HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 082 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, November 7, 2017

Chair

Mr. Dan Ruimy

Standing Committee on Industry, Science and Technology

Tuesday, November 7, 2017

● (1105)

[*English*]

The Chair (Mr. Dan Ruimy (Pitt Meadows—Maple Ridge, Lib.)): I call the meeting to order.

Good morning, everybody. Welcome, on this beautiful sunny cold day in Ottawa, to meeting number 82 of the Standing Committee on Industry, Science and Technology, as we continue our study on Canada's anti-spam legislation.

Before we begin, I would like to do a quick shout-out. I know some of us are participating in the Big Brothers Big Sisters shadow day on the Hill. Can we just get the Boys and Girls Clubs people to stand up?

Look at all these folks, new to the Hill, shadowing their MPs. Welcome to our committee. We hope to keep you entertained with our theatrics.

Today we have Kim Arsenault, senior director of client services at Inbox Marketer.

We have, very intriguingly, from Interpol, Louis Lau, digital crime officer in the cybercrime directorate, all the way from Singapore. I have to give you credit; it's midnight over there. You have it worse than we do.

Then, from Spamhaus Technology, we have Chris Lewis, chief scientist.

We'll start with Louis Lau, from Interpol.

You have eight minutes to present to us. Go ahead; the floor is yours.

Mr. Louis Lau (Digital Crime Officer, Cybercrime Directorate, INTERPOL): Thank you, Mr. Chairman and fellow members. Thanks for inviting me to this statutory review of Canada's anti-spam legislation.

I am Louis Lau, police officer from Hong Kong, seconded to Interpol. I was invited to perform the function of digital crime officer under the cybercrime directorate of Interpol. My work station is the Interpol—

The Chair: I'm sorry, Mr. Lau, just one second. We're getting some volume issues here.

Let's give it a shot.

Mr. Louis Lau: Let's try again.

The Chair: Thank you. That's excellent.

Mr. Louis Lau: My work station is the Interpol Global Complex for Innovation in Singapore. In fact, I am in Singapore right now.

The role of the cybercrime directorate is to provide operational support to member countries in the area of cybercrime investigations. The main functions of the cybercrime directorate include assisting member countries in coordinating and facilitating investigations into transnational crime and focusing on pure cybercrime—botnets, malware, and high-end cybercrime enablers, such as bulletproof hosting services, professional remittance services, or DDoS.

I understand that we are here to discuss the anti-spam legislation. Please be aware that from the perspective of the cybercrime directorate of Interpol, we do not focus much on anti-spam activities. Instead, we focus on criminal investigation. However, I can provide details in the context of cybercrime, since a lot of cybercrime originates from spam emails.

Among these, one of the most typical examples is the business email compromise, the BEC fraud. Email fraud spamming is one form of normal commercial spamming activity. Of note is that we are not talking about normal and commercial spam emails, which only contain commercial messages and do not contain any attachment or malware. Most BEC fraud, which we sometimes call the “CEO fraud”, starts with spam emails.

Before going further into these emails, we need to understand the modus operandi of such crime. For most situations, the CEO, or any high official of the company, receives spam emails with a malicious attachment. If someone executes such an attachment from the spam email, it allows their computer to be compromised. The culprit, after being able to access the email account of the CEO, through reading the emails studies the operation of the company, the way the company spends money, and even the style of email writing of that CEO. The culprit will then choose optimum timing—for example, during the vacation of the CEO—to send fraudulent emails on behalf of the CEO to order payment to specific bank accounts.

This modus operandi that I mentioned was further confirmed from the BEC cases provided by member countries who asked for assistance from Interpol. It can also be confirmed from a proactive investigation that Interpol participated in. In 2016, with the assistance of experts from external companies, we carried out reverse engineering on some malware samples that we found on common spam emails. We found that the attachment of the spam email, after being executed, would equip the function of capturing the email log-in credentials from the victims. With detailed analysis of the behaviour of the malware, we were able to dig out some of the clues that led to the identification of the suspect who controlled the malware. Eventually, we were able to fully identify the suspect through open-source investigation. The same information was passed to the law enforcement agency in the country where the suspect was situated. At last, in June of 2016, the suspect was arrested.

After the arrest, our unit was further asked to assist in the examination of the notebook computer seized from the suspect. The sending of spam emails in order to phish for compromised email accounts from victims was further confirmed. Evidence suggested that the suspect downloaded millions of email addresses and used specific software to send out bulk junk emails in an automated manner. The content of the email was very simple:

> Good day,
> Final invoice copy attached.
> Best regards,
> xxx

A file named “invoice” was attached to the email. We carried out further analyses on this attachment file and confirmed that it was malware. It had the capability to steal email credentials from victims.

● (1110)

After stealing email log-in credentials, the suspect logged in to victims' computers and their email accounts and breached their email. There was evidence that suggested the suspect logged in to some of the accounts over 200 times within a few months, and hundreds of emails were compromised.

There was also evidence to suggest that the suspect modified invoices that he very likely obtained from the compromised email accounts. In his computer, he amended the bank account details of the original document, with a view to deceiving the financial staff into depositing money into malicious accounts.

Interpol did not collect crime figures from member countries, and I'm afraid that I cannot give you detailed quantitative statistics. However, Interpol got feedback from member countries that the issue of BEC has been one of the types of crime of most concern recently.

Interpol has organized two international conferences recently, one in Spain in June and one in France in October, both concerning BEC fraud. A total of 60 participants from 30 countries participated in the meetings and raised concerns about BEC.

That's all.

The Chair: Thank you very much.

We're going to move to Ms. Arsenault.

You have up to eight minutes.

Ms. Kim Arsenault (Senior Director, Client Services, Inbox Marketer): Thank you, Mr. Chair and committee, for the opportunity to be here today. My name is Kim Arsenault. I'm senior director of client services at Inbox Marketer.

We are a data-driven email marketing services and technology solutions company, and we've been leaders in the email marketing space for over 15 years, servicing clients across North America and into Europe. We've been at the forefront of CASL for over eight years, working closely with the Canadian Marketing Association as part of the 2005 federal task force on spam as well as with Industry Canada to help educate companies on what it means to be CASL compliant.

The good news is that three years post-CASL, the clickstream data that we have reviewed from a cross-section of our clients compared to one year pre-CASL indicate that email metrics have improved overall in terms of engagement rates, bounce rates, unsubscribe rates, and deliverability into the inbox. This is largely due to senders adopting better list hygiene practices that have resulted in better-quality email lists and less sending to unsolicited or invalid email addresses.

In our opinion, since the implementation of CASL in 2014, Canadian email marketers have become more disciplined in their email operations, and legitimate marketers in Canada have taken CASL very seriously. Responsible marketers have adapted by being more diligent. We have seen them create task forces and appoint individuals to actively manage CASL compliance through regular spot checks, technology integrations, and organizational training.

With that said, we do have a few concerns we want to bring forth to the committee today.

The first is the economic burden that CASL compliance is placing on many Canadian businesses. It is costing them anywhere from tens of thousands of dollars to millions of dollars, depending on the size of the organization, to properly be able to update their processes and technologies to be CASL-compliant. These are just process and technology costs. You also have to factor in the resource costs of continually training and educating staff on corporate compliance.

A related concern is that even when businesses have implemented corporate compliance programs and updated their processes and technology, it's still very unclear what exactly is required in terms of record-keeping, which is very problematic for organizations that are attempting to comply with the law. The CRTC has issued general guidance with respect to compliance, but has also repeatedly stated that companies are free to interpret how to apply effective record-keeping to their situation.

The fact is that companies are having to invest a lot of money and resources into setting up their systems and processes based on their interpretation and educated assumptions, only to risk finding out that these may not be acceptable in the event of a CASL challenge. It would be very helpful if the government could provide clear guidance and specific examples on exactly what type of record-keeping practices would be acceptable in order to provide assurance to organizations that the time and resources they are expending are bringing them into full compliance with the law.

Second, we are still seeing that many organizations do not view CASL as a straightforward or intuitive piece of legislation. It's confusing for many companies, and for those who are not deeply familiar with it, it becomes a nebulous beast to try not only to understand it but also to consistently train their employees on what they think is correct.

Three years later, we are still consulting companies that are seeking clarification on what the difference is between implied and express consent. Due to the ambiguity and lack of clarity and guidance that has come from the government, we have seen some organizations eliminating the email channel as of way of communicating with their customers and prospects. We've heard from various financial and insurance companies, for example, that before CASL, they had sales teams and advisor teams that were using the email channel as a way of communicating offers and valuable content to their existing customers. With CASL fully in force, the fear and anxiety experienced by some organizations because of the lack of clarity and inaccurate information out there has inevitably caused them to eliminate email as a communications channel.

