HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Industry, Science and Technology

INDU • NUMBER 083 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, November 9, 2017

Chair

Mr. Dan Ruimy

Standing Committee on Industry, Science and Technology

Thursday, November 9, 2017

● (1105)

[*English*]

The Chair (Mr. Dan Ruimy (Pitt Meadows—Maple Ridge, Lib.)): Welcome, everyone, to meeting 83 of the Standing Committee on Industry, Science and Technology as we continue our study on Canada's anti-spam legislation.

Today we have with us, from the CRTC, Neil Barratt, director, electronic commerce enforcement; Steve Harroun, chief compliance and enforcement officer; and Kelly-Anne Smith, senior legal counsel. We have an hour.

Steve, you'll be our main MC guy, I believe?

Mr. Steven Harroun (Chief Compliance and Enforcement Officer, Canadian Radio-television and Telecommunications Commission): I guess so.

The Chair: All right. You have 10 minutes, and then we will go into questions.

Mr. Steven Harroun: Good morning and thank you, Mr. Chair, for providing us with another opportunity to appear before you as part of your review of Canada's anti-spam legislation, known as CASL.

My name is Steven Harroun, and I'm the chief compliance and enforcement officer at the CRTC. I am joined today by my colleagues Kelly-Anne Smith, CRTC senior legal counsel, and Neil Barratt, director of electronic commerce enforcement.

We have followed your proceedings closely, and welcome this chance to comment on some of the recommendations for changes to the legislation that the committee has heard. We know that concerns were raised by many witnesses about various aspects of CASL. Despite their criticisms, the legislation is largely effective. You heard repeated testimony endorsing that view during your hearings—from consumer advocates, various technical experts, and academics.

As we explained during our first appearance, it is important to keep in mind that CASL came into force only three years ago. In that short time, the CRTC has built up its expertise in cyber-threats and computer forensics. We've operationalized the spam reporting centre and taken enforcement actions against companies in violation of the law. As such, while the review is welcome, we believe it could be counterproductive to open up the legislation in these early days. Businesses have invested in compliance programs and systems based on CASL as it is currently written. It would be costly and burdensome to review and modify those systems now.

[*Translation*]

Even though it is still early days, we think the legislation has already proven its worth. You heard from our colleagues at the Department of Innovation, Science and Economic Development that only one year after CASL's implementation, a third-party study showed there was 29% less spam email in Canadians' inboxes, and a 37% reduction in spam originating from Canada.

Internationally, Canada is no longer in the top 10 spam-producing countries. And according to some sources, since CASL came into effect, it is no longer in the top 20.

We believe strongly that any challenge or burden of compliance needs to be balanced against the significant consumer and privacy benefits CASL provides.

[*English*]

This doesn't diminish the perception among some witnesses that compliance is challenging. There's no question that adapting to new legislation takes time and effort. As we outlined the first time we addressed this committee, that's why we publish substantial guidance and conduct regular outreach to both consumers and businesses to assist them. They are coming to the CRTC's website to find information. Our spam- and CASL-related pages attracted nearly 100,000 visits last year alone. In fact, we designed numerous guidance documents and tools specifically to address issues that witnesses raised with your committee, including the installation of computer programs and compliance for SMS messages.

Guidance comes in many forms. For instance, since our last appearance, the CRTC published a decision related to a company called Compu.Finder. Among other things, the decision provided extensive guidance to industry on the business-to-business exemption, unsubscribe function, implied consent, conspicuous publication, and due diligence.

It's true that our early enforcement efforts have mostly targeted major senders of commercial electronic messages. This was based on the scope and volume of complaints and targeted by the commercial sector to encourage broad-based compliance, all of which is consistent with our mandate under CASL. However, what's overlooked is that a lot of our work actually protects businesses and consumers from malicious threats. As one example, we assisted with the takedown of a command and control server infecting computers around the world. We also work with organizations whose email servers have been compromised—sending out unwanted, malicious, or fraudulent emails—to help them clean up their infrastructure.

What concerns us is that witnesses have made statements about the chilling effect CASL has had on business, something that we believe needs to be put into perspective. Creating exemptions for every situation, even when well-intentioned, would only make the legislation more difficult for businesses to understand and for the CRTC and our partners to enforce.

More to the point, large companies have a duty and the resources to appropriately comply. Your committee heard from Canadian entrepreneurs and innovators that market-based solutions for CASL compliance exist. It's up to businesses to use them.

We also disagree with the assertion that CASL increases cybersecurity threats and risks. We collaborate across government to ensure that our activities feed into a comprehensive approach to Canadian cybersecurity.

One final issue I want to briefly touch on is the criticism of the legislation's opt-in requirement. Committee members undoubtedly recognize that in today's challenging online environment, it's even more important that consumers consent to any application installed on their devices. The opt-in regime was adopted after extensive study, including a broad review of international best practices. Experiences in other countries with opt-out regimes have been less than successful. Transitioning to an opt-out regime at this point would be complex and have significant consumer impacts. It would also negatively affect our ability to use the intelligent tools we have at our disposal, including the spam reporting centre.

For all these reasons, Mr. Chair, we think it would be prudent to adopt a cautious approach at this time when it comes to making amendments to the act. We firmly believe that CASL's current regime is adequate and effectively promotes the public good, and that the committee should allow it sufficient time to achieve this goal.

We'd now be happy to answer any questions you or your committee members may have.

● (1110)

The Chair: Excellent. Thank you very much.

We'll move right into questioning with Mr. Baylis for seven minutes.

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

Thank you for coming.

You're correct that we heard an awful lot of different opinions on CASL. If I understand your first statement, you're suggesting that we don't change anything?

Mr. Steven Harroun: I would suggest that it's early days. It has only been in force for three years.

