



The coming into force of Canada's anti-spam legislation (CASL)

resulted in amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the federal private sector privacy law which covers the collection, use and disclosure of personal information in the course of commercial activities. These changes to the law included restrictions related to electronic address harvesting.

What is electronic address harvesting?

- By and large, it's the use of a computer program to indiscriminately collect electronic addresses, such as email addresses.

Why is this important to organizations that don't engage in this practice?

- While many organizations may not harvest addresses, the restrictions are highly relevant to organizations of all shapes and sizes, in all sectors. All organizations are responsible for ensuring that the electronic addresses they, or third parties acting on their behalf, collect in the course of their commercial activities have been obtained with appropriate consent.

What can organizations do to avoid contravening the law?

- All organizations conducting email marketing need to:
 - ▶ Follow due diligence to avoid inadvertently harvesting, or using harvested email addresses; and
 - ▶ Take appropriate precautions when:
 - working with a third party that has been contracted to do email marketing on their behalf; or
 - buying a list from a vendor to do email marketing in-house.

What are some practical steps to take?

1) Ask questions: It is your responsibility to confirm if a third-party company you are dealing with is aware of PIPEDA and abiding by its provisions. So, when buying a list of addresses from a vendor or employing a firm to conduct e-marketing on your behalf, be sure to ask:

- ▶ **Where do they get e-mail addresses and how were they gathered?** For example, are people providing their addresses knowing what they will be used for and have they provided their consent to this use? Or, are the addresses being generated or scraped, or otherwise collected indiscriminately?
- ▶ **How was consent obtained?** Even when your organization relies on a third-party to collect e-mail address lists for marketing purposes, you are responsible for ensuring that appropriate consent is obtained. Generally, an organization is required to inform individuals in a meaningful way of the purposes for the collection, use or disclosure of their email address, which is their personal information. Consent should be obtained before or at the time of collection, and renewed when a new use of the address is identified.
- ▶ **How are the lists kept up to date?** Organizations should enable individuals to withdraw consent to the use of their personal information at any time, subject to legal or contractual restrictions and reasonable notice.
- ▶ **How are organizations purchasing and using lists kept informed of changes?** When people whose addresses are on a list you purchased withdraw their consent, you need to know this, so that you can stop sending them commercial messages.

2) Put it in writing: Once you've asked these questions, take appropriate steps to establish that you have exercised due diligence, by keeping a written record and/or contract with the list vendor or e-mail marketing firm. Make it a clear obligation up front that you don't want to have your commercial messages sent to people who have not consented to:

- ▶ providing their email addresses; or
- ▶ receiving commercial messages.

Who is responsible for what under CASL?

Our Office shares responsibility for enforcing CASL with the Canadian Radio-television and Telecommunications Commission (CRTC) and the federal Competition Bureau.

The CRTC is 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 addresses false or misleading representations and deceptive marketing practices in the electronic marketplace.

We meanwhile focus on two types of violations:

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

Where can I get more information?

To find out more about the Office of the Privacy Commissioner of Canada's responsibilities under CASL, visit www.priv.gc.ca/casl or call 1-800-282-1376.

For information about CASL overall and the responsibilities of our enforcement partners, visit www.fightspam.gc.ca