and was trying to work with businesses across Canada, with a lot of warning letters and stuff like that. I've heard from two witnesses today that they're heavy-handed now. As an independent, not being in a business-related field, what's your comment on that?

Dr. Michael Geist: My comment is twofold.

One, I think the CRTC has failed to target, as I think you rightly point out, the remaining large spamming organizations. From my perspective, it's inexplicable, given that we know where they are. It was amazing when the law was being crafted and we had at least one large Canadian-based spammer who was openly blogging and laughing about it, and in a sense almost urging enforcement, and yet we haven't seen that. I do think they've fallen short in that regard.

On the other hand, I certainly have some amount of sympathy for large businesses that say they feel they're being targeted. I think in some ways it links a bit to your first question on how we can ensure that businesses are at least aware of the legislation. There is, I think, a certain element which is that the CRTC is going to go after some of the bigger fish, so to speak, partially because they ought to know better—they have the resources to do it—and partially I think because that may actually assist in ensuring there is the effect of having many other businesses becoming more aware of their obligations under the law.

Mr. Jim Eglinski: I have 30 seconds left.

I contacted the three largest police forces in Canada: the national police force, Ontario.... Not one of them deals with any of this. Should we be taking it beyond the scope of the CRTC? Does anybody want to answer that?

Dr. Michael Geist: I'm happy to tell you that as a task force we met with law enforcement regularly. It was a real challenge at the time in regard to convincing them that some of these issues rose to the level of deserving some of their attention and the use of their scarce resources.

Years later, when we take a look at what we've seen, particularly in some of the malware cases, let's say, and some of the other major sorts of cases.... It's not that I think we should be looking for law enforcement to say that they're going to take everybody off their existing jobs to focus on this, but there are serious implications, not only economic but political and otherwise, and I think real resources need to be put to the issue.

Mr. Jim Eglinski: Thank you.

The Chair: Mr. Sheehan, you have five minutes.

Mr. Terry Sheehan (Sault Ste. Marie, Lib.): Thank you very much to everyone for another thought-provoking session.

I am glad we're reviewing the legislation, based on all the testimony I've hard so far. I want to continue on with some of the questions I asked in the last session. The particular legislation talks about the “activities that discourage reliance on electronic means of carrying out commercial activities, and...amend the Canadian...” and it goes on. It talks about the various means of contacting and picking up.... There were some questions about Facebook today again.

Michael, when I take a look at when your task force went out, in 2004, I reference the fact that the same year there was another big thing happening, then called TheFacebook. You probably weren't delving into TheFacebook at that particular time.

My question is based upon these numbers that I see: Facebook just hit two billion users a month; YouTube has 1.5 billion per month; Instagram has 700 million; Twitter has 328 million, and so on. I'm not going to name the other various social platforms that are out there. They're all important. I use them all. They're generational too. Certain ages use more than others do. Generationally, privacy, in my opinion, is a different issue. My daughter is not as concerned as my father is about who sees what on social media.

My question concerns why or how this particular legislation affects the various platforms that are out there. Even Facebook has a messenger now, which uses basically email. I can't get into the technical terms of it. How will this legislation affect these various social platforms going forward? If it doesn't, why not, and should it?

Does anyone want to kick it off? Michael, I guess I'll start with you, and then perhaps other people will have an opportunity.

● (1230)

Dr. Michael Geist: I want to pick up on that notion that back in 2004 we couldn't or wouldn't have predicted necessarily the rise of social media and some of these other technologies. I think that's true. In fact, the committee recognized that there was a rapid pace of change taking place. Ironically, based on the recommendations we are hearing today, we were urged to adopt as much of a technologically neutral approach as possible. The idea was to not limit this just to this narrow band of what is seen as spam, but rather to ensure that the law can be effective as some of these technologies change, which is why there is that ability to be effective against spam, spyware, malware, and potentially even some of these new technologies.