Mr. Frank Baylis: I understand that, but we heard a tremendous amount of testimony about what I thought were great opportunities to improve, clarify, and simplify. Are you saying that all that testimony was non-valid?

Mr. Steven Harroun: I would suggest that there are definitely opportunities for tweaks. I would caution against a complete overhaul of the legislation.

Mr. Frank Baylis: So there are opportunities for tweaks.

Mr. Steven Harroun: Absolutely, based on the witnesses and the testimony you heard.

Mr. Frank Baylis: Okay. I just wanted to clarify that.

I'd like to delve in on penalties. First, what penalties have you applied to date, what size, and against who?

Mr. Neil Barratt (Director, Electronic Commerce Enforcement, Canadian Radio-television and Telecommunications Commission): As you know, we have a range of different tools at our disposal, from warning letters to notices of violation and administrative monetary penalties. If you're referring specifically to monetary penalties, in total we've issued about $2.5 million's worth of administrative monetary penalties in the three years that CASL has been in force.

Mr. Frank Baylis: How many people; how many companies?

Mr. Neil Barratt: Those have been issued to five different companies.

Mr. Frank Baylis: Five companies: and how many warning letters?

Mr. Neil Barratt: Over the three years in total, we've issued 22 warning letters.

Mr. Frank Baylis: You've issued 22 warning letters and five penalties totalling $2.5 million. Are there any other things you've done in that section?

Mr. Neil Barratt: Yes. When a party is interested in voluntarily coming into compliance, we have the ability under CASL to negotiate an undertaking with them, which can include a monetary payment. It also often includes a robust compliance program, and it's done on an—

Mr. Frank Baylis: This is a forced negotiation, where you go to the company and say “We need to talk.” Is that what you're talking about?

Mr. Neil Barratt: It's not forced. It's up to them if they would like to enter into an agreement with us. It gives us the ability to flag concerns that we have with the company and then allows them, if they choose, to start a discussion with us. We share the information we have with them about what we see as potential violations, and then we can come to an agreement.

Mr. Frank Baylis: One of the suggestions that came up quite a lot —from very small companies, from people who were both pro-CASL and anti-CASL, if I can say it that way, and from very large companies—was that there should be a gradient built in, with a warning letter first, then after a warning letter maybe a small penalty, and then a bigger penalty. Then someone else suggested there should be one penalty for accidentally sending an email out to 100,000 people as opposed to maliciously sending an email out to phish for addresses. There's a difference between inadvertent errors and malicious activity.

Should there be a gradient for first, second, and third infraction? Should there be something more severe for malicious versus non-malicious intent emails?

Mr. Neil Barratt: I would suggest that there is, in the enforcement options we have at our—

● (1115)

Mr. Frank Baylis: You have the option to do that, but it's not written. It's not clear to anybody. Should that be written in there?

Mr. Neil Barratt: I would say that having that mandatorily or written into the law would greatly limit our discretion and our ability to adjust to the facts of a given case. As you said, every case is going to be different. If we have to start with a warning letter, then that would limit our ability to ensure that we're reaching an appropriate outcome with the company in question.

Mr. Frank Baylis: We had one testimony from a gentleman who's actually pro-CASL, trying to get small companies to get on board, and he sells a solution starting at $695. He said a huge problem is that CASL says the penalties are $10 million, so all the small companies say that it has nothing to do with them. He cannot get buy-in because they see this huge penalty, and they say that it's to deal with the Rogers and the Bells of the world. So they're not complying based on the way the penalties are written.

Mr. Neil Barratt: I don't think our enforcement actions bear that out. We've taken actions against individuals operating businesses out of their homes, against very small businesses, and of course against very large businesses like Rogers or Porter Airlines. I think we have to be able to respond to the complaints we receive, and as well as—

Mr. Frank Baylis: But CASL has been in place three years. You've done 27 activities, with 22 warning letters and penalties for five companies. At 27 divided by three, that's nine. That's nine per year.

We heard a tremendous amount of testimony that there's a lack of knowledge, a lack of awareness; many, many of the small companies are not aware of it. I'm looking to find ways that we could have an escalation and a differentiation.

First of all, did you see in your penalties and your activities dealing with people who are trying to comply and having a hard time and people who are up to malicious activities?

Mr. Neil Barratt: I think mostly what we've seen is companies that haven't paid adequate attention to the rules that are in place currently. They haven't done a good job of reviewing the consent rules and ensuring that their email lists meet that test. Also maybe they haven't always done as great a job as they should in terms of keeping records to demonstrate that they've obtained consent, that they're in compliance, and that the messages they send out are—

Mr. Frank Baylis: But clearly, one of the key aspects of CASL was to go after people who have malicious intent emails, right? We heard from Professor Geist that there used to be seven of these well-known malicious actors, and they're down to two left. We asked him why these two are left, and he said for us to ask you.

Why are they left, and why have you not done anything about it?

Mr. Neil Barratt: With our activities we're trying to tackle several things at once. As you know, CASL includes not only regular commercial emails. It also includes the installation of software programs and the alteration of transmission data. So we're trying to —

Mr. Frank Baylis: Are you aware of these two malicious actors he's referring to?

Mr. Neil Barratt: Yes, and we're looking at how we can tackle those malicious actors, the illegitimate side of the business, but also create a level playing field among legitimate businesses.

Mr. Frank Baylis: To sum up, then, you would not have us change anything in the penalties, not look to differentiate between malicious and non-malicious activity and not look to have a gradient?

Mr. Neil Barratt: I'll give you one example. We completed a case last year, which was a widespread fraudulent activity in the coupons business. These individuals, these companies, were selling coupons to Canadians and Americans. Without actually having had a relationship with the business, they weren't able to follow through on what they were selling.