The email channel, for many years, has proven to give a 40:1 return on investment. Numerous studies continue to show that consumers prefer the email channel as a way for brands to communicate with them, so when a large organization eliminates the email channel for fear of not being compliant, it can have a very large impact on an organization.

Our third concern is that the regulators took years to write the CASL legislation. It started in 2004, and as we all know, it came into force in 2014. Technology moves at a very different pace. Marketing, for example, has changed more in the past five years than it has in the past 50 years, and the next five years are unpredictable in terms of how fast technology and digital media are going to evolve. We cannot have Canadian businesses in today's day and age relying more on vehicles like the phone, which are more expensive and less efficient than email and social media, because they're too afraid of what might happen when they use email. That's exactly the scenario that some Canadian businesses are in today.

● (1115)

CASL's objective is to promote the efficiency and adaptability of the Canadian economy. Having organizations eliminate the email channel or deciding not to market into Canada is not supporting this objective.

Many ask what the regulators are doing to keep up with the pace of technology and social media. The guidelines around how CASL applies to social media are extremely vague, yet social media are evolving rapidly. For example, more than half of the world's population is now online, which includes 2.7 billion active social media users. The fact is that digital and social marketing are a central part of a brand's tool kit today.

I have some further recommendations to be considered. The regulators need to allocate time and resources to keep their website updated and provide a lot more clarity on the issues that follow.

First, what constitutes a CEM, a commercial electronic message? This is not clear for many. This could be a newsletter, for example, where the content is focused around the credibility and knowledge of the organization. If the logo in the top left-hand corner links to their website, which then promotes commercial activity, does that make the newsletter commercial? It's unclear. Additionally, the fact that purely transactional-type emails are being considered a CEM under subsection 6(6) is extremely confusing, difficult to implement, and unnecessary. The recommendation is to remove subsection 6(6) entirely from the act.

Second, the regulators should provide more clarity on what is and is not allowed on social media so businesses can properly leverage those channels as part of their tool kit.

Third, the regulators should provide full transparency on what is required for proper record-keeping. Organizations should have comfort in knowing if their $4-million solution is going to be one that the CRTC will accept.

Last, the regulators should remove the confusion and requirement around six-month versus two-year implied consent. They should clearly define what express versus implied is and remove the time frame of six months and two years. It's a big challenge for many companies, both small and large, to properly maintain this level of detail that can be constantly changing and updating. Not all technology solutions out there are equipped to properly document this.

If you think of a large enterprise company that has multiple lines of business—multiple customer relationship management systems, multiple CRM systems—and they all have a business need to communicate with their customers, many of these customers are going to cross over the various lines of business. To expect that all messages are going to be managed and controlled in one central spot is not realistic for many organizations today.

It is also very confusing for many organizations regarding what scenarios allow for six-month versus two years implied, so what we've seen is that some organizations only allow express consent to communicate. The impact of this is that organizations are losing out on opportunities to grow their business because they don't fully understand how to rely on implied consent. There's too much fear, risk, and uncertainty for them.

Thank you again, Mr. Chairman and the committee, to have the opportunity today to share with you some of the impacts CASL legislation has had on Canadians and Canadian businesses.

● (1120)

The Chair: Thank you very much.

We're going to move now to our final witness.

Mr. Lewis, from Spamhaus Technology, you have up to eight minutes.

Mr. Chris Lewis (Chief Scientist, Spamhaus Technology Ltd.): Thank you, Mr. Chairman. *Bonjour* and good morning.

My name is Chris Lewis. I'm the chief scientist at Spamhaus Technology, which is part of Spamhaus, one of the largest and most well-respected sources of Internet threat intelligence in the world. While most of you may not have heard of us, more than half of the Internet is using our data in one way or another, whether it's branded as Spamhaus or not.

Unlike most of the people speaking to you on the subject of Canadian spam, I work deep inside the technology itself. To me, this is a 24-7 effort, and with the technology we use, I am seeing on the order of 750 million to a billion email spams a day through systems I administer to try to analyze what's going on and come up with solutions to stop it.

I worked in Ottawa first as senior security architect for Bell Northern Research, which later of course became Nortel, from 1991 through to 2012. I've been working on spam in one way or another since about 1993. By the time the 1997-1998 time frame rolled around, it became obvious that email was the battlefront that needed to be saved for the Internet to prosper and email to continue.

Since that time, I have focused primarily on spam, malware, and botnets, as opposed to the deliberate sending of email that did not have permission, but specifically on the technical side of stopping some of this. In 2003, I developed a new technology that greatly increased the effectiveness of our filtering at Nortel, which required vast amounts of data from all over the Internet. I would analyze this data coming in from partners and people who contributed this data, turn it around, and give it back to the Internet for free. That's how that continued for many years. Then late in 2012, Nortel downsized to the point where they no longer needed me to run a mail server for 50 people, and so I transferred to Spamhaus the next day.

I am one of the founding members of the Coalition Against Unsolicited Commercial Email, CAUCE. I have been invited to speak at the Federal Trade Commission spam panel; advised on the U.S. CAN-SPAM Act, am a founding member of the NCFTA- FBI Project SLAM-Spam; won an award from the FBI for my efforts in helping secure U.S. government networks; was invited to be a senior technical adviser for the Messaging, Malware and Mobile Anti-Abuse Working Group, or M3AAWG; belong to many technical working groups targeting specific spam and malware; have trained and assisted with many law enforcement regulatory groups around the world, including the CRTC and organizations in the Netherlands, Australia, the United States, and many other countries; and am a member of the London Action Plan, which is now called UCENet. Don't ask me what that means, because I've forgotten.

Currently Spamhaus is supplying to Public Safety's CCIRC, free of charge, a very large dataset of spam attacking Canadian email addresses, which they use for a number of purposes, including prosecutions through the RCMP and the CRTC. They're also using it as a way of alerting Canadians to infections of their systems, and they periodically give out reports telling providers, and in some cases individuals, that they have been infected with something and how to resolve it.

I'm speaking here primarily on spam, though other forms of online abuse are just as big, if not bigger, and more dire. The malware fraud and phishing scenario, as has already been somewhat alluded to before, is as big a problem, and they're all getting worse.

Of particular interest here is that much of my time as an adviser to M3AAWG was spent with the email sender community—with Inbox Marketing, and so on—helping to come up with best current practices on how to manage subscriber lists, when you have permission and when you do not, and I was heavily involved in drafting part of the M3AAWG sender best common practices, BCPs, which are still being updated and published. The BCPs are considered to be one of the industry's most important set of guidelines that most of the large sender community is already complying with. In fact, a sender organization can't be a member of M3AAWG unless they comply with it.

● (1125)

It raises the question that if most of the industry is complying with the M3AAWG BCPs—which to a very real extent are mapped directly on CASL, with the very same principles and the very same things—why is there such a concern about compliance?

I'm going to go on to some specific facts and details from the last few years.

We operate email sensors that monitor, in one sense or another, billions of emails per day via arrangements with providers. We also run our own infrastructure to receive email that is being sent to people who no longer exist on the Internet. A particularly good example is some email addresses that were at Nortel many years ago. Public Safety's CCIRC now owns those domains, and they have asked us to operate them as if there were still a user base there. We can see what spam comes out, see where it's coming from, identify correlations, and publish information to our customers—in many cases for free—on how providers and so on can protect their users from this stuff.

Over the past seven years, there was a peak in 2011 of 10 billion spams per month, with peaks to 750 million per day on our own servers. This was not the big cloud of contributed data, but the stuff we run ourselves. Most of this was the Rustock botnet, which was infamous for high volume, with fake pills and fake brand name watches. The latter is just fraud, but the first one is dangerous, because many of these pills were analyzed by people we know in the industry and found to contain, literally, street sweepings and so on. Whatever they could squeeze together and dye blue, they would sell.

For a few years after that, the volume averaged around three billion spams per month, because the Rustock botnet was taken down by efforts from a number of organizations on the Internet, as well as the FBI. Over the past year, the volume has climbed almost all the way back up to 10 billion per month. Instead of fake pills and watches, it's ransomware from the Necurs botnet and Russian dating spam. Also from the Necurs botnet, which is even more disturbing, is the ransomware we hear about on the news, the type that encrypt hospitals' entire datasets so that they cannot get them back or have to spend an enormous amount of money to get them back.

Still, within those enormous volumes of that sort of dangerous material, there are very high volumes of affiliate spam advertising legitimate, semi-legitimate, and outright fraudulent companies and products from people who have no concept of privacy—those who hire hackers to steal and provide them with email addresses, phishing, and so on.