One of the discouraging things that I'm hearing now is that the recommendations are, “No, don't do that. Get as specific and narrowly tailored as possible. We don't need to have that broad base on some of these issues. It's too broad in scope.”

That was seen by many as a feature, not a bug, back when we established this. I think one of the ways to ensure that the law is effective and relevant as things change is to ensure that it can be applied as some of these things change. I would certainly point again to things like IoT and those sorts of technologies. The idea that we would bring those technologies into our homes without effective protections against misuse of our information is a real problem.

Mr. Terry Sheehan: The other Michael.

Mr. Michael Fekete: I would like to take a different perspective. There is no question that we need effective privacy legislation. The discussion and the points that Michael is raising are about privacy, agreed. That's why we have PIPEDA. That's why we have a very active, internationally respected privacy commissioner who sets out guidelines and provides direction based on very technology-neutral legislation that is based on principles.

The problem with the anti-spam legislation is that it's not based on principles; it's based on very prescriptive rules that don't necessarily work in these new environments. The Internet of things is a great example. If you don't have an interface through which you can get consent, how do you comply? There is an unintended application of these prescriptive rules to a technology we didn't fully understand or didn't see in the way that we see it today. Our privacy legislation provides the framework for technology-neutral legislation that is flexible to allow for technological change. CASL isn't that legislation, because it's overly prescriptive.

We have to fix the prescriptiveness. We have to make it more principle-based to achieve the outcomes that we all agree are necessary to protect consumers and to ensure that businesses don't exploit the privilege of contacting individuals or the right of installing an update to a computer program.

● (1235)

The Chair: Thank you very much.

Mr. Masse, you have two minutes.

Mr. Brian Masse: I'll start with Mr. Fekete.

If the private right of action were fixed—and this is ironic, because you're concerned about frivolous lawsuits. We haven't had any lawsuits. We're just speculating now that it will be the place, and I don't want to get into a whole debate as to why it's going to happen, or whatever. But if it were eliminated—in terms of the speculation, which would basically be lawyers inappropriately acting against other lawyers, because that's how you create the lawsuits to begin with—would you support that at all, if we got rid of that and if it were just for serious cases?

I'll maybe go across the board really quickly, if that's possible. If it were cleaned up so it would involve only the most serious cases, and not the speculating...?

Thank you.

Mr. Michael Fekete: I think there would be broad support if the private right of action were targeted on the truly bad actors, and we had a situation where we weren't combining a private right of action, broad standing to sue, and statutory damages, because that's where the potential for frivolous class actions becomes most prevalent. Narrowing the scope and enabling private enforcement against the bad actors, I think, is something that would be broadly supported.

Mr. Adam Kardash: I completely agree, as I said in my opening remarks.

Dr. Michael Geist: I think we need to understand that the existence of the private right of action under the law is not an accident. We looked at other jurisdictions which had it, and then spoke to organizations that had used it and found it was effective.

In the United States, where you see some of these actions, we spoke to organizations that had used the law, and they found that the misuse, sometimes of their domain or other sorts of spamming activities, declined after they brought those actions. That was why we brought it in.

I think we can speculate about all the potential misuses of the private right of action if it were to come into place, but with a less litigious society, typically the United States—and we've actually seen effectiveness there—from my perspective, I thought we surely should have at least seen how it worked. That's what these kinds of hearings are for—to see if it has been creating unintended consequences and if we think there is an opportunity to fix it after the fact, rather than taking away what was viewed as an important element in the tool box to try to deal with the problem.

The Chair: Thank you.

I'm sorry. We have enough time to do one more round of five minutes each, so I'm sure Mr. Masse can get back to you guys.

We'll move right on to Mr. Baylis.

You have five minutes.

Mr. Frank Baylis: I'd like to explore a bit more the concept of prescriptiveness.

I think, Mr. Messer, you brought up the idea about being more principle-driven, as opposed to having rigid and complex directives. Could you expand a little bit on that?