We conducted this investigation. It took nearly two years. We issued notices of violations and administrative monetary penalties against those companies, but we issued warning letters to the email service providers that were sending out the commercial messages inappropriately without the required identification.

The tools allow us to ensure that the enforcement action that we take responds to the nature and scope of the violation and to that person's role in it. Those emails—

Mr. Frank Baylis: Why can't they be written, though?

The Chair: I'm sorry, but we have to move on.

Thank you very much.

[*Translation*]

Mr. Bernier, you have seven minutes.

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

I want to thank the witnesses for joining us today. Their presence is welcome.

I would like to continue on the issue of penalties. You say that you agree with what is currently in the act.

[*English*]

So what we have in the legislation right now on the penalties is okay for you to do your job. I must agree a bit with Frank about maybe having a stage or some level of penalties. You don't see the necessity to have that in the legislation?

Mr. Neil Barratt: I would suggest that it would be difficult to ensure that you could respond to every situation with mandated enforcement actions.

Ms. Kelly-Anne Smith (Senior Legal Counsel, Canadian Radio-television and Telecommunications Commission): The commission already has direction in the legislation in what the appropriate circumstances are in the factors that the commission and the chief compliance and enforcement officer have to take into consideration when determining whether to issue a notice of violation with an administrative penalty, and, if so, what that quantum should be. When we're looking at those factors—number of complaints, number of violations, nature of the violations—that's when we consider whether we should issue a penalty, and, if so, what that quantum should be.

That particular section of the act, section 20, gives the chief compliance and enforcement officer the discretion to determine the appropriate remedy and what the quantum should be. There are several factors that are enunciated as well as the opportunity for the chief compliance and enforcement officer to consider other factors. It's that particular tool that allows him to determine whether a penalty is appropriate, and if so, what the quantum should be.

As my colleague suggested, in order to properly investigate and enforce the act, the commission needs the discretion to determine on a case-by-case basis the appropriate remedy. If we are placed with issuing a notice of violation to a first-time violator, in which the violation is of such a proportion that they're sending malware or installing botnets, that is not the appropriate tool. What the chief compliance and enforcement officer needs to do is determine the appropriate tool to use in this circumstance to ensure compliance, to bring the company into compliance with the law. Sometimes that's a warning letter, but oftentimes it's not. If the behaviour is egregious, if it's an egregious violation of the act, if, when examining the factors enunciated in section 20, it's a strong violation, then he needs to use a stronger tool to ensure compliance with the act.

● (1120)

Mr. Steven Harroun: I'll just add to that.

One would have to look at the precedent that would set. Let's say in a graduated system the first time you offend, it's a warning letter; the second time, it's a citation; and maybe it's not until the fifth time that we consider an administrative monetary penalty. Well, one of the key components of the legislation is to make sure we don't have recidivism. I don't want people to be in front of me a second time. I don't want to investigate the same company a second and third time.

From the very first time we choose any level of enforcement action, from a warning letter right to an administrative monetary penalty, I want that to solve the problem. The goal is compliance, ultimately.

Hon. Maxime Bernier: What do you think about the private sector knowing a bit better the predictability of their actions? Usually people want to know what the penalty will be if they're doing something. If you have that kind of discretion, it's a bit difficult for people in the private sector to know that if they're doing that, they're going to pay this fine. There's less predictability for the private sector. They have to look at your case law. They have to look at....

Mr. Steven Harroun: Absolutely. It's definitely precedent-based. I understand the concerns that have been raised on the record. It's “up to” $1 million per violation for an individual and “up to” $10 million per violation for a company. Certainly our enforcement actions over the last three years have not realized monetary penalties to that great a degree. But certainly every decision we publish and every action we take provides guidance to the lawyers in this community and also to the companies to understand, okay, if I have five violations against the act, it probably means this, and if I've had 500,000, I probably need to go to the higher level of the scale of enforcement actions that the CRTC has taken.

Each decision that we publish, each enforcement action that we take, I think provides that guidance. I think we've been consistent over the three years when we assess cases: is it like case X or is it like case Y?

Hon. Maxime Bernier: Okay.

You were also saying that you can help business people to be in compliance. The people who are doing that are not the same ones who are doing the enforcement. It's a service that you're giving. But at the same time, you're in charge of enforcing the law, to be sure that people are in compliance. Do you see any conflict of interest in these two functions?

Mr. Steven Harroun: I actually think it's extremely important that the chief compliance and enforcement officer's staff are the ones out giving that guidance. We are seeing in every case.... We talk about, if you will, some 20-odd cases that we've closed. We do lots of investigations that conclude with no action taken—

Hon. Maxime Bernier: Yes.

Mr. Steven Harroun: —but we are able to offer those companies guidance, such as, "You should clean up things over here. You should make sure you're doing this properly." My outreach team, which does not do actual investigations, collaborates a lot with our enforcement team to understand what problems we are seeing and what areas we need to focus on when we do that outreach. I think it's important that those two groups talk together and that we go out there and say, "This is what we're seeing. This is what you've seen in our decisions, but this is also what we're seeing in our complaints. This is what we're seeing in our investigative actions." They may not be public, if you will, because they've closed without any actual official enforcement action.

● (1125)

Hon. Maxime Bernier: Thank you.

The last question is on the cost for small businesses of being in compliance. A lot of businesses were telling us a couple of sessions ago that the cost is huge and that they need to have more guidelines.

What do you think about this? Do you have any idea about the compliance costs for a small business owner?

Mr. Steven Harroun: Certainly there are costs to complying with any piece of legislation and regulation.

I can let my colleagues add to this, but one has to look at the fact that you've heard about some creative technology solutions over the period of your testimony where there are options for people just to purchase. Large companies probably have the wherewithal to comply, but for small companies—we expend much of our outreach effort and our guidance on the small and medium-sized enterprises—compliance can be at the end of the day an Excel spreadsheet that says, "Yes, Mary across the road said I can email her." It does not have to be a grand compliance program.

