Canada's Law on Spam and Other Electronic Threats

Office of the Privacy Commissioner of Canada

Discussing the OPC's responsibilities under CASL

On July 1, 2014, key provisions of Canada's anti-spam legislation (CASL) come into force. CASL includes updates to the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Under these changes, the Office of the Privacy Commissioner of Canada (OPC) will share responsibilities for enforcing the CASL with the Canadian Radio-television and Telecommunications Commission (CRTC) and the federal Competition Bureau.

The CRTC will be responsible for investigating the sending of unsolicited commercial electronic messages, the alteration of transmission data and the installation of software without consent.

The Competition Bureau will address false or misleading representations and deceptive marketing practices in the electronic marketplace.

The OPC meanwhile will focus on two types of violations:

- the harvesting of electronic addresses, in which bulk lists of email addresses are compiled through mechanisms that include the use of computer programs to automatically mine the Internet for addresses; and,

- the collection of personal information through illicit access to other people's computer systems, primarily through means such as spyware.

The following FAQs provide information specifically about the OPC's mandated responsibilities tied to CASL. For general information about CASL or issues under the responsibilities of the CRTC or Competition Bureau, go to http://www.fightspam.gc.ca

Frequently Asked Questions

For the sake of simplicity these FAQs refer generically to computers but the same advice largely applies to mobile devices, such as smart phones, netbooks and tablets.

Electronic address harvesting

What is electronic address harvesting?

Address harvesting refers to various techniques used to automatically compile lists of electronic addresses (e.g. email addresses) for bulk electronic mail-outs. This can be done by the spammers themselves or other entities (some known as electronic address harvesters) who then sell address lists.

How can I know that my address has been harvested?

While it's very difficult and often impossible to know for sure, you can suspect you've been a target of address harvesting if you experience a significant increase in spam, either actually delivered to your electronic account or blocked by your spam filter.

If I can't tell whether or not my address has been harvested, how can I alert your Office and trigger an investigation?

If you have reason to believe that your electronic address may have been harvested, you are encouraged to submit your concerns to the Spam Reporting Centre via fightspam.gc.ca. The OPC's investigations may be triggered based on analysis of accumulated submissions from many users and/or information received from domestic and international partners.

Under Canada's anti-spam law (CASL), what should I do if I suspect my address was harvested?

Once CASL is in force, make a submission and send details of the incident to the Spam Reporting Centre. Submissions received by the Centre will help the Office of the Privacy Commissioner determine whether there are reasonable grounds for launching formal investigations.

Personal information collection through illicit access to computer systems

What is the collection of personal information through illicit access to other people's computer systems?

This refers to computer programs known as malware or spyware that collect personal information and are downloaded and remotely installed on a computer without the user's knowledge.

Some kinds of spyware gather information about web-browsing.

Others can collect information about user computer activities and send that data to someone else via the Internet. This can include "keylogging", the recording of individual keystrokes to capture things like passwords and credit card numbers.

Certain types of malware meanwhile can take the form of a virus specifically designed to harvest addresses from a user's e-mail address book or instant messaging programs.

How can I know that my computer or device is infected with spyware?

Here are some warning signs of a spyware infection:

- a barrage of pop-up ads, even if your computer isn't connected to the Internet;
- a hijacked browser that goes to sites different from those typed into the address box;
- sluggish performance when opening programs or saving files;
- a sudden or repeated change in your Internet home page;
- your web browser suddenly closes and stops responding;
- random error messages;
- new and unexpected toolbars; and
- new and unexpected icons in the system tray at the bottom of your computer screen.

How do I know if spyware on my computer or device has been collecting personal information?

Again, as with address harvesting, you may not know for sure. However if someone has taken the trouble to install spyware on your computer, it's highly probable that personal information has been collected and relayed elsewhere.

To delve deeper, once CASL comes into force, send details of your concerns to the Spam Reporting Centre via fightspam.gc.ca. Submissions received by the Centre will help the Office of the Privacy Commissioner determine whether there are reasonable grounds for launching formal investigations of parties who are likely using spyware to collect personal information.

Reports, investigation and enforcement

What should I submit to the SRC to help investigations into electronic address harvesting and the collection of personal information through illicit access to other people's computer systems?

Following July 1, to make a submission, go to fightspam.gc.ca, click on the link to the Spam Reporting Centre's consumer interface and fill out the form.

Will I be contacted following the submission of my report?

You will be asked to provide contact information, however you will not be contacted in order to acknowledge receipt. Instead, one of the enforcement agencies mandated with enforcing CASL may contact you to support an investigation that may follow.

Why shouldn't I just file a complaint dealing with electronic harvesting or spyware directly with the OPC?

It is important that you submit your concerns about email address harvesting, spyware and other similar electronic threats to the Spam Reporting Centre.

The Spam Reporting Centre is the central repository for information about spam-related activity and threats. While a submission from a single individual about a possible contravention may not provide sufficient evidence to enable the OPC to open an investigation, the collective submissions of many Canadians will help identify possible organizations contravening the legislation which may warrant action.

Your submission may also be a matter of interest under the CASL mandates of either the CRTC or the Competition Bureau.

How will the OPC investigate incidents of electronic address harvesting and the collection of personal information through illicit access to other people's computer systems?

Analysis of the accumulated reports along with information received from domestic and international partners will greatly assist the OPC identifying email harvesters and spyware that collects personal information. Based on this information, the OPC will determine whether there are reasonable grounds to launch an investigation.

What penalties can the OPC use to enforce its responsibilities under CASL?

The OPC can investigate alleged contraventions of PIPEDA and issue reports setting out its findings and recommendations. Where possible, the OPC seeks to obtain voluntary compliance with its recommendations. The OPC does not have the power to issue orders or to impose penalties for contraventions of PIPEDA. However, if an organization fails to comply with the OPC's recommendation, the OPC may apply to the Federal Court to obtain an order compelling an organization to correct its practices.

For businesses

What if I hired a supplier to do something like email marketing? Is my business accountable for work done by a third party on my behalf?

Yes. Your business must make sure any third party whom you employ complies with the provisions of CASLand PIPEDA.

What questions should I ask of e-mail marketers who may be carrying out work for me to help ensure that I don't run afoul of the electronic address harvesting provision?

Ask them to explain – in detail – where they get the e-mail addresses they will use to promote your business. If the list was purchased from elsewhere, then ask the marketers to explain how the e-mail addresses were originally gathered and how consent was obtained as required under CASL. For more information on this, please consult the CRTC's resource page at http://www.crtc.gc.ca/antispam.

Email and other electronic messaging is an important way for me to reach and stay in touch with my customers. How can I ensure that I do this without breaking the law?

While there are some exceptions, in order to send people commercial electronic messages, you need to have their consent, an area in CASL over which the CRTC has responsibility. For more information, you may visit theCRTC's resource page at http://www.crtc.gc.ca/antispam.

What are the guidelines about gaining proper consent?

Under CASL, the CRTC is responsible for the rules regarding the sending of commercial electronic messages and appropriate consent. For more information, you may visit the CRTC's resource page at www.crtc.gc.ca/antispam.