Industry leaders such as SenderBase Talos, which is actually part of Cisco, have long been sources of reliable, “on the wire”, real statistics, and they generally tend to agree with our numbers. We don't expect them to agree exactly, because everybody's spam sample is different—it is surprising how differently it can vary from one place to another—but the trends, spikes, and everything else, we coincide with exactly.

I've had the opportunity to monitor the volume of email and spam received by some of Nortel's old domains for almost 20 years. I built and ran the mail servers that handled them when they were in service and for the 18 years they have been defunct. As I mentioned earlier, those domains are now owned by CCIRC as a national threat resource, and they have requested that we operate those domains for them.

By 1997, Nortel decommissioned these domains and moved all users to the main email domain that Nortel was using at the time. In 1997, there were three million emails per month, of which 40% were spam; by 2001 there were four million, all of which were spam; by 2003 there were seven million spam messages, and by April 2016 there were 150 million. Today it is 350 million per month. This is a 350-fold increase over 20 years.

You're asking yourself, “Did my spam volume go up by that much?” No, it hasn't, but it is only because of efforts by your ISPs and organizations such as ours that it has lessened.

● (1130)

The volumes keep growing. Spammers game our systems, and it's very difficult to continue.

I'm being waved at, so I'm going to cut this a little short.

One of the issues with CASL is the private right of action. One of the things we want to be able to deal with is a situation of individuals getting very high volumes. An associate of mine had an email domain for himself and his wife, and one day it started receiving a million email spams a day. We don't know why. I have some suspicions, but we have no solid information as to why that happened. The volume was so high that he couldn't even run his own server anymore, because it was costing too much. PRA gives him a chance to deal with this.

To finalize, spam is not a technical problem but a human problem, and it has to be dealt with from both aspects.

The Chair: Thank you very much.

I only have an English version of your document. We're going to get it translated and make sure that everybody gets it, because there is a little more in here. We'll make sure it gets passed around once it has been translated.

Having said that, thank you to all three of you for your presentations.

We're going to jump right into it, starting with Mr. Longfield.

You have seven minutes.

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

Thanks, everyone, for coming from far away. From Guelph, it's great to have Inbox Marketer here.

I want to touch on what we've been hearing in testimonies about separating technical from fraudulent from normal activities.

Ms. Arsenault, I know you are a co-founder of Inbox. You've seen the development of email marketing over the past few years. You've mentioned in your testimony already that CASL has helped with the efficiency of email marketing.

I'm hearing that you see a need for CASL, but also that there's some confusion around interpretation. Could you expand on the efficiency that has been gained and how CASL has helped with efficiency?

Ms. Kim Arsenault: I think from the efficiency standpoint, it has enabled marketers to look at their email community and take out any of the addresses that were unknown. As we were consulting with a lot of companies, we had to audit their database and inquire about where they got permission for all the records. For anybody they didn't have permission for or for whom they didn't know the source of the opt-in, we recommended that they take the conservative approach and just suppress.

What we found is that when CASL came into force, marketers and brands were forced to remove email addresses that were maybe not of good quality. In the email marketing space, some brands go for quantity over quality, and it forced marketers to drop their list sizes. Some list sizes went from a million records to 200,000 records, but those 200,000 records are now engaged, relevant people who want to be in the database. Now their email marketing programs are working a lot harder for them, so it's more efficient, because all of their practices are getting them a higher return on investment at this point.

It has been efficient in that way, and we agree that there have to be regulations on how we use email. There have to be restrictions on it. However, CASL has been way too onerous and costly for organizations, and it's too complex. A law like this shouldn't be that complex, and three years later we shouldn't have companies coming to us asking what the difference between "implied" and "express" is.

● (1135)

Mr. Lloyd Longfield: I'll share a question with you and Mr. Lewis about the consulting that happened before CASL and whether the consulting has continued to go on as technology changes.

Is the group that met before CASL still getting together from time to time?

Mr. Chris Lewis: Informally, there have been some discussions. Naturally, for example, since I have been consulting directly with CRTC, they are evolving. What they are dealing with is evolving. They themselves are learning. There's a very steep learning curve in trying to deal with this, so they are getting better at it.

One of the things that struck me when I first saw the draft CASL back in 2012, I guess it was, was that it covered everything, and it was written in a way that it could be extended as necessary for the technology.

I do not think that the law itself is too narrow or too restrictive. It's more a matter of education and deciding when this particular area becomes a problem and where you allocate your resources.

Mr. Lloyd Longfield: Thank you.

Do you have anything to add?

Ms. Kim Arsenault: No. Once CASL came into force, the task force wasn't actively involved. We've let the legislation ride and are waiting for the three-year post-opportunity.

Mr. Lloyd Longfield: Okay, terrific.

We've been considering and looking at the details of private right of action. Mr. Lewis, you talked about private citizens. We're having trouble getting the voice of private citizens to this table in how private right of action might apply. Can you separate the legitimate and semi-legitimate businesses from the fraudulent businesses, and how that might happen?

Mr. Chris Lewis: I believe protection is built into the law about the private right of action. For example, there's the CRTC, the Privacy Commissioner, and the competition branch's ability to override an individual lawsuit. The laws in Canada are fundamentally different in this regard from the United States. Some of the abuses that we have seen in the States—and indeed they have been abuses—are not likely to be an issue here. It gives individuals a chance to deal with things that the CRTC, the Privacy Commissioner, and the competition branch may not be able to tackle because it doesn't meet the statutory requirements for the number of complaints or the number of people being attacked, and so on. The situation I was referring to in a nutshell was he could do something about it in law, but it would cost him $10,000 to get a lawyer to be interested.

Mr. Lloyd Longfield: Okay. Thank you.

From an Interpol standpoint, on the private right of action we compare ourselves to the States just because we're close, but when you're on the net, membership doesn't matter. Is this a best practice from other countries we can learn from in enforcing private rights of action? Do you know through Interpol whether that's more broadly used by some of your member countries?

Mr. Louis Lau: We don't have many studies about this. I'm not sure I can share some of my experiences with you, but as I mentioned, we focused mainly on the criminal investigation. As I said, spamming is one of the major sources of a lot of cybercrime, especially BEC or the ransomware that we mentioned before.

Mr. Lloyd Longfield: We only have 20 seconds left, so thank you to everybody for coming. I have a lot more questions, but I'm sure my colleagues will be grabbing on to some of my thoughts as well.

The Chair: That's excellent. Thank you.

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

You have seven minutes.

Mr. Jim Eglinski (Yellowhead, CPC): Thank you.

Mr. Lau, have you looked at the spam regulations in Canada? If you have, how would you compare our regulatory control to other countries that you deal with internationally? Are we better? Are we worse? Do we need to improve?

● (1140)

Mr. Louis Lau: Anti-spam legislation is still not being enforced in some countries, especially developing countries. I'm not able to comment on the Canadian legislation in a very professional manner. I have done a lot of assessment of different countries—for example, some of the developing countries—and anti-spamming legislation is not very common in that part of the world. I think it's a good move to have the implementation of anti-spam law, and I also support the consulting process that we are having here right now.

Mr. Jim Eglinski: Okay. Thank you.

Have you and Interpol worked with any cases in Canada or with any of our agencies, say the CRTC?

Mr. Louis Lau: Our main concern is cybercrime, the actual crime that arises from spamming, and we have organized a number of international conferences to address this issue.

In the conference we held in Madrid, in June, Canada was one of the countries that expressed a concern about business emails being compromised. We sat together and discussed how we could deal with this situation. That is all the involvement we had with Canada.

We know Canada is keen to work further with Interpol and with other countries to tackle the problem of businesses being compromised. We are now working on a number of follow-up operations.

Mr. Jim Eglinski: Mr. Lewis, you told us your background. It's quite impressive, and you have been involved in the industry for a long time.

Since this legislation came out in 2012, do you think it has hindered industry and businesses, or do you think it has helped them? Do you think it is complicated? We've heard from some witnesses that it's complicated and costly. I'd like to know your opinion.

Mr. Chris Lewis: I was part of the FASTF deliberations back in 2005-2006. I consulted when they brought it in, and I have watched industry follow it. It has surprised me that some of the companies seem to be going a little overboard with compliance.

I have to think that various people are making more of it than they need to, perhaps because it's legislation rather than best practices. I don't see this as being any different from basic industry practices. We can see that the EU has regulations almost as strong as ours, as does Australia, and the European ones are about to get a lot stricter. We have to consider where things are going elsewhere. It has always struck me that people have gone overboard.

Currently, when I give my email address to a Canadian entity, I know it's not going to get sold. This has changed. It used to be that they just it spread all over the place, and there was no way of controlling it. It is much better now than it used to be.

