Speech

Archived - Manon Bombardier to the 5th Canadian Internet Forum

Archived Content

Information identified as archived is provided for reference, research or recordkeeping purposes. It is not subject to the Government of Canada Web Standards and has not been altered or updated since it was archived. Please contact us to request a format other than those available.

Ottawa, Ontario
October 9, 2014

Manon Bombardier, Chief Compliance & Enforcement Officer
Canadian Radio-television and Telecommunications Commission

Check against delivery

Thank you very much.

Canada's anti-spam legislation came into effect this summer. For us at the CRTC, this was a significant event. That's because it's good news for all Canadians who use electronic communications. And that means nearly all Canadians. The response was immediate. Within the first week, we received over 8,000 submissions on possible spamming activity.

Everyone knows what it's like to have your inbox flooded with commercial messages that you don't want and didn't ask for. It's annoying, intrusive and inconvenient.

It opens the door for deceptive marketing practices. Messages may be carrying malicious software in attempt to steal your identity or intellectual property. And it creates a bad environment for businesses that want to use the Internet responsibly to make contact with consumers.

The CRTC aims to ensure that Canadians have access to a world-class communications system. We organize this mission around three pillars: create, connect and protect. The protect pillar defines the work we do to enhance the safety and the interests of Canadians, including their right to privacy.

It's this protection work that is our main focus in C&E—the Compliance & Enforcement sector. I'm

first going to give you an overview of the new legislation and how we are carrying out our new responsibilities. Then I'll turn to some of the other aspects of what we do.

CASL

The actual title of the *Act* contains 53 words in English, so it's generally known as Canada's anti-spam legislation. Around the CRTC we just call it CASL.

Under Section 6 of CASL, it is now prohibited to send commercial electronic messages without the prior consent of the people you're sending them to. Even with that consent, the senders must now identify themselves and provide contact information. They must also provide an unsubscribe mechanism, so that Canadians can opt out of receiving further messages.

Under Section 7, transmission data may not be altered without consent so as to redirect the transmission to another destination. For example, when you click on a link to a website, it will be a violation of the law for someone to substitute another link so that you wind up at some other website.

Section 8 prohibits downloading of computer programs without consent in commercial activity, or causing such programs to send messages. It will come into effect on January 15 of next year, and it's intended to capture the use of malware and botnets.

These are serious threats. A 2013 global threat report by Websense Security Labs ranked Canada as the 10th most popular location to host malware and the 8th most commonly targeted country by cyber criminals. Earlier this year, the Washington-based Center for Strategic & International Studies estimated that cybercrime costs the Canadian economy about US$3.2 billion annually.

The new requirements set out in CASL provide strong protection for Canadian consumers.

Protecting business

They also protect the interests of businesses. The law was developed through extensive consultations with both consumers and business.

There are exemptions in place to safeguard the free flow of information between buyers and sellers, once some kind of relationship has been established; for example, through inquiries, subscriptions, previous purchases, requests for quotes, and so on. Exemptions are provided for business-to-business relationships. There are also transitional provisions that allow implied consent to carry over from the time before the applicable parts of CASL came into effect.

It is one of the aims of the law to ensure that businesses can continue to compete in the global marketplace within a secure online environment.

Electronic communications are woven into many aspects of Canadian life and commerce. So it's not surprising that the fight against spam required not only a new Act of Parliament but also amendments to existing Acts.

The *Competition Act* was amended to prohibit misleading and deceptive practices online. The

Personal Information Protection and Electronic Documents Act, or PIPEDA, was amended to cover activities such as unauthorized address harvesting, which is what happens when somebody steals your entire email contact list.

Enforcement process

Canadians can now report spam and related violations to the Spam Reporting Centre, which we are hosting. There are two ways you can report a suspicious message. You can fill out an online form at **fightspam.gc.ca** to let us know about the incident. Or you can forward the message to us at this address: **spam@fightspam.gc.ca**

The fightspam website also offers a wide range of information on CASL—both for consumers who may be receiving spam and for the businesses and organizations that want to get their messages out in compliance with the law.

Now, how will the terms of the legislation be enforced?

The CRTC has the primary enforcement responsibility, but two other enforcement agencies are also ready to act: The Competition Bureau and the Office of the Privacy Commissioner. The nature of the complaint will determine who handles it.

The three agencies have signed a Memorandum of Understanding which outlines our respective enforcement roles and how we will cooperate and coordinate. We've agreed to share information to support each other's investigations.

The CRTC has assembled a top-notch team to conduct our own enforcement activities. It includes former RCMP officers, experienced criminal investigators and sophisticated experts in computer forensics.

Our team uses state-of-the-art tools to carry out their work. We have a new cyber-forensics lab. It's an in-house centre designed and built by some of Canada's foremost technology leaders. We are able to search, seize and copy digital evidence to prove violations. We can index tens of millions of messages. We have the capacity to reverse-engineer malware. And we can track malware and spam to their source.