Mr. David Messer: Certainly. When you look at PIPEDA, businesses can look at it and figure out whether or not they are in compliance. They usually don't have to hire a lawyer to do that, and they have a relationship with the Privacy Commissioner, to whom they can reach out. It's much more of a partnership to make sure they're in compliance.

A more principles-based approach along those lines for CASL would help businesses be more willing to reach out and make it easier for them to comply, as opposed to saying, “Is this far enough along that it is a transaction? If I say these words, does it count as commercial?” There are a lot of very finite details, and it's difficult to tell.

Mr. Frank Baylis: I imagine in a world where things are changing so fast, for example, that it becomes even more important. It would be very difficult to be prescriptive and capture everything, so principles might apply even more if it's a highly dynamic world, with such things as electronic messaging, Facebook, Twitter, and all that.

Mr. David Messer: Yes. A principles-based approach will give companies a little more confidence that they are leaning this way or that way, so they'll be able to have confidence in their decision and then develop a history and guidance to help them. For instance, if you use a hashtag in a transactional message that says your company's name, does that mean it's partly an advertisement? There are a lot of questions to which there aren't really clear answers. From my members' experience—

Mr. Frank Baylis: It's very difficult, as I believe the hashtag might not even have existed when the first draft of this came around. So it would have been hard to be prescriptive on that, and so where does it fall?

Your argument about principles is understood.

I believe, Mr. Fekete, you were making exactly the same argument. Would that fall in line with what Mr. Messer is saying?

Mr. Michael Fekete: Let me give you two real-life examples.

The law tells you how you must request express consent.

● (1240)

Mr. Frank Baylis: So it has to be this way.

Mr. Michael Fekete: You have to say this is my business name, and this is my mailing address and either my email address, my web address, or my telephone number. And I must say that you have the right to withdraw consent, or you can withhold your consent, or pull it back later.

If I don't ask it in that specific way, with that information, the consent is not valid, so—

Mr. Frank Baylis: So even to the point of the way you unsubscribe, or the way you ask for consent, it's so prescriptive that it may not.... For example, if Twitter were advertising, I couldn't get that into Twitter. I doesn't fit the 127-character limit.

Mr. Michael Fekete: That's a great example.

Another example is on implied consent. I'm in full agreement with Dr. Geist that we need a strong consent regime, but there has to be a willingness to look at the circumstances and ask whether it makes sense for this small business to send a message to a customer based on a prior relationship.

Mr. Frank Baylis: On that issue, then, it can't be too prescriptive, because you don't know what's coming. You would agree with Mr. Messer, then, that we should look more at principles rather than be highly prescriptive in those areas.

Mr. Michael Fekete: Absolutely. If I've made a purchase within the last two years, you can send me a message, but if I've subscribed for a free service—I didn't buy anything—maybe you can't send me a message. I say “maybe” because we're left scrambling to interpret the law. It's too prescriptive to make sense to business, let alone to the legal community who have to interpret it.

Mr. Adam Kardash: You could make changes consistent with Mr. Fekete's comments, and there's a ton of common ground with Dr. Geist. It might not appear that way, but there really is. You could make a series of tweaks to eliminate some unnecessary wording, to clarify the ambiguity—

Mr. Frank Baylis: I fully understand. What happens often with government is that we make strong laws, and the only people who show up to apply them are good, honest, hard-working citizens, while the people we actually want to target are not in this room and will never come to testify in this room; they're gone or they're hidden somewhere else.

A voice: You could subpoena to them.

Mr. Frank Baylis: We could, but as Mr. Geist has pointed out, it's not working to the point it should, because we still have bad actors in Canada. When we had the CRTC here, it was very clear that they hadn't tackled any of them, and yet, all of these good people are working as hard as they can with good faith to try to meet those roles.

I subscribe to the view that if, in a perfect world, there is no spam from the good people, we would know just to kill everything else, because it would be all bad. That's not the perfect world, but....

I appreciate your coming, and I take your feedback as legitimately trying to advance the cause here. Thank you for that.

The Chair: Mr. Eglinski, you have five minutes.