The Chair: Thank you very much.

We'll move on to Mr. Masse for seven minutes.

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

Well, you certainly don't look like the storm troopers described by some of the testimony we received.

Voices: Oh, oh!

Mr. Brian Masse: I don't know if you left your masks behind, or if your Death Star is in shambles. It depends upon what version, I think, of—

Mr. Steven Harroun: I'll take that as a compliment.

Voices: Oh, oh!

Mr. Brian Masse: Yes.

I apologize for being a little bit late, but I caught the end of it, and that's where I want to go. How much has it cost to monitor and do your enforcement operations under this legislation since passed? Do you have any idea what your annual budget might be for this? If you don't have it, maybe you can get back to us, but can you give us any idea of the operational cost necessary to ensure compliance with the legislation?

Mr. Steven Harroun: Do you mean for the entire compliance and enforcement sector at the CRTC?

Mr. Brian Masse: No, I mean just for CASL and that area. I think there was an original extra budget provided, and I don't know whether there's a continual amount.

If you don't have that now—

Mr. Steven Harroun: It's an ongoing amount, for sure. I'd have to look exactly at my CASL funds. The challenge is that I'm also responsible for the national "do not call" list and for the voter contact registry. I can give you $4 million off the top of my head, but that's for my entire program rather than for CASL. CASL is probably around $2.2 million, give or take, at the CRTC level. But we can provide that information, absolutely.

Mr. Brian Masse: That would be nice.

Do you think you're on a cost-recovery basis right now, or is it probably more just a compliance and...? You're not really on a cost-recovery basis. Your fines or your penalties are not subscribed based on that.

Ms. Kelly-Anne Smith: No. Any administrative monetary penalty that we issue and collect and any specified quantum that we would collect as part of an undertaking goes to the Receiver General for Canada. It does not come back to the CRTC. We're not on any kind of cost recovery.

Mr. Brian Masse: It's interesting, because when I first got here, I worked on and was successful in getting the elimination of tax deductibility for fines and penalties. I'm redoing some of that work, however, because some loopholes have popped up over the last decade that are actually allowing for tax deductibility of some of the compliance fines. That's another story in itself. The point is that it's costing money to do this.

There was a case that I thought was interesting. One of our telecoms came here—I can't remember which one it was—and said that they had been fined, I think, but had received no warning. I know there is supposed to be a notification process and that usually there are provisions for undertakings in respect of rectification of a situation and so forth. It's not that it just happens.

Do you have any comments on that? Maybe you can you walk us through what happens if I do send spam. Are there several interventions before an actual fine takes place?

I was surprised by one, though, who suggested that there hadn't been much communication.

Mr. Neil Barratt: As we said earlier, we're not always going to send a company a warning letter to tell them that we see complaints about their situation, but in the course of an investigation we're going to be collecting records from any company we're looking at, asking them for compliance details and what their record of consent is; we look at all their record-keeping. For any company, that's an opportunity—it's a bit of a red flag—to come to talk to us, ask what we're looking at, and settle an undertaking with us on a voluntary basis before the investigation goes any further.

● (1130)

Mr. Brian Masse: I guess my expectation as an elected representative would be that if we had continual abuses, the fines and penalties would move, I guess, stronger and faster. Is that the potential out there if that does take place? That's what I expect, at least, and I think that's what my constituents expect when it comes to spamming.

Again, I come from the perspective that this is a privilege: to receive unsolicited information that's designed for the purpose of the engagement of resources, that being your data, your device, and all those different things that can affect you quite seriously, from your privacy to a number of things, I don't view that as a warranted right to dispense that information upon people. I think that's a privilege. That's my perspective, anyway.

I would expect, then, that if there's an escalation or a continual pattern, there would be a reciprocal response from the CRTC on that.

Ms. Kelly-Anne Smith: We have a legal responsibility when looking at the administrative monetary penalty. It's one of the factors that we have to look at. If there is recidivism, if there has been a past violation or a past undertaking, we have to take that into consideration in determining the quantum of the penalty, and we do.

Mr. Brian Masse: But there has been the suggestion—I'll be quite frank, although I'm probably not going to be popular in saying this—that it's the responsibility of a business to know the law. At the end of the day, as a citizen, it's part of my right to know what's legal and not legal for me to do. At the same time, there seems to be a pattern that there could be perhaps some better outreach or responsibility. I joked about it being like "CASL for Dummies" or something like that. I may be wrong on that, but do you think there is some type of bridging or some type of work that can be done on that? Or is that basically something you're not in the business of doing or not supported or funded to do, and that's part of the problem here?

Mr. Steven Harroun: It's definitely one of our objectives. Definitely something we are funded for is CASL outreach. Absolutely, it's within our appropriation for that. We do an extensive amount of outreach, and I know at my last appearance here at this committee.... I mean, we do go from Newfoundland to Vancouver almost every year. We are, if you will, oversubscribed on the number of people who want to talk to us. We try to target as many people as we can through conferences, association events, annual meetings of real estate brokers, bankers, or whoever. That's where we try to target our outreach so that we can tackle as many companies as we possibly can.

I'd be remiss not to talk about our fightspam.gc.ca website, which has a wealth of information, as well as our colleagues at the Office of Consumer Affairs, who also have a mandate under the ISED department to provide information to consumers and small businesses. There is certainly an extensive amount of work being done. There can always be more work done, absolutely.

Mr. Brian Masse: I'm willing to bet—don't take offence to this—that a lot of the people who get an email from the CRTC probably do unsubscribe.

Voices: Oh, oh!

Mr. Brian Masse: Bureaucratic information is probably not the most warranted traffic that is often sought, but it's probably more engaged during times of urgency than it in times of not.

