April 2011

Sending commercial electronic messages under Canada's Anti-Spam Legislation

Bill C-28, Canada's Anti-Spam Legislation (or "CASL", formerly known as the *Electronic Commerce Protection Act* and the *Fighting Internet and Wireless Spam Act*), will come into force later in 2011. The following provides an overview of CASL's main requirements and penalties that apply to sending commercial electronic messages.

Overview of legislation and consequential amendments

CASL establishes rules for the sending of commercial electronic messages ("CEMs"), the installation of computer programs, and prohibits the unauthorized alteration of transmission data.

The *Competition Act* has also been amended to prohibit false or misleading representations in the sending of a CEM, whether in the content, subject line, or sender information of a message.

Related amendments to federal privacy legislation, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), address the use of address harvesting and dictionary attacks - two techniques that allow for the automatic collection and generation of electronic addresses. In addition, PIPEDA expressly prohibits the use of computer programs to surreptitiously collect personal information from a computer program.

CASL provides the Canadian Radio-television and Telecommunications Commission ("CRTC") - the primary enforcement agency under the legislation - with new investigatory powers, as well as the ability to impose administrative monetary penalties. CASL also includes a private right of action that allows individuals and companies to sue and recover damages resulting from violations of the Act and related amendments to the *Competition Act* and PIPEDA.

All businesses, including email service providers ("ESPs"), advertising agencies and direct senders, need to be aware of their exposure under the legislation, as potentially significant penalties can result from violations of the Act. The following provides an overview of CASL's main requirements and penalties that apply to sending CEMs.

Commercial electronic messages (CEM)

A CEM is broadly defined to include any electronic message that includes any commercial content whatsoever, including advertisements, offers or promotions relating to the purchase or sale of goods or services, as well as business or investment opportunities. This also includes a message that promotes a person who does any of the forgoing (e.g., a real estate agent).

CASL addresses all forms of electronic messaging, including email, SMS text messages, and messages sent via social networking. The rules apply broadly to any CEM that is sent from or accessed by a computer system located in Canada. This means that the law applies to all senders of CEMS into or out of Canada, no matter where they are located.

Three primary rules

There are three primary rules when sending a CEM: consent, identification, and unsubscribe.

1. Consent

The default rule under CASL is that the sender must have consent from the recipient before a CEM is sent. Consent may be either express or implied, depending on the circumstances.

Consent is not necessary if the message:

- is sent to someone with whom the sender has a personal or family relationship;
- is an inquiry about or an application for a product or service;

Consent is also not required if the message solely (note that the identification and unsubscribe requirements still apply):

- provides a quote or estimate, if requested;
- facilitates a commercial transaction;
- provides warranty or safety information;
- provides information about an ongoing subscription, membership, etc.;
- provides information related to an employment relationship or benefit plan; or,
- delivers a good or service.

Consent may be implied in any of the following four circumstances:

1. The sender and recipient have an existing business relationship. An existing business relationship arises where the sender and recipient have done some business together in the two years before the message is sent, or an inquiry was made by the recipient in the six months before the message is sent.
2. The sender and recipient have an existing non-business relationship. A non-business relationship exists where the sender: (a) is a charity, political party or political candidate, and the recipient has volunteered or made a donation within the previous two years; or (b) is a club, association of volunteer organization of which the recipient has been a member within the previous two years.
3. The recipient has conspicuously published their electronic address (e.g., on a website), has not expressly stated that they do not wish to receive unsolicited messages, and the content of the message is related to the recipient's professional capacity; or,
4. The recipient has disclosed their electronic address directly to the sender, has not expressly stated that they do not wish to receive unsolicited messages, and the content of the message is related to the recipient's professional capacity.

Note that CEMs cannot be sent once this time periods described in 1 and 2 above expire, unless express consent is obtained.

2. Identification

Senders must be clearly identified in each message. If the message is sent on behalf of another person, that person must be identified as well.

3. Unsubscribe mechanism

Every CEM must contain a functional unsubscribe mechanism that enables the recipient to unsubscribe, at no cost. The law states that unsubscribe requests must be processed 'without delay', and in any event no later than 10 business after the request has been sent. The unsubscribe mechanism must remain functional for 60 days after the message is sent.