Mr. Jim Eglinski: I'm going to follow through on the same thing I started with earlier about enforcement. I notice that Australia uses the federal courts to deal with the legislation; the United Kingdom uses the information commissioner; the U.S. uses the Federal Trade Commission; and we use the CRTC. I'd like to ask each one of you to tell me quickly—in a little under 45 seconds each, as we have only five minutes—whether you think the CRTC has the proper tools and is the right enforcement body to be doing this in Canada and how you think we compare with the other countries.

Let's start with Mr. Fekete.

Mr. Michael Fekete: I'll start by providing some advice to the CRTC about helping organizations comply. The CRTC does not issue findings or decisions that provide the rationale for the fine or the circumstances in which the offence or violation took place. That contrasts with the behaviour of the Privacy Commissioner, who provides very helpful, very meaningful findings explaining the perspective of both parties as well as the commissioner's interpretation and outcome. That is what we need in order to better understand the law.

Mr. Jim Eglinski: Thank you.

Mr. Kardash.

Mr. Adam Kardash: For clarity, there isn't one enforcement body, but rather three, so it's quite complex. There's the Competition Bureau, depending on the provisions; the CRTC; and the Office of the Privacy Commissioner of Canada. In fact, depending on the nature of a particular activity, you could have multiple investigations going on. The CRTC—

Mr. Jim Eglinski: Is that a problem?

Mr. Adam Kardash: Well, it can be cumbersome. The CRTC clearly has the necessary tools to appropriately enforce against bad actors. That, again, is not our issue. Our issue is enforcement against the good actors, that and their not being subject to disproportionate penalties for technical, immaterial violations. That's it.

Mr. Jim Eglinski: Okay, thank you.

Dr. Michael Geist: I agree with Mr. Kardash on this. There are three agencies. I don't have any sense that the particular agencies themselves represent the problem at this point in time.

Again hearkening back to when we were working on the report, we met with authorities from the United States and talked to various people who were involved in groups such as the one known as M3AAWG, which brings together people engaged in enforcement activities around the world. What they needed was a Canadian representative who had the tools and the power to essentially play ball in the same way that they were able to.

For many years pre-CASL, we weren't in a position to do that. We are now, so the fault doesn't lie with the legislation, but to the extent to which enforcement hasn't been as good as it needs to be, it lies with the agencies themselves.

● (1245)

Ms. Deborah Evans: I think the enforcement agencies are the right bodies. I think they have the right tools, which I feel they may be applying in a disproportionate manner, as I mentioned in the opening remarks. We didn't receive a warning letter. I spoke to my colleagues at Porter. They had an experience similar to that of Rogers. There was no warning letter, and it went straight to the investigation and punitive damages immediately.

I think, speaking to the point of the colleagues here on the panel, that more guidance and tools could be issued from our enforcement bodies to help businesses.

That's my comment.

Mr. David Messer: I would say that the CRTC is the right body, but to some extent it is hamstrung by the legislation itself and the regulations, because it doesn't have a whole lot of flexibility in some cases because they are so prescriptive.

The other piece that's missing is that the CRTC hasn't made a concerted effort to partner with industry, to learn from industry. Some of our recommendations, those around making the private right of action focused on telecoms or other bodies that actually bear the costs of spam, would be able to bring these other industry actors into the game to help reduce spam for everyone and truly partner with CRTC.

Mr. Jim Eglinski: That's a good point.

Mr. Geist, I have a really quick question for you. I think you mentioned earlier in your evidence that in Australia the spammers were gone because there is tough legislation. Do you think that's possibly partly because the federal courts versus a bureaucracy-type agency were dealing with them?

Dr. Michael Geist: No. The evidence we received was that it wasn't about who was doing the enforcing. It was about the penalties. It was clear if you took a look at some of the weak laws, say, in the United States, just like the CAN-SPAM act, fundamentally if you were a spamming organization, you just weren't all that fussed about the law, because there weren't really tough penalties behind it; whereas Australia put some real muscle behind it, and it changed the risk analysis that those organizations engaged in.