Mr. Steven Harroun: I will try not to be hurt by that comment, honourable member.

Voices: Oh, oh!

Mr. Brian Masse: There you go.

The Chair: I'm feeling the love here.

Voices: Oh, oh!

The Chair: We're going to move on.

Ms. Ng, you have seven minutes.

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

Thank you so much for coming back. As you said, the law has been in place for three years. I think what we heard from the testimony that came in is that people are giving us feedback about how they're working within it.

To the point my colleague made, I think we heard from businesses that they are trying to comply. I think that's certainly the intent, and they're looking to us to understand where there could be some improvements to help with compliance. For sure, applaud and know that the intent here is to try get at anti-spam and at the bad actors that can hurt overall confidence. The intent is to protect consumers. We heard, virtually overwhelmingly and unanimously, that there needs to be some clarification in some of the definitions. Maybe that's what I'll focus on, and you can talk about that.

For commercial electronic messages, we heard from many, almost everyone, asking for some clarity around that, because there's a lack of understanding around a CEM for business-to-business use. We heard examples of someone or an organization not being able to communicate to a customer to give them a notification.

Can you talk to us from your perspective? We heard the testimony. Is it worthwhile to do some further clarification on the definition of CEM to help with compliance?

● (1135)

Mr. Steven Harroun: I'll start, and then my legal counsel will get me out of trouble.

I think that's a really good point. Obviously, for every piece of guidance that we give, we try to provide that clarification on everything from the definition of a commercial electronic message to other issues.

I think it's interesting; I read the blues on the weekend from this committee on the entire study, and you're right that people bring that back. What I found interesting in some of that testimony is, for me, clarity on the fact that people don't understand some of the exemptions. There are exemptions for business to business. There are exemptions for charities. If I am a credit card holder with a certain company, and they want to text me or email me to tell me something about my account because I've given them that information, that is permitted; there is an existing business relationship there.

I was a bit surprised by some of the testimony I was reading in that they felt they couldn't do certain activities or that they were unable to do certain activities.

With respect to certain clarifications with CEM, I'll let Kelly-Anne tell you more, but I think the key thing for me as the chief compliance and enforcement officer is to make sure that we don't get so granular that it becomes even more challenging for people to comply or for me to enforce a particular activity.

Ms. Kelly-Anne Smith: The definition in the act is a broad definition, I think. We have heard as well that there's a lack of clarity with respect to the definition. I think the definition contains other definitions, other terms that you need to refer to other terms, in order to determine what those terms mean.

In the recent Compu.Finder decision, the commission itself has provided some clarification and some guidance as to what in their view constitutes a commercial electronic message. I think the definition is so broad in order to capture circumstances where a party could be soliciting. If you want to make tweaks to the definition, it is your opportunity to do so. I do note that when the witnesses testified, people criticized the definition but didn't offer any suggestions for how we could clarify the definition. I would certainly be open to commenting on how we could clarify the definition, but I would exercise caution there. If you tighten it up too much, you might restrict our enforcement of real spam emails that are sent.

There are so many exemptions, some of which are not even consent-based, that if you have any kind of relationship with a party, you really can send a commercial electronic message.

Ms. Mary Ng: That's helpful. I guess the concern really is that we just heard overwhelmingly—and if you read the blues, it's overwhelming—about the lack of clarity on the definitions, and under what circumstances implied or explicit consent is needed. I think that chilling effect that is being borne is real, because this is what organizations are facing in trying to comply. So the ability for us to be able to give a set of recommendations that genuinely can then help improve the intent of the legislation...but at the same time also give clarity so that there is a practical implementation, just because people have now lived with it for a few years now, right? So that's helpful.

On the exemptions that exist such as business to business, personal to personal, charities and so forth, do you have any ideas about how we could make those modifications, or what action could be taken that would then help with a better understanding? It's a combination of clarifying CEM but also—

Ms. Kelly-Anne Smith: There is a multitude of exemptions, there's no doubt, and I think in some cases there is an overlap.

● (1140)

Ms. Mary Ng: It's perhaps that overlap that is just providing a lack of understanding.

Ms. Kelly-Anne Smith: I think so.

Ms. Mary Ng: In an absence of direction, people and businesses are just saying they can't do it, and because there are penalties that could be quite severe, they really aren't doing it. How do we incent and enable people to get that level of comfort to adopt and then make all of us safer?

Ms. Kelly-Anne Smith: I think maybe you could tighten up the exemptions. There are areas where there's an overlap. In the GIC regulations, there's the exemption where, if you're a business and you have a relationship, you can send to another business. But then there's the existing business relationship exemption. If you're a business, you already likely fall under the existing business relationship exemption, so there's an overlap there.

I'm sure you heard about subsection 6(6).

Ms. Mary Ng: Yes.

Ms. Kelly-Anne Smith: I'm going to be very cautious here, but I think there is likely an opportunity to clarify with respect to subsection 6(6).

Subsection 6(6) is a bit of an oxymoron in that it says that these commercial electronic messages are exempt for consent purposes. But if you look at what those provisions are, a lot of them are not really commercial electronic messages by their very nature. We've heard a lot of confusion from people with respect to subsection 6(6), and we've tried to give them comfort, but we can't change the way the legislation is worded.

Ms. Mary Ng: One point I want to go to really quickly is software. People said that there's an inability, because of the requirements for consent, etc., to get software in that's going to essentially help them be more compliant or be more secure; or in the world of the Internet of things, where things will just update, they don't know that they're able to do it, because in doing so they may violate CASL.

At any rate, there's no time for an answer. Maybe someone else will bring it up.

The Chair: Thank you. We can come back to this.

Mr. Eglinski, you have five minutes.

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

Thank you again for coming back.