We also have a wide range of investigative and enforcement powers available to us under the terms of CASL:

- A Preservation Demand requires an organization to preserve transmission data that would otherwise be lost.
- A Notice to Produce then requires a person to produce that information or any other information that's required for the investigation.
- Warrants may authorize an investigator to enter a place, use its communications or computer systems, examine data, remove anything for examination, or control access to the place.
- An Undertaking is an agreement to come into compliance, which may be accompanied by an administrative monetary penalty.
- A Notice of Violation is issued for serious or repeated violations. These may also carry

administrative monetary penalties. The maximum is $1 million for an individual and $10 million for a business, per violation.

These are powerful tools. However, there is no way that we can eliminate all spam or all misuse of the Internet. Some will get through. But we will be doing our best to capture a wide range of violations. We will pay special attention to the most severe types of violations, the most egregious violators sending the highest volume. Our main targets right now are abusive spammers and interlopers running botnets located in Canada.

Beginning on January 15, we will also be targeting malware and malicious URLs.

International cooperation

The CRTC has the expertise and the technological resources that it needs to provide effective enforcement. But spam and other forms of online threats are not just a Canadian problem. It is worldwide. Much of the spam that targets Canadians originates outside our borders. International problems demand international solutions.

So we collaborate actively with our international counterparts, such as the Federal Trade Commission in the U.S., the Office of Communications, or OFCOM, in the U.K., the Australian Communications and Media Authority, and others.

We're an active member of the London Action Plan, which is an international cybersecurity and telecommunications enforcement network.

The CRTC will be partnering with the new Interpol Global Complex for Innovation in Singapore, which is due to become operational next year. It's a cutting-edge R&D facility to identify cybercrime and cybercriminals, and combat them through innovative training, operational support and partnerships.

We are also receiving tens of thousands of messages each day that have been sent to international spam “honeypots. ” Honeypots are fake email addresses and domains that have been set up by enforcement agencies to monitor spam activity. Spam messages that pass through Canadian networks for delivery to those addresses are then forwarded to the CRTC for analysis and possible investigation. The information collected through the honeypots can help track down the senders.

So we are reaching out internationally. We are also reaching out here at home.

Outreach in Canada

The CRTC has been working with Industry Canada to conduct webinars and information sessions across the country. These sessions are designed to prepare businesses and consumers for CASL's coming into force. We've spread the word about the requirements of Section 6 on consent, sender identification and unsubscribing. We've had a chance to hear about people's concerns face-to-face. This has helped us to prepare guidance materials on how businesses can comply with the law.

We’re also preparing guidance for software developers, based on feedback we’ve received from the

industry. These materials will be posted on **fightspam.gc.ca**, as well as the CRTC's own website.

In November and December, again with Industry Canada, we will be conducting sessions for software developers in the major cities to help them comply with the new requirements.

Working with businesses

I said earlier that the CRTC has a range of tools to enforce the new law. Many people are worried we will take advantage of those tools and impose stiff penalties for even the slightest violation.

Our goal is to work with Canadian businesses to ensure compliance. We recognize that most businesses will want to comply with the law. Therefore, in those cases, a positive result will be achieved without having to resort to stiff measures. In other cases, penalties will need to be applied.

Our announcement a few days ago is a perfect illustration of what I mean.

Over the summer, reports came pouring into the Spam Reporting Centre of spam messages being routed through a Canadian Internet service provider (ISP). When we began investigating these reports, we realized that the messages were actually coming from one of the ISP's clients, a small Saskatchewan-based computer reseller. Its server had become infected with malware, which had caused it to join the botnet "Ebury." The company and the ISP were completely unaware that the server was sending out millions of spam messages.

The CRTC quickly alerted the unsuspecting company and its ISP. They both offered their full cooperation and removed all traces of the malware. As a result, we were able to stop the server from sending millions of additional spam messages to Canadians, with all their potential to do harm.

Here's another example of cooperation: Over the course of a separate investigation, we found that a medium-sized organization was unknowingly sending out spam emails promoting a new work-at-home opportunity in German. We worked with the organization to resolve the problem and it is taking steps to prevent this from happening again.

We will continue to cooperate with businesses and organizations to stop unwanted or malicious spam messages from being sent to Canadians.

National Do Not Call List

I'm now going to turn to some recent work we've been doing on the telephony side.

Just as the flood of spam led to Canada's anti-spam legislation, the flood of unwanted and intrusive telemarketing calls led to the CRTC's Unsolicited Telecommunications Rules—the UTRs.

These include several types of protection.

First, the National Do Not Call List (DNCL), which has just passed its sixth anniversary, allows Canadians to opt out of receiving telemarketing calls. So far more than 12 million numbers have been registered. This represents about 29% of Canadian households. These registrations are now

permanent unless they are specifically revoked by the owner of the registered number.

Telemarketers are required to register and subscribe to the List.

There are a number of exemptions to ensure freedom of communication in several important areas. These are calls made for political campaigns, charities, surveys, solicitations for newspaper subscriptions, and calls made to people with whom the caller has an existing business relationship.

Even though such calls are exempt from the National DNCL Rules, they are still subject to the Telemarketing Rules, which require telemarketers to maintain their own internal do-not-call lists.