Mr. Jim Eglinski: Ms. Arsenault, we had a witness a couple of meetings back who gave us a cost breakdown. You also gave us a cost breakdown, which was pretty loose—$10,000 to millions of dollars. That's not what we heard before. I wonder how you justify those amounts, because we were told that in some smaller companies it was $600 to start up with the advice and information and then $200 to $300 a year to continue it and check it out. Could you clarify what you said earlier?

● (1145)

Ms. Kim Arsenault: Yes, I can. We work with a lot of financial and insurance companies and some big global brands. A big financial institution might have upwards of 40 different CRM databases, and the law states that you have to track down to the individual every single communication they receive and what they subscribe to and unsubscribe from. If you have upwards of 40 CRM databases across a global company, that does not cost $1,000 to integrate.

Companies we have advised and spoken to have told us they have had to invest over $5 million in technology to update their systems so that they can track the level of permission that CASL has asked for—implied versus express, six months versus two years. Then, of course, smaller organizations have smaller databases. They don't have as many CRM databases, so the cost to them is a lot less.

There is also the cost to train employees and the cost of the time this takes. A lot of clients and brands have had to seek legal counsel because they're not confident in their interpretation of the law, and it's costly to seek legal advice.

Mr. Jim Eglinski: It grows as the cost of business is growing, as a firm grows.

I think I'm almost out of time.

The Chair: You're over time and in the penalty box.

Voices: Oh, oh!

The Chair: We're going to move to Mr. Masse, who I believe will be submitting a notice of motion.

Go ahead, please.

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

It's a simple notice of motion to allow this committee to participate in a process. I'll just read it, and I understand that it will be for future business.

Since there have been new and recent revelations of massive tax evasion in Canada through several media reports and since there is a government bill currently in the Senate that offers an opportunity to immediately implement specific measures that would improve Canada's ability to address tax evasion and money laundering, the motion to the industry committee is:

> That the House of Commons Committee on Industry, Science and Technology develop amendments to be referred to the appropriate Senate committee through correspondence that will review Bill C-25, An Act to amend the Canada Business Corporations Act, the Canada Cooperatives Act, the Canada Not-for-profit Corporations Act, and the Competition Act, that would address issues of fiscal transparency in Canada, including tax policy, beneficial ownership, and banking regulations.

Essentially, this is for future business. It could be a letter that this committee sends to the Senate, for example.

Thank you, Mr. Chair. I'll go to questions when appropriate.

The Chair: Go ahead.

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

Mr. Lau, one of the things we're studying with CASL here is—and I come at this from the perspective that especially when it comes to your own personal devices, be it your mobile phone or your computer, you pay for the service and the physical device, and you take your own time to administer that—that sending unsolicited email and information to someone is a privilege and not a right somebody should have, given that it involves a cost to someone else.

I'm concerned about the additional cost of spam to people's personal privacy and security.

In your business, do you see that heightened? Is there a greater threat, through spam, of undermining people's personal privacy or of invading financial records or other things? I'm worried about the continued exposure for consumers and Canadians and those in the rest of the world to illegal activity through spamming.

Mr. Louis Lau: Let me clarify a bit. Are you concerned about the effect or about the ability of the spamming emails to cost individuals?

Mr. Brian Masse: Is the threat getting more complicated and worse to deal with in terms of stuff that comes through spam that could compromise your privacy and your personal information?

● (1150)

Mr. Louis Lau: I think first of all we need to distinguish between two kinds of spamming emails. Some spamming emails focus only on business information, and some spamming emails have documents or files attached to them. We are basically focusing on those spamming emails with attachments. There are a lot of different forms of attachments that can be sent through the emails.

As we mentioned before, some of the emails contained the software called malware, and in my situation, which I explained before, we have evidence regarding the suspect who conducted the business email compromise. The malware he sent was capable of obtaining the log-in credentials of the email accounts. For example, if you accidentally click on that particular email with that attachment, the log-in credentials of your email account would be leaked to the suspect. Then the suspect was able to look into your email account, which you wouldn't notice. He kept on monitoring your email account for a long period of time so that he could find the optimum time for impersonating you and for sending emails to some people from the finance department in order to get some monetary reward. This is only one of them.

We also have some situations involving ransomware. It is also commonly sent through spamming emails. If you execute those files, some of the files in your computer would be encrypted so you would have to decrypt them on your own. You would either have to pay for the decryption tools or use your own means to get the decryption tools. Otherwise, the files will be encrypted permanently. In this respect, Interpol is trying to help victims to get some of the decryption tools.

These are two common activities.

Mr. Brian Masse: We have a choice right now. We're reviewing legislation. We can sharpen the legislation, we can keep the status quo, or we can loosen it, which I guess would allow more potential for spam. I'm just trying to boil this down to simple basics.

Right now, if we actually loosen the law.... Do you think the exposure to consumers and people and their privacy on issues like ransomware has grown in the last couple of years? This bill is really three years old, but by the time we actually gazetted it.... It's only been in operation for a couple of years. Has the threat to Canadians and their privacy lessened in the last number of years? If we decide to loosen the rules on it, is that threat essentially going to lessen in the years to come, or is it going to increase?

I know you can't predict the future, but in your professional opinion, what do you think is going to take place?

Mr. Louis Lau: I would suggest that we can look at this matter at two different levels. First of all, there are the messages sent from people in the business sectors. They don't have malicious intent when sending out those emails. Maybe those are for a commercial purpose, but they're just abusing the system. This is one form of it.

What we are talking about here are the people who obviously have a malicious intent when sending out those emails, so what I am talking about is focusing on those people. For these kinds of people, I think that even with the most comprehensive legislation, you can't stop them from sending. The most effective way is to do it from the infrastructure level. We do it from either the ISP level or the infrastructure level to block these kinds of emails. This is the most effective way.

When we're trying to understand this situation, we need to understand that those origins are different. These are two totally different types of spamming emails that we're talking about.

Mr. Brian Masse: Thank you very much.

The Chair: Thank you.

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

Mr. Frank Baylis (Pierrefonds—Dollard, Lib.): Thank you, Chair.

I'd like to examine the malicious emails a little more in speaking to you, Mr. Lau and Mr. Lewis.

One of the main objectives of CASL was to help curtail malicious emails. Mr. Lau, in terms of your interaction with Canada, one of the things CASL was supposed to do was facilitate the international sharing of data. Have you come across that issue or that need? Can you speak to that issue about your communications with Canada?

● (1155)

Mr. Louis Lau: As I mentioned, Canada participates in some international conferences concerning business email being compromised. They're very keen to work with Interpol and other countries in tackling these issues. I must say that currently we don't have established systems to share case information with Canada or other countries that have the same concern, but—

Mr. Frank Baylis: You don't have those systems to share data because you're not set up to receive it or because Canada is not sharing it? Is it because Interpol is not set up yet to receive the sharing of data?

Mr. Louis Lau: Yes and no. We don't have the systems to share it. Also, we need to consider how we will work on the shared data even if we eventually, let's say, have the systems to analyze it.

I understand that the situation is a bit different from the European countries. At Europol, they have the systems. Their situation is that the countries in the EU have the systems and the people to do the analysis of the data. Europol is a bit different from Interpol.

Mr. Frank Baylis: Thank you.

Mr. Lewis, one of the points that was brought up again in talking about malicious emails and penalties is that some witnesses said there should be stricter penalties if the activity is malicious, as opposed to an inadvertent error. For example, let's say Rogers sends out 100,000 emails by accident and there's no phishing or spyware involved. They say that this should have a type of penalty that would be different from the type of penalty for an email that's malicious in intent. What are your thoughts?

Mr. Chris Lewis: The law already has provisions for a lot of that material, for a lot of that sort of thing: if there's an innocent mistake, you write a letter and tell us you're not going to do that again. That's actually in the law.

It strikes me that it's fairly gentle in that sense, in that someone can avoid major penalties, or any penalty altogether, if they can establish they were operating reasonably well and were doing reasonable things, and they simply made a mistake. For example, there are the override provisions from private right of action across to CRTC and so on.

I think the law is pretty well done that way. It is reasonable. It's not, "You did this, and it will cost you this amount of change." It's not done that way. From a background of—

Mr. Frank Baylis: Fair enough. Moving on, in your experience in looking at old Nortel emails and all that, do you see a reduction of spamming originating in Canada? Do you look at it that way, if you follow me?

Mr. Chris Lewis: We do. I'm specifically looking at botnets, but I do see what's going on elsewhere. There is considerably less of what you would call "white spam", which is somebody making a mistake and sending out stuff they shouldn't have. We're seeing the criminal side. There is more grey. More black is predominating. We are still tracking down people who are running botnets with a Canadian affiliate, and that sort of thing. We're seeing a lot of that. We're tracking back all sorts of stuff to Canadians. We're tracking all sorts of stuff to Canadian hosting, which is where the CRTC has been doing really well in being able to go to a hoster—

Mr. Frank Baylis: You're seeing malicious ware, not necessarily originating in Canada but from a company that has affiliates in Canada. Is that what you're saying?