Neil, there were some questions being asked earlier by Mr. Baylis about the amount of enforcement you did. I think somebody did the quick math and said you only did nine every year for the last three years. Being a former police officer, though, I've had three or four guys work on a very serious crime case for four of five years with only one charge. You casually let slide that one of your investigations lasted upwards of two years. I know you need to get the evidence, and you need to have the right materials, if you're going to do the fine.

Can you expand on that a little bit? Let's look at maybe Rogers or Porter Airlines, two that came up that all the lawyers want to throw at us and stuff like that. How long would that investigation have taken, and how many people would you have had working on it?

Mr. Neil Barratt: I don't have the details specifically for that one, but you are right that they take a lot of time and can often require several investigators to be involved at the same time.

In general terms, an investigation is going to start with the intelligence we have in the spam reporting centre or elsewhere, but we need to be able to validate all that information. In the case of a legitimate company that's sending out messages, we need to ask them to get their consent records. There can often be millions of records, so we're talking about a spreadsheet with millions of lines for each email: who they're sending emails to, when their business relationship was established, and things of that nature.

Going through all of that information obviously takes time. We need to then also contact any complainants we may have and get witness statements to validate and corroborate the other information we have. It's a long process, and when we get into cases that are multi-party, such as the coupons investigation that I referred to earlier, then you have several legal entities that you're looking into at the same time, and people in different jurisdictions. In that case we had one American and one Canadian. It necessarily takes a little longer when we're dealing with partners in the U.S., for example.

Mr. Jim Eglinski: So we're looking at lengthy investigations.

Mr. Neil Barratt: Yes. As we get closer to cases of malware and things of that nature, that's only going to increase the complexity and the amount of effort and resources going into the investigations.

Mr. Jim Eglinski: How many people do you have working in your department?

Mr. Neil Barratt: I currently have about 12 investigators.

Mr. Jim Eglinski: Now, Steve, you mentioned during your presentation that during the time that evidence has been given—obviously you guys have been listening, so thank you—you are already making some changes. Could you tell us about some of the things you are adapting right now? I think your submission mentions some new “tools” as a result of evidence from the committee.

● (1145)

Mr. Steven Harroun: With every piece of information we get, whether through an investigation or through our outreach activities, and we've certainly taken it upon ourselves also to look at the testimony of this committee, if people see that there's confusion and we have the opportunity—we have guidance we can showcase on our website, or information we can share with others—we've taken it upon ourselves to look at it and say that we may need, perhaps, an infographic on such and such. We have the information, it is public, people can find it in four different places on our website, but perhaps we should look at how we can tighten it up and make our CASL information pages more accessible to people.

We've looked at that, have noted that there still seems to be some confusion, and asked whether we can add some new FAQs to our website, for example. That would probably be the most immediate thing we've done: “Let's make sure people are clear as a registered charity”, and so on. We've tried to make tweaks as we go, because every piece of learning we get is helpful for us. For us it's all about wanting everyone to comply, so the more guidance the better.

Mr. Jim Eglinski: Going back, do you keep a record? You've told us how many major investigations you've had, and you spoke about having many inquiries where you have dealt with companies individually, gone through things, and made recommendations. Do you keep a record on the corporate end of how many people you've dealt with over the last three years?

Mr. Neil Barratt: We track the number of warning letters that we issue, and obviously, the number of undertakings we enter into or notices of violation that we issue. Do we track every time we have a conversation or a back-and-forth with a company about compliance? Maybe we do it a little bit less robustly than we do those other metrics, but every time we get information or questions from people, we use them to develop the next set of presentations we're going to give. We presume that, if someone comes to us with a question, there are probably several other people who have that same area of concern.

Mr. Jim Eglinski: But there's no one there asking you how much you're really doing, or what you're really doing?

Steve doesn't get on your case and ask you to justify your 12 or 13 guys?

Mr. Neil Barratt: Am I allowed to say “no comment” on that?

Voices: Oh, oh!

Mr. Steven Harroun: It would definitely be in the hundreds a year, though, with regard to conversations we have back and forth. We use the intelligence we get from the spam reporting centre, from complaints, and from other sources of information that causes us to do that initial outreach and say, “We're seeing a problem here.” It can be something very simple, such as “Oh no, it's this”, to which we might say, “Okay. Thank you very much.”

It would definitely be in the hundreds per year.

The Chair: Thank you.

We'll move to Mr. Jowhari for five minutes.

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

Welcome back.

What I heard is that the CRTC focuses on education and investigation as well as enforcement. I also heard that you have an outreach group that goes across the country and tries to educate and answer questions.

You also talked about the fact that, because of those sessions, and because of some of the inquiries made to the outreach organization, you've made some improvements in things such as frequently asked questions, graphics, and posting. You also touched on subsection 6 (6) as an example.

Now, if I break it down, there's some legislative clarification that could be done, and there's some better practices clarification that could be done, and I'm getting the sense that you're doing a lot of that clarification through the various means you have.

Through this process, what have you heard that would help us to identify one, two, or three areas on the legislative side, as part of this exercise, so we could say that, if we make this amendment or if we make this change, it would improve the situation through better education and better adoption, leading to higher compliance, and therefore, a reduction in the number of complaints?

Ms. Kelly-Anne Smith: As I mentioned, I think subsection 6(6) is definitely an area that, if you could tweak it, that would improve my life 100%.

Mr. Majid Jowhari: So we've got subsection 6(6).

Ms. Kelly-Anne Smith: Yes.

Mr. Majid Jowhari: I understand you've been three years in there, and I understand better is always possible, so give us another one. Subsection 6(6) is one. What would be another one?

Ms. Kelly-Anne Smith: Another one would be some of the overlaps in the exemptions. I did give the example of an existing business relationship and a business-to-business relationship in the GIC regulations.