Penalties and enforcement

CASL is enforced by the CRTC. Related amendments to the *Competition Act* are enforced by the Competition Bureau, while the Office of the Privacy Commissioner of Canada ("OPC") is responsible for enforcing PIPEDA.

The CRTC has the ability to impose administrative monetary penalties for violations of CASL up to $1 million per violation for individuals, and $10 million per violation for other persons (e.g., businesses).

CASL also includes a private right of action, which enables any person affected by a violation of CASL and related amendments to PIPEDA and the *Competition Act* to sue for and recover actual and statutory damages.

It is important to note that officers and directors can be held liable for violations committed by a corporation. Organizations are also vicariously liable for violations committed by employees or agents acting within the scope of their authority.

CASL was drafted to provide protection for "honest mistakes" committed by otherwise compliant organizations. Most important in this regard is the "due diligence" defence, which provides that a person must not be found to be liable for a violation if they establish that they exercised due diligence to prevent the commission of the violation." This makes it vital for senders and ESPs to ensure that they have taken appropriate steps to ensure compliance with CASL.

Enforcement against non-Canadian senders

It is tempting for non-Canadian organizations to ignore CASL based on the assumption that it cannot be enforced outside of Canada. However, the Canadian enforcement agencies have been provided with extensive powers to share information and cooperate with foreign agencies, such as the Federal Trade Commission. Furthermore, private litigants that obtain a judgment in one country are often able to have those judgements enforced abroad.

Application to service providers

CASL applies broadly to anyone who "sends", "causes", "permits", "aids", "induces", or "procures" a CEM to be sent. While telecommunications service providers are protected from liability where they "merely provide a telecommunications service that enables the transmission of the message," whether or not this protection applies to ESPs will depend on the nature of the services provided.

This means that ESPs are potentially liable for messages sent by or on behalf of clients in contravention of CASL (note that the concept of a "routine conveyance" does not exist under CASL). It is essential that ESPs undertake

appropriate measures to prevent violations of CASL from occurring in the first place, and, secondly, to protect themselves from liability by being able to demonstrate that due diligence has been exercised should any type of enforcement against an ESP be pursued. Such measures include making clients aware of their obligations under CASL, and appropriately allocating liability through agreements with clients.

How to prepare

While the penalties under CASL are potentially significant, businesses do not need to be afraid to continue to engage in electronic marketing campaigns to reach out to existing and potential customers. In many cases, only a few small changes to existing practices, if any, may be necessary.

It is important that **anyone** involved in the process of sending CEMs - brand owners, marketers, email service providers, etcetera - be aware of the law's requirements to ensure that they are protected from liability under CASL, through the following measures:

- Audit existing practices to ensure compliance with CASL, and take appropriate remedial steps where necessary; and,
- Ensure that evidence of consent exists - whether express or implied.

ESPs should

- Educate clients and obtain assurance that clients are CASL compliant; and
- Appropriately allocate liability for non-compliance through agreements.

n*N*ovation LLP is a preeminent Canadian law firm specializing in federally regulated matters, including privacy, advertising, electronic commerce, and competition law. n*N*ovation LLP lawyers have extensive experience with online marketing, and have been involved in the development and implementation of CASL. Look for a compliance guide authored by Shaun Brown and Kris Klein to be published by Carswell in the of spring 2011. For more information please contact Shaun Brown at (613) 656.1297, or sbrown@nnovation.com.

The Email Sender and Provider Coalition is a cooperative group of industry leaders working to create solutions to the continued proliferation of spam and the emerging problem of deliverability. Its membership provides volume mail delivery services to an estimated 250,000 clients - representing the full breadth of the U.S. marketplace. The ESPC is currently working on solutions to spam and deliverability concerns through a combination of legislative advocacy, technological development, and industry standards. For more information please contact the ESPC at info@espcoalition.org.

* The forgoing is provided for informational purposes only, and is not a substitute for qualified legal advice.