Mr. Jim Eglinski: Thank you for that clarification.

The Chair: You have 30 seconds.

Mr. Jim Eglinski: I'll pass it on to my friends across the table.

The Chair: Well, you're passing it next to you.

Mr. Masse, you have five minutes.

Mr. Brian Masse: Maybe Ms. Evans and Mr. Messer can answer the previous question that they didn't get a chance to answer, the one I asked about the private right...the suing.

Ms. Deborah Evans: I would say the private right of action, if it were to be brought back in legislation, should focus on the deliberate actors who are doing more of the egregious things, such as deliberately disseminating malicious software, engaging in false or misleading advertising, or email harvesting. Those are really what the private right of action should focus on.

Mr. David Messer: As I mentioned previously, we would say the private right of action should be targeted toward the companies that bear the costs of spam and allow them to partner with CRTC in enforcement.

Often the networks' email providers can tell you who the bad spammers are. They are the ones in the best location to often find them, and so if the private right of action were changed to allow them to partner with CRTC, to themselves go after and recoup the costs from the spam on their own networks, that could help everyone and help the law be more successful.

Mr. Brian Masse: Yes.

I'm quickly going to go back the other way now to Mr. Geist.

One of the things that hasn't been brought up too much about the private right of action but that was mentioned by you was about Australia and others. Here's my concern. We have a model right now such that the policing of all of this still falls to the public service with the CRTC. We can't forget that the CRTC is publicly funded. That's the sole recourse for the public to actually get some type of revenue back for all this behaviour that's bad for the economy and for businesses, and that is unfair for consumers who actually subscribe and pay for all these things, and it's only through the fines that would actually be applied.

I think there's a real issue with the 30 days and not even providing notice. I think that's a real problem. That's a communication issue that's really serious, actually, especially for a larger businesses. That should be looked at very seriously by the CRTC with regard to the 30 days. That's just inappropriate in many respects. Notification would be helpful. That's the easy stuff.

If we take away the private right of action, why should the public have to pay entirely for this thing through the CRTC and through the fact that we have to foot lawsuits?

Dr. Michael Geist: I'm going to pick up on that with one other point, and that's to say that we pay not just for that but also in terms of the spam we receive. I would disagree with respect to Mr. Messer's point that somehow it's the telecom providers or the ISPs that bear the cost. No. We bear the cost, and we all know about the problems we have with affordability of Internet access and the kinds of data charges we face. When we looked at this, we saw that ISPs were up front, and they could give a per-customer cost in terms of what they were paying for the technology, the bandwidth, and the equipment they needed to deal with these issues. We pay that cost in the very high fees we face. As for the idea that somehow it's just the Rogers of the world, I'm sorry, but it's not.

In terms of the enforcement, you're absolutely right. From my perspective, it is very difficult to understand why there was a tool in the tool box that would have effectively outsourced some of this enforcement. We recognize that it would be very effective, given how nervous people are about the prospect that people would actually try to engage in this sort of enforcement, and yet we took it away and left it solely to an agency that hasn't done a good enough job, with the costs being borne by the public and the taxpayer.

● (1250)

Mr. Adam Kardash: I can speak on behalf of multiple companies, and I would add that certainly spam is hugely problematic for businesses too. They bear the cost. What we are trying to accomplish here is to reduce the cost of compliance, with the aim of the legislative scheme being that it should be focused on bad actors.

Yes, the public bears the cost—I get that—all of us do, but businesses also bear significant costs.

Mr. Brian Masse: Then the customers of the business pay the cost. It's all passed on. At the end of the day, we are the recipients of all this, paying for all this in one form or another. The sad thing about it is that you are paying for it without even being asked.

I guess that's the balance we are all trying to strike in this. With regard to the PRA, I was really surprised that.... I'm hoping the minister has the courage to go through with it and take a look at implementation, and see if we do have these problems. Right now, how many frivolous lawsuits have been acted upon? None, because...what the minister may have said, but we don't know what was even in store. It has just been based upon speculation.