● (1200)

Mr. Chris Lewis: An example is advertising fake pills. These are being done by groups of people, many people, who when they send out their spam will have a link on it so that when someone follows that link to the illegal pill site, there's a cha-ching that gives the affiliate a penny. It's that sort of thing.

The other form is when I said hosting—

Mr. Frank Baylis: And that affiliate is a Canadian affiliate.

Mr. Chris Lewis: And that affiliate was Canadian.

Mr. Frank Baylis: Is the CRTC, to your knowledge, taking any action against any of those things you're seeing?

Mr. Chris Lewis: They are. I don't know if any of them have gone all the way through yet, but they are looking at that.

The other thing they are working on, at a less than "in front of a judge" level, is dealing with Canadian hosting environments or hosting providers who provide web services to someone when, through one way or another, they take on part of a criminal spamming infrastructure, meaning that the website for pills is there, or a command and control point for malicious botnets—

Mr. Frank Baylis: Is the way CASL is written, specifically for this type of malicious activity, strong enough? Does it need to be more enforced, or are there changes—

Mr. Chris Lewis: It's quite good. The CRTC needs more time and experience in dealing with them.

Mr. Frank Baylis: You're saying the law is good, but CRTC could do more to go after these people. Is that it?

Mr. Chris Lewis: Yes. It's a matter of experience and time and working away at it. Mr. Lau is not seeing it, but I'm seeing how the CRTC is interacting with international organizations, law enforcement, and regulatory bodies.

Mr. Frank Baylis: You're seeing that they do—

Mr. Chris Lewis: I'm seeing it. There's a lot more going on than we used to see.

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

[*Translation*]

Mr. Bernier, you have five minutes.

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

[*English*]

My first question would be to Ms. Arsenault.

[*Translation*]

Good morning, Ms. Arsenault.

[*English*]

The costs—it's all about the costs. You explained, in answer to the questions from my colleagues, about the costs for big business, but for a small or medium-sized business that wants to do good marketing, what would be their option to be in line with the legislation and respecting it? Do you have any clients that are small and medium-sized businesses? Do you know what they are doing to be in line with the legislation?

Ms. Kim Arsenault: Yes. We talk a lot about the level of risk that organizations are willing to take. A big financial institution with a big brand is going to have a very low level of risk, whereas a smaller organization might be willing to take a little more risk, so its policies and procedures may not be as tight as those of a big corporate brand. We see that a lot of them are following typical industry best practices. Even though they might not be able to do everything as a strict reading of what the law says, they feel comfortable enough if they are following legitimate industry email best practices—sending to people who have expressed interest in receiving email from them, sending relevant content, and suppressing unsubscribes. Then it's a little easier for them to take advantage of the email marketing initiative. For them, the costs are not going to be as high.

Again, with a big brand, they have to have the technology so that if they are called upon, they can actually prove exactly what version of any email has gone out.

Let me give you an example. Some of the large organizations want to send a million different variations of an email. They're beyond the "batch and blast", in which everybody gets the same message. Some of these big companies are trying to figure out how they are going to set up their system so that if they are called upon, they can prove the exact variation of any email that any customer was given on any day. That's difficult to do. The smaller organizations aren't that sophisticated.

Hon. Maxime Bernier: You are asking for more clarity in the guidelines from the CRTC and the government.

Ms. Kim Arsenault: Absolutely.

Hon. Maxime Bernier: Okay.

Mr. Lewis, you are offering your services to big government organizations, but my understanding is that the public cannot have access to your software. Could you explain the process for a small business, if they want to be as secure as the government organizations? How are they going to be able to have access to the kind of technology you are offering to the government?

● (1205)

Mr. Chris Lewis: Spamhaus offers its threat intelligence data to individuals and small organizations for free. It always has. We are all believers in doing that. However, when we get into a big organization, we figure that we are saving them millions of dollars and making their customers happier. It costs us money to run our organization and to buy equipment, so they need to pay for it. All the small guys get it for free, though.

All the country-based incident response teams get our data for free so they can help secure their countries. CCIRC gets our data for free. CRTC gets some of our data for free. We are doing a lot of that. Not very many other companies do that; some do.

In terms of small companies trying to protect themselves, they can use our data as we suggest. They can go with other organizations that have similar data or with software techniques. We tend not to require the user to buy software. They are buying the information and they are using the software they already have to use it, but there are other solutions that do a much better job.

Hon. Maxime Bernier: Do you think that in the private sector there are a lot of corporations that can offer these services to the small and medium-sized businesses?

Mr. Chris Lewis: Yes. In fact—as she was referring to with the question about how small organizations do their marketing and whether they are going to worry about trying to do it themselves—there is a burgeoning market of companies that are specifically intended to run mail and marketing campaigns for small companies. Some of them are free, or virtually free. You can use their machinery, their software, and their stuff, and for very small amounts of money you can be pretty sure that you are very close to being fully in compliance with CASL.

Hon. Maxime Bernier: Thank you.

The Chair: Thank you.

Mr. Jowhari, you have five minutes.

Mr. Majid Jowhari (Richmond Hill, Lib.): Thank you, Mr. Chair. I will be sharing my time with Mr. Lametti.

Thank you to all the witnesses.

Mr. Lewis, I'm going to focus on the PRA and ask you some clarifying questions.

From previous testimony, we heard that we should probably narrow the focus of the PRA and make sure the punishment fits the crime. In your remarks, the way I understood it, you talked about other elements that are in place that don't make it necessary for the scope of the PRA to be narrowed. You talked about the innocent mistake provision and the override provision.

You specifically talked about the fact that CRA has the ability to override. You also mentioned that the laws are different in Canada and the U.S. Can you expand on how CRA can override, and how it's been effective, as well as on the differences in the laws?

Mr. Chris Lewis: Did you say the CRA?

Mr. Majid Jowhari: Sorry; I meant the CRTC. It was my mistake.

Mr. Chris Lewis: Okay.

As I understand it, if you raise a private right of action against company X and then CRTC or the Privacy Commissioner or the competition branch decides that this a situation they wish to deal with, then the private right of action goes away.

That's my understanding of the way the law works in that regard. The CRTC can supersede a private right of action.

Mr. Majid Jowhari: How would one determine that?

Mr. Chris Lewis: Well, for example, if CRTC saw that I was suing someone for doing something, the CRTC could say it was a result of a larger issue or something like that, and then they would institute an investigation. Then the private right of action is suspended.

Mr. Majid Jowhari: Okay.

How about the difference between the laws in Canada and the U. S., then?

Mr. Chris Lewis: My understanding is that one of the main differences is that Canada is a loser-pays environment, whereas the United States is not. What that means is that enormous amounts of money can be made by showering people with spurious lawsuits, because they'll often back out.

I believe one of the situations that happened was in Nevada. A legal firm had gone to a prison and got the people in the prison to say they were subrogating all their private right of action rights, in terms of spam, to this legal firm. Then, with every email they got, the legal firm was making enormous amounts of money suing people. As I understand it, that can't happen here.

● (1210)

Mr. Majid Jowhari: Okay.

I am going to ask Mr. Lametti to ask a question.

Mr. David Lametti (LaSalle—Émard—Verdun, Lib.): I guess it's in a similar line. It's on the private right of action.

Would you restrict it to actual damages that people have, or would you maintain the statutory damages?

Mr. Chris Lewis: I would maintain the statutory damage, in that it can be extremely difficult to prove certain things. What it should really be is, “I was sent this after I told them to stop.” That should be sufficient, as long as the court, on a case-by-case basis, thinks that's plausible.

It has to remain relatively broad, because it should not just cover email spam, which is what CASL partially covers. The other thing CASL covers is distributed denial of service attacks of various varieties. If you narrow it down to email spam, then you're leaving out your neighbour deciding to blow your computer off the air. They can do that now, and dealing with it legally would be very difficult.

The private right of action allows you to do something about it, because it's an unsolicited message that you were being sent. It's covered.

That was why I mentioned earlier in my presentation that I was so pleased this law was written to cover just about everything we could possibly think of. So far, it still would, in a very real sense, and this is 12 years or 13 years later. That's not bad.

I wouldn't change it so much. I would make sure that there were some limitations, perhaps, on abuse of it, but I think the broad breadth is about right.

Mr. David Lametti: Okay.

Similarly, on the private right of action, how do you feel about the class action potential?

Mr. Chris Lewis: That does make me nervous.

