Bloomberg BNA

Privacy and Security Law Report®

Canada's Anti-Spam Law—The Countdown Begins

BY MICHAEL FEKETE AND PATRICIA WILSON

The clock is ticking. The Canadian federal government has announced that the electronic messaging provisions of its game-changing anti-spam law will come into force **July 1, 2014**.[1] The provisions regarding installation of computer programs will come into force **Jan. 15, 2015**. The private right of action for breaches of Canada's anti-spam law (CASL) will not come into force for an additional three years, **July 1, 2017**.

While regulations published Dec. 4, 2013, exempt some activities,[2] legitimate businesses and organizations are not insulated from inflexible, prescriptive rules that will require them to make significant changes to how they operate.

Not Limited to Spam and Spyware

You don't need to be a spammer, or even be located in Canada, for CASL to regulate the everyday activities of your business—such as sending an e-mail, text or instant message to a customer or updating a copy of your mobile application installed on a customer's smartphone.

CASL creates an express (opt-in) consent-based regime that will apply to almost all electronic messages sent for a commercial purpose—even if encouraging participation in a commercial activity is not the primary purpose of the message. The same express, opt-in consent standard will apply to the installation of almost all computer programs—even if the program is necessary or useful for the continued operation of a consumer product.

CASL also introduces new prohibitions on using address harvesting software, sending misleading electronic messages and altering an electronic messages' ''transmission data.''

Likely the Most Onerous Legislation of Its Type in the World

While some other jurisdictions have adopted ''opt-in'' consent models, CASL goes two steps further. It prescribes how consent needs to be requested and provides no generally worded ''implied consent'' exception to its opt-in standard. While some exceptions to express consent exist, they are limited to specific, identified situations and do not allow for an assessment of what is reasonable in the circumstances.

What Compliance Means for Business

Once CASL comes into force, relying upon e-messaging and software installation practices established under existing laws—whether it be the U.S. CAN-SPAM Act or Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)—will be inadequate. Of particular importance will be ensuring compliance with CASL's unique rules that govern:

- requests for consent;

[1] An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities That Discourage Reliance on Electronic Means of Carrying Out Commercial Activities, and to Amend the Canadian Radiotelevision and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23 (Can.), *available at* http://laws-lois.justice.gc.ca/PDF/E-1.6.pdf. The Canadian government announced the implementation dates in December 2013 (12 PVLR 2071, 12/16/13).

[2] Electronic Commerce Protection Regulations, SOR/2012-36 (Can.), *available at* http://laws-lois.justice.gc.ca/PDF/SOR-2012-36.pdf.

Michael Fekete is a partner at Osler, Hoskin & Harcourt LLP in Toronto and co-chair of the firm's Technology Group.

Patricia Wilson is a partner in Osler's Litigation Department in Ottawa. Fekete and Wilson both have extensive experience advising clients on Canada's anti-spam law and privacy laws in Canada.

- demonstrating that CASL-compliant express consent has been obtained or that one of the exceptions to consent applies;
- the content of commercial electronic messages;
- the presentation and operation of an unsubscribe mechanism; and
- assistance in removing or disabling a computer program.

The disruptive impact of CASL has been compounded by compliance guidelines issued by the regulator with primary enforcement powers, the Canadian Radio-television Telecommunications Commission (CRTC). The CRTC has taken the position that an unchecked opt-out box or a pre-checked opt-in box cannot be used to obtain express consent. In addition, the CRTC has suggested that requests for consent must not be contained in, or bundled with, requests for consent to the general terms and conditions of use or sale.

Transitional Relief After Coming Into Force

CASL does provide limited transitional relief after it comes into force. Implied consent for a period of 36 months will be deemed to exist (unless consent is withdrawn earlier) where there is a CASL-qualifying existing business or non-business relationship and the relationship includes the communication of commercial electronic messages (CEMs). During the transitional period, the definition of existing business or non-business relationship is not subject to the limitation periods (two years and six months) for implied consent to exist that would otherwise be applicable under CASL. The law provides a similar three-year transition period for the installation of updates or upgrades to a computer program installed prior to the coming into force of the law's computer program provisions.

The other requirements of CASL, however, such as those relating to the form and content of opt-out opportunities, will apply during the transition period. And, to the extent that the transitional provisions do not apply, CASL consent requirement will apply in full with respect to electronic messages, updates and upgrades as soon as CASL is in force.

Why CASL Can't Be Ignored

It is not only organizations operating in Canada who will need to comply with CASL. The legislation has been deliberately drafted to capture electronic messages sent to, and computer programs installed on, any computer system in Canada. This will mean that commercial electronic messages and computer installations originating outside Canada but sent to a Canadian computer will be regulated under CASL, even absent a business presence or affiliate in Canada.