Mr. Michael Fekete: The challenge with the PRA in CASL is in no small part because of the complexity of the law and the innumerable situations in which compliance is next to impossible, and because it's combined with statutory damages. If you are a class action lawyer, you make an economic decision, by commencing a suit, about whether there is likely to be a return on your investment in time. Statutory damages give that.

If you fix the legislation while enabling businesses and potentially others to enforce the law through a private right of action, you won't have the same chorus of opposition, because the legislation will be balanced. What we have now is unbalanced legislation with a very strong penalty in the PRA.

Mr. Brian Masse: We don't really know, but potentially....

The Chair: Thank you very much.

Mr. Jowhari, you have the last five minutes.

Mr. Majid Jowhari: Thank you.

I want to go back to innovation, where my colleague Ms. Ng left off, and give you, Mr. Kardash and Mr. Fekete, an opportunity to respond. I'm very clear on what Mr. Geist's position is. You wanted to interject, but my time ran out. I'm happy that I got the time back.

I now want to focus on what the specific actions for us would be if we wanted to make amendments or changes to the legislation. What should we do? What recommendations should we make to stop those innovation inhibitors?

Mr. Adam Kardash: I'll start with a basic proposition. What we are hearing from clients every day is that, anytime you have uncertainty, you have risk, and that poses a problem. It doesn't completely stop innovation—that would be an overstatement—but it introduces a level of risk in which, in our view, in the vast majority of circumstances, excluding the bad actors, you have to remove the uncertainty. Again, there is so much common ground here, and I think that's something we should really seize upon.

Part of the uncertainty is due to the fact that it's a very complex regime. We do this every day, and it takes us a lot of time to work through with clients to get very innovative types of new products and service offerings through into the digital sphere, which inevitably involves sending, or permitting to be sent, tens if not hundreds of millions of messages on a monthly basis.

None of this is illegitimate; all of this should be done in a consent regime. No one is even disputing that. What we are talking about is having clarity and removing unnecessary prescription. Then, all of a sudden, with the appropriate narrowing of the scope to keep the legitimate stuff outside the scope, focusing on the bad actors. They would be able to get the two remaining in the country, and hopefully prevent others from even thinking about coming to Canada. They wouldn't. That would be the approach.

I can't overstate the suggestion I made to the committee in my opening remarks. We deal with these every day. I urged the committee, and I urged by implication, to go through use cases, because these examples of how to fix it explode at you in their glory. Go through use cases.

● (1255)

Mr. Majid Jowhari: Can any of the witnesses submit any use cases to the clerk so we can use them?

Mr. Adam Kardash: I can't speak for others, but IAB Canada is going to submit a more detailed brief. With respect, three pages is not sufficient for us to provide the range of types of use cases and other suggestions. We will present use cases so the committee can see how there is unnecessarily expansive scope. We'll get rid of that, and then, with the narrowing of the scope, there will be a lowering of temperature in terms of opposition to the legislation thereafter.

Mr. Michael Fekete: I agree with what Mr. Kardash just said, but I would like to provide an example of why the computer program provisions are too broad. If you're a start-up company and you're deciding whether to start up in Silicon Valley or in Waterloo, you look at the laws and at how they apply. Computer program installations and updates are a core part of your business. If you set up in Canada, your worldwide operations are subject to these prescriptive rules that have no parallel anywhere else. We're creating an incentive for people to set up in the U.S. I think we have to look at harmonization to the extent that is appropriate to ensure a level playing field. We want to encourage the Canadian technology sector and not have laws that interfere with it.

Mr. Majid Jowhari: Thank you.

The Chair: That will bring us to the end of our session today. I thank all the witnesses for a very spirited day of questions, answers, and presentations. We'll be sure to take all of this into consideration.

Committee members, we have witnesses coming in on Thursday as well as next Monday. So we have the next two sessions of witnesses.

The meeting is adjourned.