In the case of a private right of action, I wouldn't mind seeing that have a further.... You know, three years down the line, we'll allow private right of action. I do like the way that we sometimes bring these things in stages: "How is it going so far?" "It's not bad; let's turn it up another notch, and if that doesn't work, we'll back off." Since we have the mandatary reviews in the law, there's an opportunity to do that.

I really wouldn't want to do class action right now on PRA. Let's go with the individual ones.

The Chair: Thank you very much.

We're going to move back to Mr. Bernier.

[*Translation*]

You have five more minutes.

[*English*]

Hon. Maxime Bernier: *Merci beaucoup.*

My question would be for Mr. Lau. Thank you very much for being with us via the technology.

I have a short question about the relationship that Canada is having with other countries to work with you and your organization.

Do you think we need to have a new international treaty? Is the treaty that we have to share information and work together sufficient right now, or do we need to update what we have with other countries, with our relationship with Interpol?

Mr. Louis Lau: I would say that the current situation is sufficient in most cases. Currently we have established systems for sharing information and connecting different police forces to the platform of Interpol. I would say that is sufficient for general purposes.

For spamming information in particular, I would suggest and I would welcome more communication between Canada and other countries, but in terms of a criminal investigation or sharing of case information, I would suggest that the current system provided by Interpol is sufficient.

● (1215)

Hon. Maxime Bernier: Thank you.

I will share my time with Jim.

The Chair: You have three and a half minutes.

Mr. Jim Eglinski: I'm going to share one question with both Ms. Arsenault and Mr. Lewis.

Suppose today is your big day, and you know what CASL stands and what's in the legislation. What's the one thing you would change today if you had the opportunity to change it? That's to either one of you.

Ms. Kim Arsenault: Get rid of the six-month and two-year requirement.

Mr. Jim Eglinski: Would you explain why?

Ms. Kim Arsenault: It's an unnecessary complexity for a lot of organizations. Consumers don't necessarily understand the "implied" relationship, and it's difficult for organizations to manage. It's unclear for a lot of companies what defines six months versus two years, so the impact is that some organizations don't rely on implied consent at all, which loses them opportunities. I think it simplifies it to get rid of the six-month and two-year requirement.

Mr. Jim Eglinski: Mr. Lewis, would you comment?

Mr. Chris Lewis: I mentioned being impressed with the law when it was first proposed, and I still am. There are a couple of operational things that I would tweak: resourcing, stability, and better interactions. I wish PRA was in place. Things probably do need to be clarified better, but I think the law is pretty darn good just as it stands.

Mr. Jim Eglinski: You're good with it, while Ms. Arsenault would like to see one change.

How much time do we have left? Not much?

The Chair: You've got one and a half minutes.

Mr. Jim Eglinski: Ms. Arsenault, you deal with clients. Do you think that the clarity of CASL is adequate, or does it need changes in certain areas to make things—

Ms. Kim Arsenault: I don't believe it's adequate. As an agency, we do a lot of consulting, so our clients are well equipped in terms of what needs to happen to be CASL compliant, but a lot of organizations that we don't work with come to us and ask us for advice. It's way too complex. There's a lot of ambiguity. There are contradicting points in the legislation.

I think the government can do a much better job in clarifying the legislation and not leaving so much up to interpretation. I think what makes it difficult for organizations is that it's up to them to interpret the law, and it needs to be a little more black and white.

Mr. Jim Eglinski: I think I have a few seconds left for Mr. Lewis.

The Chair: You have 30 seconds.

Mr. Jim Eglinski: Do you think that some companies are making it overly complex, as you said, especially the larger companies? It seems that when the bigger legal branches get into it, it becomes more complex.

Mr. Chris Lewis: I've been very close to the law for very long, and it strikes me that complying is simpler than it appears. There are really only four operative sections in the whole thing, and the rest of it is just infrastructure underneath it.

Yes, it needs clarification, but I think a lot of people are making it more complicated than it needs to be. In some cases, I think they're doing it in order to extend their own business opportunities.

The Chair: Thank you.

We're going to move to Mr. Sheehan.

You have five minutes.

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

The first question is to Kim.

In your statements you mentioned how CASL was applicable to social media, such as Facebook and other messaging. We've heard back and forth in different testimony, and there certainly was some confusion out there: it did apply; it didn't apply. Then we did hear from the Competition Bureau that, yes, it does apply to those forms of electronic messaging.

Could you describe, in your opinion, the difference between social media messaging per CASL and email? We spent a lot of time on email, but how exactly is CASL affected in social media?

Ms. Kim Arsenault: What we are asked a lot is, "Are we allowed to use social media platforms like LinkedIn as a way of communicating in the B2B environment?" There is a lot of uncertainty as to whether people can use LinkedIn. The email address is conspicuously published. Does that give me six-month implied, does that give me two-year implied, and does that fall under the B2B exemption?

There are many unknowns as to how to use LinkedIn. Some organizations, instead of reaching out, are just picking up the phone and using traditional ways of prospecting and making sales. It's not efficient in today's day and age. We require more clarity on how businesses, mostly on the B2B side, can leverage social media channels like LinkedIn to properly engage in email communications. There are way too many unknowns on how to use those tools.

● (1220)

Mr. Terry Sheehan: Chris, do you have a comment on the social media platforms?

Mr. Chris Lewis: One of the fundamental differences between social media and email is that social media is a pull—you actually have to go looking for content to do something with it—whereas email is a push. I send email to you, whereas with social media, I've gone someplace to see something.

Where the line gets is blurred is something like LinkedIn, where you've gone on the platform to maintain your professional relationships with someone else, and then someone starts sending you advertisements for something. That sounds an awful lot like push, whereas in general, little companies have their Facebook pages, their friends, their colleagues, and they write comments about the food they have and all that sort of stuff. That's very much a pull. That's not being slammed in my face. It's not requiring me to spend money that I wouldn't normally have spent to deal with it. It's purely voluntary. I have opted in by using my eyeballs on it. I've actually gone looking for it, whereas sending unrelated advertising to a LinkedIn account is a different thing. In fact, especially in the example of LinkedIn, the only thing that's really appropriate for LinkedIn is advertising for job offers.

Mr. Terry Sheehan: Thank you.

Kim, we've heard testimony over and over again about businesses feeling it is ambiguous, because of the lack of education or the lack of communication. We did have the CRTC here to state that a lot of its questions are on the web, but it's very passive. You have to go looking for it and whatnot. Many businesses are opting out of engaging in electronic marketing, or they lawyer up, and the lawyers say, "Don't even take a risk."

Your business is basically in the business of educating people, and helping them where the government perhaps isn't there. What advice could you give the government on how it might do a better job of educating the public?

Ms. Kim Arsenault: I don't think the government's website is actively updated as often as it could be, so its website is one low-hanging fruit. It could probably put out more webinars. I've joined several webinars, and sometimes the questions aren't directly answered, so even the answers to the questions are ambiguous. To Mr. Lewis's point, the government needs a bit more time and experience to fully understand digital media and how CASL is impacting the law.

A lot of the government's answers have been, "Use your interpretation and use your judgment." That's very difficult for companies that don't want to take a lot of risk. It makes them fearful that if they interpret it in the wrong way, it can have huge impact on their business.

Again, it needs to provide more black and white, more specific examples, and fewer grey areas that are open to interpretation. It should provide more webinars and papers and it should also consult with organizations. Many organizations are fearful to go to the CRTC for fear they might raise something inadvertently with the CRTC. Many companies want to stay under the radar, so having the CRTC appear more open to conversation may help organizations.

The Chair: Thank you.

Mr. Terry Sheehan: Those were great comments.

The Chair: Mr. Masse you have two minutes.

Mr. Brian Masse: Thank you.

One of the things that we're still faced with is the repercussions. If I receive an ad in the mail, I have to pay for the recycling of it through my municipality, and I have to pay with my time. If I receive an ad on TV, it doesn't infect my TV with a virus. It's my time and my space. I can change the channel. I can turn it off.

Suppose I receive a legitimate ad that I've agreed to from PlayStation, for example. The problem is when my privacy is breached later on, which it was.

What are the real repercussions then in terms of the engagement that we have in the protection of privacy and its use? There are two things. What do you think is fair for consumers to get out of this, especially in terms of unsolicited electronic messaging and the cost to them. What do you think is fair?

The inundation of advertising is not what the communication devices were really set up for. The way that they're used now is for emergencies and a whole series of other things, as well as the common stuff. For my phone to be tied up by a virus from an unsolicited email is not only an inconvenience; it can be quite a problem because it can't function in the meantime. What do you think is fair for consumers in this relationship? I would appreciate your input on that.