There are stiff penalties for noncompliance with CASL, including administrative monetary penalties of up to C$10 million ($9.2 million) for corporations (C$1 million ($920,000) for individuals). The power of the CRTC to levy administrative monetary penalties comes into force **July 1, 2014.**

In addition, class actions are very likely, given that CASL's private right of action creates what can be described as the ''perfect conditions'' for class proceedings:

- standing to sue by any person who is ''affected'';
- broad and inflexible rules; and
- statutory damages of up to $1 million a day.

Although the private right of action will not come into force until **July 1, 2017**, compliance activities undertaken today may be critical to protect against the anticipated lawsuits.

Also important is that an organization cannot insulate itself from liability by having a service provider send commercial electronic messages or install computer programs on its behalf.

Vicarious liability provisions in the statute mean that officers, directors and agents of an organization may face personal liability.

What You Need to Do

Below are the 10 most critical (and challenging) compliance planning activities:

1. **Creating a comprehensive list of the categories of the CEMs sent by your organization.** This includes identifying all of the circumstances in which each business unit within your organization uses e-mail messaging, text messaging, instant messaging and social media messaging to encourage participation in a commercial activity.

2. **Developing a policy and guidelines for determining whether a message is a CEM and whether an exception applies.** This policy will enable a case-by-case determination in light of the specific circumstances of each category of CEMs that your organization sends.

3. **Creating a comprehensive list of the categories of computer programs that your organization directly or indirectly installs on any computing devices that it does not own.** In addition to identifying any software included in the organization's products or services offerings, this includes identifying the circumstances in which the organization distributes software updates or upgrades.

4. **Developing a policy and guidelines for determining when the organization will need to (and when it will want to) obtain CASL-compliant consent for installing a computer program, including whether an exception applies.** This policy will enable a case-by-case determination in light of the specific circumstances of each category of computer program that the organization installs and will include an assessment of whether CASL applies to software that is downloaded by end users.

5. **Determining if electronic addresses your organization collected previously can be used after CASL comes into force and, if not, scrubbing existing databases or obtaining ''fresh'' consent will be necessary.** This includes evaluating if you have an ''existing business relationship'' and how you may be able to benefit from the three-year transition period found in CASL.

6. **Updating processes for requesting consent.** This may include providing an opportunity to withhold consent separate from acceptance of the terms of a consumer agreement.

7. **Ensuring there are adequate systems in place for maintaining a record of each consent obtained.** For written consent, this ideally means storing a record of date, time, purposes and manner of the consent in a database; for oral consent, this ideally means verification

  PVLR ISSN 1538-3423

Final CASL Regulations Provide Limited Relief for Businesses

The delays in CASL coming into force are attributable, in part, to the government undertaking a lengthy consultation process on regulations that define certain terms and provide exclusions for certain business activities that would otherwise be prohibited. These regulations were published in final form Dec. 4, 2013.

While the regulations were disappointing in many respects (including the lack of binding guidance on the meaning of ''commercial electronic message,'' the scope of the computer program provisions and the situations in which previously acquired consent will be adequate after CASL comes into force), they do include some meaningful exclusions.

Exemptions to the electronic message provisions added through the regulations include those CEMs:

- that are internal and concern the activities of the business;
- that are external where the sending and receiving organizations have a relationship and the message concerns the activities of the recipient;
- sent to enforce or satisfy legal rights or juridical obligations, court orders or judgments; and
- sent on certain limited access websites by the account provider (such as electronic banking websites).

Exclusions to the express consent requirement in respect of the installation of computer programs that are added through the regulations include a program that is:

- installed by or on behalf of a telecommunications service provider* solely to protect the security of all or part of its network from a current and identifiable threat to the availability, reliability, efficiency or optimal use of its network;
- installed, for the purpose of updating or upgrading the network, by or on behalf of the telecommunications service provider who owns or operates the network on the computer systems that constitute all or part of the network;
- necessary to correct a failure in the operation of the computer system or a program installed solely for that purpose.

These exclusions are triggered only if it is reasonable to believe that the owner or authorized user of the computer consented to the program's installation.

* ''Telecommunications service'' is defined very broadly in CASL as ''a service, or a feature of a service, that is provided by means of telecommunications facilities, whether the telecommunications service provider owns, leases or has any other interest or right respecting the telecommunications facilities and any related equipment used to provide the service.'' It is possible that this definition will capture Internet-based service providers in addition to traditional telecommunications service providers like mobile phone or telephone companies.

by independent third party or retaining a complete and unedited audio recording.

8. **Building fields into the organization's databases to store the data the organization will require to rely upon implied consent.** This will typically include fields to record the date when an individual entered into a contract, purchased a product or made an inquiry

9. **Updating templates used to send electronic messages.** This includes ensuring that each template includes all mandatory identity and contact information and a compliant unsubscribe mechanism.

10. **Updating unsubscribe mechanisms and processes for giving effect to unsubscribe requests.** This includes having systems that will provide any required notices to third parties, including affiliates, and for handling requests from individuals to stop receiving all categories of commercial electronic messages.