I would have to refresh my memory as to which sections, but there is also, in the GIC regulations and in the act, an exemption for inquiry request complaint, and there's another one in the regulations. They're almost identical, but the time periods and the provisions for the exemption on consent are different. They're very similar, and consumers and the industry cannot distinguish between them.

● (1150)

Mr. Majid Jowhari: That's fine. I will ask for a submission by your department around the two or three areas on the legislative side that we could specifically look into. You don't even have to suggest that we amend them, just say we specifically look into them and focus our comments on them.

If you made that submission, that would be good.

Ms. Kelly-Anne Smith: Absolutely.

Mr. Steven Harroun: I will put one more on the record. The first time we were here, I focused on domestic sharing, right? It's easier for me to share with my international partners than it is my partners across town. That would definitely be one on our list.

Mr. Majid Jowhari: That's a great lead-in for my next question.

About information-sharing, I see that the CRTC does two types of information-sharing. There's sharing with partners outside of Canada but also with the other two groups that you work with. Can you comment on the effectiveness of the internal information-sharing with the other two organizations, the commission as well as the bureau, as well as internationally?

Mr. Steven Harroun: Absolutely. I'll also let my colleague Mr. Barratt add to my remarks.

Mr. Majid Jowhari: Where can it be improved? That's my focus. Tell me where we should improve it or make some recommendations.

Mr. Steven Harroun: One of the major things I mentioned last time, if not this time, was that our partnership with the Competition Bureau and the Office of the Privacy Commissioner is written in the legislation, which is fantastic. It's not “you should” or “you can”; it's “you must”, so we share on cases there.

Personally, I think that between those two organizations, we're fine. We've learned how to—

Mr. Majid Jowhari: This is not what we heard in the testimony, but from your point of view, you're saying it's fine.

Mr. Steven Harroun: We're working well as far as collaborating on cases is concerned. We're working well on deconflicting, for example, if it's a criminal case versus a civil case with our partners, or if it's a privacy case. Sometimes we take them from all angles, but otherwise it's “Over to you. This is now your job.”

Mr. Majid Jowhari: How about internationally?

Mr. Steven Harroun: We effectively use memorandums of understanding with agencies around the world.

Mr. Majid Jowhari: How effective has that been?

Mr. Steven Harroun: They have been very effective. Certainly, our international partners execute warrants, gather information for us, and knock on doors. We do the same for them. CASL legislation permits that. We have two streams there, which I've talked about. We have bilateral agreements with various international organizations, and we're also a member of—

Mr. Majid Jowhari: Can you also, as part of your submission, make a recommendation on where we can improve?

Mr. Steven Harroun: Absolutely.

The Chair: Thank you very much.

I'll add, however, that if you are going to do a submission, preferably it's no later than next week.

Mr. Steven Harroun: I was just going to ask you about that. All I wrote down was “Date?”

The Chair: Do we have a date?

Mr. Francis Lord (Committee Researcher): Next Thursday.

Mr. Steven Harroun: One week should be fine.

The Chair: Okay. Excellent.

[*Translation*]

Mr. Bernier, go ahead for five minutes.

[*English*]

Hon. Maxime Bernier: I will share my time with my colleague.

I really appreciate your answer about the compliance and all the penalties. I thought in the beginning that we would have to change the legislation, but I think the discretion we have right now is helping both you and the small business owner.

Speaking about complaints, can you help me to understand how it works in your organization? You receive a complaint. You have compliance people who are going to look at it. After that, you have the enforcement. In terms of the process, from a complaint to an action from the enforcement team, what would be the delay, and what would be the timing? Please just give me some details about that in order to help me understand your organization a little better.

Mr. Steven Harroun: I'll start.

It's a really good point. I've raised it before. We get approximately 4,000 complaints from Canadians into our spam reporting centre every week, so you can extrapolate that to 15,000 to 20,000 a month.

As a general practice, it's our intelligence folks, if you will, who look at those complaints. They identify trends. Are there patterns, are there particular organizations, or are there particular types of activities going on? We do regular case selection meetings, where we have our intelligence folks, if you will, talk to our enforcement folks and say that they have seen these areas as an issue in the past few weeks, months, or whatever. That helps to inform our investigations, going forward. That's how we pick cases to move on.

As I said, with 4,000 complaints a week, obviously with a small team we're not investigating every complaint. What we are doing is looking at the various pieces of the puzzle in our spam reporting centre, and we also use other sources of information provided by our friends at Public Safety, the RCMP, and others. I believe you had representatives from Spamhaus here earlier this week. We look at all these pieces of data. It's not just the complaint from Joe or Jane Canadian; it's also the other pieces that help inform the decision-making when we move on to an enforcement activity.

● (1155)

Mr. Neil Barratt: The only thing I'd add is that we have over a million complaints that have been submitted by email. They are not validated. We don't know that every one of those is an actual CASL violation. We look at trends; we look at the scope. Obviously, if we're getting a thousand complaints about a particular organization, that's going to pop up faster than one or two emails.

Hon. Maxime Bernier: Thank you very much.

Jim, do you want to...?

Mr. Jim Eglinski: Yes, really quickly, for two minutes.

We heard evidence.... I believe one of the presenters, Certimail, said that only 5% to 15% of companies are compliant. Have you done research to look at the overall picture of compliance in Canada? Do these figures match your thoughts, or was it just a scare tactic?

Mr. Steven Harroun: I would have to defer to the department on that. I know that the last time we appeared, certainly Mr. Schaan and his folks provided some details.

I would suggest that it's a very low number. I would not agree with that.

But have we conducted research at the CRTC? No, we have not.

Mr. Jim Eglinski: If you do have that data, I'd like it if you would send it. I think it would be very worthwhile for us to see whether the evidence given was right or not.

Mr. Steven Harroun: I don't think I have anything. The department might.