● (1225)

Ms. Kim Arsenault: I agree that consumers need to be protected from some of that malicious activity. What we're seeing is that the legislation has impacted legitimate email marketers who are trying to do a really good job of sending consumers in Canada relevant offers and relevant content, and, in the B2B environment, of being thought leaders and producing really good content. Legitimate marketers want to protect their consumers as well by being engaging and relevant.

Mr. Brian Masse: You call them “legitimate”. Fair enough, but what really gives them the right to basically tie up, destroy, or cause damage or privacy loss in the first place?

I understand your arguments about the CRTC needing to reach out more and so forth, but it seems to me that we have this backwards to some degree. The cost isn't borne by those sending the messages; it's borne by the people receiving them. If I'm engaged in a relationship whereby I've agreed to receive your email, or I haven't agreed, and your message ends up costing me time, money, and other things, what do you think would be fair for me as a consumer to get out of that?

Ms. Kim Arsenault: It's a great question—

Mr. Brian Masse: It's the responsibility of those who are marketing to pay for that restitution.

Ms. Kim Arsenault: Absolutely. I don't think that PlayStation expected to be hacked. I believe they were trying to protect their consumer data as well as they could. The reality is that the digital world is evolving more quickly than a lot of people suspected, and there's malicious activity. Mr. Lewis could probably speak better to it than I could.

The Chair: I'm sorry. I'm going to have to cut you off. I've let it go on a little too long. You will have another seven minutes, though.

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

The Chair: We've come to the conclusion of round one, and we have time for a few more questions. We're going to go back to Ms. Ng for seven minutes. Then we'll go to Mr. Masse, and then back to Mr. Baylis.

Go ahead, Ms Ng.

Ms. Mary Ng (Markham—Thornhill, Lib.): Hi, there. Thank you to all the witnesses for coming in. I have just a couple of clarification questions.

Ms. Arsenault, you had talked about CASL being able to provide a framework that allows for better data and better emails and therefore better business for marketers. Then you provided some suggestions for simplification of the current legislation around the definition of a CEM or by getting rid of the six-month and two-year aspects.

The question isn't actually for you; it's for Mr. Lewis, and that's the context.

Ms. Arsenault sort of suggested that she, her clients, and so forth want to engage in good practices. They want to enable small, medium-sized, and large enterprises to do good marketing and to do business in today's digital world.

Do you agree that the simplifications she is suggesting are the right tweaks to CASL to help it be more effective for the business community, while at the same time ensuring that the protections, as they are intended, are there and will continue to be there?

Mr. Chris Lewis: I'm not exactly sure what two periods she was referring to. Is that something to do with...?

Ms. Kim Arsenault: It was the six-month inquiry versus the two years of EBR. If someone makes an inquiry on a form, you have six months of implied consent, whereas if you have an existing business relationship and download—

● (1230)

Mr. Chris Lewis: Okay.

Ms. Mary Ng: We did hear both of those suggestions. We've heard from other witnesses. I would be interested in your perspective about whether that makes sense.

Mr. Chris Lewis: As long as the user has initiated it as opposed to the other side initiating it, a reasonable timeout of six months to a year.... I don't see that you necessarily want to make it more complicated by making it different for different circumstances.

Ms. Mary Ng: What we heard was that the ability for enterprises to keep track of when they received the consent, whether express or implied, and the requirement for businesses to keep doing that as time continues—

Mr. Chris Lewis: That's always struck me as kind of strange. I'm a long-time customer of our bank, and every once in a while I get another query asking if I accept to continue receiving this, and I say, “The fact that we're dealing with you at least a dozen times a year makes this kind of silly.” A six-month or a year's timeout on a business transaction or an inquiry is the sort of thing.... They should be keeping the permission alive indefinitely. It doesn't need to be renewed.

Ms. Mary Ng: You're saying that's an acceptable modification to CASL, that it would help—

Mr. Chris Lewis: Yes. I'm in fact sure that if CRTC were presented with something that hinged on that thing alone, they'd say, “It's case by case and you're a reasonable person. You've done your due diligence and you've done a reasonable job, so what's the problem?”

Ms. Mary Ng: That's good. Thank you.

On the one hand, Ms. Arsenault, you talked about the need for CRTC to be clearer with some direction to businesses. Mr. Lewis, you talked about CRTC working its way through and getting better at its role in CASL.

What needs to happen? In other words, do we say to CRTC that what we've heard from a lot of testimony is that there's a lack of clarity and businesses certainly could use more direction and clarity in the interpretation, whether it's webinars or just communication—that it's just the clarity, and CASL itself is fine—or do we actually have to do something?

Mr. Chris Lewis: I think one aspect of the problem we're seeing today is that when you talk to an individual person at CRTC, if they're not a lawyer and they don't speak for CRTC, they're not going to judge specifically one practice versus the other.

I'm wondering whether it would be better for CRTC to try to express more along the lines of, "This is what we're trying to achieve. If you do your due diligence and follow the basic principles of what we're trying to do here, then you will be safe."

Ms. Mary Ng: Would that help? We have heard that from a lot of the testimony that came in, and I take your point, Mr. Lewis, about the magnitude of what we might be hearing. I'm trying to understand it to see whether we can come to a good balance that provides consumer protection on the one hand, and ease of businesses to do business, while at the same time recognizing that email spam is actually the first point of very malicious and fraudulent activity that we have to be very concerned about.

Mr. Chris Lewis: It's a matter of making sure the basic principles are understood. Then from there, you say what is reasonable within those principles. The law is always trying to set concrete limits, but human beings in courts work on basic principles and on what's reasonable—what a reasonable person would do, due diligence tests, and so on. Educating people on how to understand and deal with that in an area that's never seen this sort of stuff before can be a long and time-consuming process.

Ms. Mary Ng: What we heard was about a pragmatic way, perhaps by the CRTC, to make sure there is pragmatic information that contemplates and considers how businesses work and provides practical application, interpretation, communication, and understanding so that those who are operating small and medium-sized businesses have the tools and the interpretation they need without having to hire a legal team to try to understand what this piece of legislation is intended to do.

● (1235)

Ms. Kim Arsenault: I agree.

Mr. Chris Lewis: Also, written interpretive documentation might help.

Ms. Mary Ng: Okay.

Ms. Kim Arsenault: Show examples. The record-keeping is a big thing. Show us exactly the level of documentation that is required if we're called upon.

Ms. Mary Ng: Sure.

Do I have time?

The Chair: That's it.

Ms. Mary Ng: Thank you.

The Chair: We're going to move to Mr. Masse for seven minutes.

Mr. Brian Masse: Thank you, Chair.

Mr. Lau, what can Canada do better to improve the chances of getting to some of the international spammers and some of the content that we get in our country? Before we had this law known as CASL, Canada was known as being one of the havens for spamming. In fact, we were one of the genesis areas for much of the international stuff that took place. Is there something that we can do better or that can work in a stronger context?

One of the frustrations we're hearing is the excuse that it happens so much from international sources and what we do here really doesn't matter at all, so we may as well just loosen restrictions here, because it's happening from Nigeria or somewhere else. I don't subscribe to that philosophy, because I don't think that's a solution at the end of the day, but what things can we do, either by sharing our experience or by joining organizations or resources or whatever? Are there any suggestions you can provide?

Again, I view this a little differently, in the sense that receiving electronic messaging in documentation, especially unsolicited, is a privilege, and it should not be a right for somebody to do that, because you own and control and contribute financially through your device. Can you provide any suggestions with regard to our country?

Mr. Louis Lau: Maybe I can try to provide that from a practical point of view. You probably heard me mention that Interpol works with one of the west African countries. We were able to analyze the computer of a particular suspect and found that the suspect was using some automated programs on the Internet to send out spam emails. Imagine that you input some of the fake personal data in that program and then that email automatically sends out thousands of emails to different recipients.

This program is supposed to be operating in some sort of server in some of the physical locations, right? If it's operating in Canada, let's say, how can the authorities or the law enforcement agencies tackle it? Also, if this sort of server or service is not operated in Canada but is being controlled by Canadians, is there any provision for the Canadian authorities to work with other jurisdictions or the law enforcement agencies to tackle these kinds of services? I think those are the facts.

Mr. Brian Masse: That's interesting, because we haven't really thought of that too much. I want to get this right. There could be a program, service, or technology developed here in Canada that is exported and then becomes a tool to re-import spam and other unsolicited messages through, I guess, our own technology coming from our country.

Mr. Louis Lau: There are different perspectives. Either it can be developed in Canada and then operated in other countries, or it is developed and also operated in Canada. When considering legislation, I think we need to look into this aspect. This is more about the criminal aspect, and it is really malicious.

Mr. Brian Masse: That's the focus, but unfortunately one becomes a vehicle.

Mr. Lewis, I'm sorry. I didn't mean to ignore you today—

Voices: Oh, oh!