Finally there are the ADAD Rules, governing the use of Automatic Dialing-Announcing Devices. These devices generate robocalls, and the ADAD Rules set out conditions for their use.

The UTRs are similar in many ways to the provisions of CASL. For example, they also require identification of the caller along with contact information.

There is, however, one important difference. CASL operates under an “opt-in” regime: Canadians can decide which messages they want to receive. The National DNCL, on the other hand, operates under an “opt-out” regime.

Enforcement tools are also similar, though not identical, and they include Notices of Violation, with potentially severe administrative monetary penalties.

Since the launch of the National DNCL, we have conducted over 1,500 investigations. We have issued close to 150 citations, 180 warning letters and about 100 notices of violation to individuals and organizations. Investigations have yielded over $5 million in penalties.

Last year alone, the CRTC took enforcement action against telemarketers that had been responsible for making over 11 million non-compliant calls to Canadians.

Spoofing

Our ability to protect the privacy of Canadians depends on our ability to enforce the rules effectively. One of the major challenges—not only in Canada but also worldwide—is the spread of Caller ID spoofing—the falsification of the phone number that appears on your Caller ID phone display. This makes it difficult to trace the caller, especially since many of these callers are located outside this country.

VoIP—Voice over Internet Protocol—adds another layer of difficulty. Instead of traditional telephone circuits, it uses the Internet, which allows the point of origin to be masked.

To find solutions, we are working constantly with Canadian ISPs and TSPs (telecommunications service providers), and also with our international partners from the U.S., the U.K. and other countries.

New developments

There are several important developments on the way that will help in our enforcement work.

The CRTC is a member of the international Messaging, Malware and Mobile Anti-Abuse Working Group. We co-chair its Special Interest Group on Voice and Telephony Abuse, whose next meeting takes place next week in Boston.

Some of your organizations will be sending representatives to Boston, and I'd like to express our gratitude for that. We're very happy that you're working with us to deal with these very important issues.

With the Special Interest Group, we're exploring the use of "honeypot" numbers to trace the origin of fraudulent, abusive or spoofed calls. The idea is the same as with the honeypot addresses that are used to trace the origin of spamming emails.

A honeypot number appears to the unscrupulous telemarketer as a normal phone number which can be a target for their schemes. The operator of the honeypot can arrange for the call to be answered by a computer or a human, and it may be recorded. Unknown to the sender, information is being logged automatically. That can be put together with data from many other calls and with what's been learned from consumer complaints. The patterns that emerge can then help identify the actual source of the spoofed calls.

We're working with our national and international partners to see how honeypots might be used to help protect Canadians against telephony abuse.

We're looking at other anti-spoofing measures too. These include trace-back methods and could involve call-blocking.

We've also been working with the private sector to develop a system to help Canadians report unwanted telemarketing calls. After an unwanted call, you would press a number on your phone to automatically send information about it to your telecommunications carrier and to law enforcement, including the CRTC. It's similar to a button you can click in your email app to report spam to your service provider.

We love this idea: it's a great use of crowd-sourcing! It would engage consumers in a new way to help us all bring a stop to this kind of abuse. We welcome the participation of the public.

We have new legal obligations to put an end to harmful activities that threaten the well-being and livelihoods of Canadians. We need all the collaboration we can get on both the telephone side and the Internet side.

Role of industry

So here today I would like to appeal to you, as members of the industry. We need your help to make this work. You are on the front lines. Whether you are an Internet or a telephone service provider, you are dealing with these problems day to day. Misuse of your networks hurts your customers and your businesses.

I'm confident that we can count on your continued support. It will pay off for all of us—and for all

Canadians.

Thank you very much.

- 30 -

Contacts

Follow us on Twitter: @CRTCeng

Media Relations:
Media Relations, Tel: 819-997-9403, Fax: 819-997-4245

General Inquiries:
Tel: 819-997-0313, TDD: 819-994-0423, Fax: 819-994-0218
Toll-free # 1-877-249-CRTC (2782)
TDD - Toll-free # 1-877-909-CRTC (2782)
Ask a question or make a complaint

This document is available in alternative format upon request.

Search for related information by keyword

Canadian Radio-television and Telecommunications Commission | Government and Politics

Date modified:
2014-10-10

Government of Canada activities and initiatives

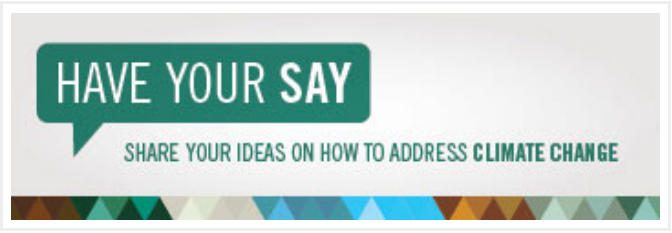
Alberta Wildfires – Get the latest

Learn what you can do to help those in need, and keep up-to-date about the Government of Canada's response to wildfires in Alberta.

Canadian Content in Digital World

Participate and learn about the ongoing consultations on Canadian content in a digital world.

Have your say on climate change today!



Share your ideas on how to address climate change