Mr. Jim Eglinski: Okay.

I think I'm done, Chair. I'll pass my time over.

The Chair: Excellent. Thank you very much. That's very collegial of you.

Mr. Jim Eglinski: It's my tie.

The Chair: It is. We're members of the bow tie club.

Mr. Sheehan....

Oh, wait: you don't have a bow tie on. You can't talk.

Voices: Oh, oh!

Mr. Terry Sheehan (Sault Ste. Marie, Lib.): I'll try to keep it bow-tie-related.

My line of questions recently has been about social media, because we've heard conflicting testimony. Does it apply? Does it not? We certainly did hear from the bureau that it does. In terms of the CRTC, just as an example, Facebook reached two billion users per month this past summer, but within their platforms they also have other things. Facebook messenger is reaching well over a billion users now. These platforms are moving exceedingly quickly. You know all the other ones, such as Snapchat and Instagram; I won't mention them all.

How does this CASL legislation apply, and the potential penalties or infractions, to social media?

Ms. Kelly-Anne Smith: With the way in which the definitions in the act are worded—i.e., for “commercial electronic message” and “electronic address”—there are features of social media where CASL does capture them. Using Facebook as an example, there's a feature where you can send a direct message to somebody. That would certainly, as an example, be captured by CASL. You cannot send a commercial electronic message to another person unless you have consent or you fall under one of the exemptions, such as family or personal relationships.

Mr. Terry Sheehan: So it does.

Ms. Kelly-Anne Smith: It does, yes.

Mr. Terry Sheehan: Then I have a quick follow-up question for clarification. Have you received any complaints and have you actioned any kind of disciplinary follow-up?

Ms. Kelly-Anne Smith: With respect to social media, yes, we have received complaints about social media.

With respect to actioning those complaints, I will defer to my colleague Neil to answer that.

Mr. Neil Barratt: We haven't completed a case in that area. We are looking at other platforms. We receive complaints via SMS, as one example, and other messaging services in the SRC. It's something we look at. It goes into the same case-selection approach as—

● (1200)

Mr. Terry Sheehan: So it's a new thing. Okay.

I'll let Lloyd pick it up from here.

Mr. Lloyd Longfield (Guelph, Lib.): Thank you.

This study was triggered by the suspension of the private right of action, to look at the legislation and to comment on the suspension. We've had a lot of testimony about subsection 6(6) around clarifying what is a "commercial electronic message". We've had a very wide range of opinions. We aren't at the point of recommendations yet, but to me it doesn't seem as though we're ready for private right of action in terms of having this legislation sunk in deep enough to be able to have a strong enforcement of it through private right of action.

Could you comment on my opinion on that?

Mr. Steven Harroun: In my role as the enforcement officer of CASL, the private right of action actually doesn't affect me. It provides another opportunity for Canadians to pursue complaints or activities that they disagree with. As chief compliance and enforcement officer, the PRA really doesn't affect the way I do my job or how I will enforce CASL, per se. It provides, if you will, another way for someone to pursue a complaint against a company or whatever.

Where it does affect, obviously, is that if there's a private right of action case, I am unable to investigate that case, and vice versa; if a company is in an undertaking or with—

Mr. Lloyd Longfield: In my opinion, we're still learning on CASL.

Mr. Steven Harroun: I would agree with that.

Mr. Lloyd Longfield: Okay.

The Chair: Thank you.

Over to Mr. Masse.

Mr. Brian Masse: Thank you.

It is interesting, though, about the private right of action. It is one of the tools, that now will be put in abeyance, for responding to activity that is illegal, or potentially even with settlements. Is there anything else you can do that would actually help with the enforcement right now in terms of the CRTC? The private right of action was one of the tools. We looked at all the different methods of how to rein in some of these things. The private right of action was seen as one of those elements to combat spam, especially in the more egregious situations where there were habitual and ongoing problems.

With that now in abeyance for the moment, are there any alternatives that we can do, or that we should be looking at, to shore up this situation, or is it just wait and see, nothing changes, with your department?

Ms. Kelly-Anne Smith: For us, investigation and enforcement will continue. There will be no change to that.

I will add, though, that with respect to the delay of the private right of action, there will be no remedy for consumers and Canadian citizens to obtain damages. When we issue an administrative monetary penalty, those funds go to the Receiver General for Canada. If individual consumers and Canadians are affected—if there are damages by spam or malware, if it affects their system, if costs are incurred to them—there is nothing we can do to help individual consumers and individual Canadians. That's what the private right of action does. It's a tool to award money to Canadians who have been personally impacted by spam. And that's one thing we can't do.

Mr. Brian Masse: Yes, and that's my point, that this is a gap. It's missing now. It is also a cost of business, and it's a cost and expense being exposed by this.

In terms of funding for the continuation of the legislation, though, is that ongoing right now? I could be wrong, but if my memory serves, there were additional funds allocated for the implementation of CASL. Is that ongoing? Is it indexed to the cost, or was it one-time funding and it sits right where it is right now?

Mr. Steven Harroun: The indexing is a good question. I'll have to look at that.

We receive a particular amount of money to enforce CASL on an annual basis. The one-time cost that you referred is from when we operationalized the spam reporting centre. It cost us a few hundred thousand dollars to get that up and running. That was more of a one-time cost. We have operational costs for the spam reporting centre. I think perhaps you were referring to that one-time cost to establish that spam reporting centre that all of our partners use. We have operational costs there now.

Our funding is reasonably constant, and has been for the past three years, as far as enforcing CASL legislation is concerned.

● (1205)

The Chair: Thank you. Excellent.

I want to thank our guests for coming in today and for sharing some really good information. I think we have some work ahead of us. Again, thank you for your time.

We'll suspend for a few minutes before we go in camera to start our draft report of IP.

[*Proceedings continue in camera*]