Mr. Brian Masse: —but there has been very good testimony from both of our previous witnesses.

What can CASL do? There is an argument out there that I've joked about that maybe we need a *CASL for Dummies*. I have some empathy. The playbook or the rule book should be really clear so that people can understand. That's one thing. I do think there is an onus on a business to understand this, though. At the same time, it does seem a little difficult, or some of the decisions seem a little unclear. Can that happen on its own, just with time, or are there things that we can sharpen right away to make that defining much clearer?

● (1240)

Mr. Chris Lewis: I'm not sure. There are a lot of players. They're all at different places in their understanding. There are people who are going to make more of it than they need to, for various reasons. The basic principles, the important items, need to be made clear. Then the person has to say his goal in running his company is to follow those basic principles, and here are some of the things he should be thinking about. It should be made clear to him that as long as he's doing a reasonable job, he's in pretty good shape.

For a large company it's the cost of doing business. They have to expend more effort on this, because it's a bigger thing. The issues for the smaller companies that are sending out a couple of hundred or a couple of thousand a month are smaller and should be much smaller, but there is a cost of doing business, because, after all, sending out a million emails is a lot cheaper than sending out a thousand postal messages.

Mr. Brian Masse: That's just it. That's the problem. There is very little cost for those who want to do it.

What disturbed me a little with some of the testimony we had earlier was that we had lemonade stands and cousins couldn't communicate and things of that nature. We're trying to get an understanding about managing a serious problem within the context of the legislation or an understanding of what needs to be changed, because change in the legislation could create even more problems.

Mr. Chris Lewis: Absolutely.

Mr. Brian Masse: I think that's one of the things that has been discussed too much

Mr. Chris Lewis: Yes. The cases we've seen go before the CRTC have not been problematic in that area at all. We're not seeing any lemonade stands being prosecuted by the CRTC. They're all large organizations that either made mistakes or deliberately did things they really shouldn't have.

The penalties from a corporate standpoint seem to have been appropriate. I brought one of the cases that the CRTC successfully prosecuted. I said these are big guys and they're important people. They're not bad people, but they should be made to be a little more careful on this particular aspect. They said giving them a sting is what they intended to do, so that they wouldn't do that any more. Lemonade stands are not going to have large things land on them.

The Chair: Thank you very much.

We are going to move back to Mr. Baylis for the final shot.

Mr. Frank Baylis: Mr. Chair, I'll be sharing my time with both Mr. Longfield and Mr. Sheehan.

The Chair: Okay.

Mr. Frank Baylis: Mr. Lewis, there's a bit of a dichotomy in some of your testimony. On the one hand you're saying it's not that hard to understand CASL and that people are making more out of it than what it is. They shouldn't be spending these millions of dollars or tens of thousands or hundreds of thousands, as Ms. Arsenault says, and then you swing back and say you'd also like to see the prior right of action have that big hammer hanging over a company.

If I'm a company and I could be facing $10 million in penalties and then also facing prior rights of action, I am going to spend a lot of money. Certainly if someone comes in here and says they have a solution for $695, if I've got a big organization, such as Rogers or Bell, I'm not going to implement a $695 solution. It makes no sense that something that simple will protect me against potential penalties and lawsuits can easily run into the millions. How do you balance those two positions you hold?

Mr. Chris Lewis: Part of it is seeing what has been happening over the years and the inability of people to deal with specific problems unique to themselves and at the same time knowing how much of an opportunity email has brought to large-scale marketing. There needs to a brake on the massive overkill that sometimes we can see.

As somebody once commented, if every small company in Canada figured they had one kick at the can per year, you'd have a quarter of a million emails in your inbox all the time.

● (1245)

Mr. Frank Baylis: We've heard from so many of the corporate witnesses that this is hard to understand. Ms. Arsenault, you've just said that when you sit down with the CRTC, you walk away still scratching your head.

This question is to both of you. I'll go to you and then go back to you, Mr. Lewis. You mentioned the definition for an electronic message and things like that. Could we really simplify it so that I could get it easily, as Mr. Masse said? It would apply to me—*CASL for Dummies*. I know he was looking at me when he said that—

Mr. Brian Masse: How about *CASL for Geniuses*?

Mr. Frank Baylis: How would that help, Ms. Arsenault?

Ms. Kim Arsenault: I smiled when you said that. *CASL for Dummies*, I think, is a great idea.

I'm not from the legal side, but I think any law should be fairly simple to understand so that we can abide by it. Drinking and driving is very black and white. In this CASL legislation there is way too much that is open for interpretation, so I think the CRTC, which I've worked with, needs to better understand it themselves, and then—

Mr. Frank Baylis: You're saying it's hard for them to understand because it's too open for interpretation, and you'd like to see a lot of things tightened up.

Mr. Lewis, would it make sense to you to tighten up a lot of these definitions, such as the definition for a CEM?

Mr. Chris Lewis: The main thing I'm concerned about is that by tightening up the definitions, you may be subjecting smaller and medium-sized organizations to more work than they need to do. You'd be making something appropriate for a large organization and trying to apply it to a small one or a very small one, such as a one-person company, so I'm a bit hesitant about saying "This is the record you must keep for every single email." For 99% of these organizations, that's overkill.

Mr. Frank Baylis: What about the electronic messaging? You just gave an example of a newsletter that has a logo, and if you click on the logo, it pulls you into something. The newsletter wasn't a commercial message, but the logo click-through is. What if we just cleaned up things like that?

Mr. Chris Lewis: We have seen things presented as non-commercial that end up being highly commercial, because that's what organizations will try to do to get some of their stuff in front of people.

Part of the issue in this technology is that things are so complicated that you intentionally have to leave the law vague in certain areas; otherwise you're not going to cover what you should be covering.

Mr. Frank Baylis: Okay. Thank you.

I'll pass it on to Mr. Longfield.

Mr. Lloyd Longfield: Thank you, Mr. Baylis.

On these topics I'd love to drill down further, but I want to take advantage of having Mr. Lau on the phone from Singapore. Thank you for staying up so late to talk with these Canadians who are scratching their heads on this legislation.

We heard testimony from one of the officials from the Canadian government that 50% of global email traffic is spam, at least in this year. Does Interpol keep track of global spam? Do you know where the lawsuits are being prosecuted and which countries are the leading sources of spam? Do you keep records on that type of thing?

Mr. Louis Lau: We don't have any special units in Interpol for doing those kinds of things, but I can give you one example of how spam emails were involved in cybercrime. We did an operation in the ASEAN region early this year, and with the assistance of some private companies we were able to identify about 8,000 malicious servers.

Just to give you an idea, among those 8,000 servers, over 7,000 were sending spam emails. The remaining 1,000 were involved in ransomware, banking scams, and other things. It is very common in the cybercrime field for criminals to use compromised computers and servers to send out spam emails.

● (1250)

Mr. Lloyd Longfield: Thank you.

I think the picture forming in my mind, based on the testimony we've heard, is that we have legislation but we also need technical solutions. We actually need both. We need to know what we're trying to trap, how we're trying to trap it, and how to find technical solutions for those multiple servers that are trying to attack our market.

Mr. Louis Lau: I totally agree.

In fact, the methodology and the techniques that were operating behind these 7,000 servers for sending spam mail were actually very complicated. They operate in an automatic way, so I agree with you that we need some sort of technical support.

Mr. Lloyd Longfield: Thank you very much.

I'll pass my time over to Mr. Sheehan.

The Chair: You have about a minute.

Mr. Terry Sheehan: Thank you.

Sticking with Louis, I will just follow up.

The United States, New Zealand, Australia, the European Union, and the U.K. all have anti-spam legislation. Would you be able to indicate to us what country you think has the most effective anti-spam legislation and perhaps maybe another country that I didn't list there?

Mr. Louis Lau: I'm sorry, but I'm not in a very professional position to comment on this, because I haven't spent much time studying others. If we really need to, we can come back and talk to you at a later stage.

Mr. Terry Sheehan: That would be appreciated.

Mr. Louis Lau: We have some studies.

Mr. Terry Sheehan: Okay.

Thank you very much.

The Chair: On that note, Mr. Lau, we'll let you get some sleep, unless you're going to patrol the streets of Singapore.

I want to thank all the witnesses for being here today. Clearly there's a lot to think about. I think we have a task ahead of us. Thank you very much for coming in.

I will just remind everybody on the committee that this Thursday we will have the CRTC in for the first hour. In the second hour, we will go to IP. I believe you've all received a copy of draft number 3. Expect to find the translated recommendations revised perhaps today or tomorrow and then hopefully we can wrap that up *tout de suite*. That would be great.

On that note, we get to leave a few minutes early.

Have a great day.

The meeting is adjourned.