

## Canada's Anti-Spam Law Casts a Wide Net – Requires all Organizations to take Action

Canada's anti-spam law (known as "CASL") will come into force on July 1, 2014. Virtually all organizations will need to make changes to their practices for sending commercial electronic messages or face significant new penalties.

CASL is perhaps the most onerous legislation in the world that regulates the use of commercial electronic messaging and the installation of computer software. It goes much further than regulating bulk, unsolicited email communications often referred to as "spam". Rather, it creates an express (opt-in) consent-based regime that will apply to almost all electronic messages sent for a commercial purpose. The same standard for consent will apply to the installation of computer programs. For a summary of the computer program provisions, click [here](#).

### **STIFF PENALTIES**

The electronic messaging rules will be enforced with stiff penalties, including administrative monetary penalties of up to C\$10,000,000 for corporations (C\$1,000,000 for individuals) and statutory damages of up to \$1 million a day. As well, beginning on July 1, 2017, a private right of action will allow consumers and businesses to commence enforcement proceedings and recover damages. Class actions are anticipated.

### **SCOPE OF THE ELECTRONIC MESSAGING RULES**

The electronic messaging rules will apply to commercial electronic messages or "CEMs" sent by telecommunication to an email, instant messaging, telephone or similar account. A message will be regarded as being "commercial" in nature if it has, as its purpose or one of its purposes, the encouragement of participation in a commercial activity.

Exceptions for limited types of messages are provided for in CASL or related regulations issued under it. Of most relevance to businesses are the exceptions for a CEM:

- that is sent to a person who is engaged in a commercial activity and consists solely of an inquiry or application related to that activity;
- that is sent in response to a request, inquiry or complaint or is otherwise solicited by the person to whom the message is sent;
- that is sent by an employee, representative, consultant or franchisee of an organization:

- to another employee, representative, consultant or franchisee of the organization and the message concerns the activities of the organization, or
- to an employee, representative, consultant or franchisee of another organization if the organizations have a relationship and the message concerns the activities of the organization to which the message is sent;
- that is sent to a limited-access secure and confidential account to which messages can only be sent by the person who provides the account to the person who receives the message; and
- if the person who sends the message or causes or permits it to be sent reasonably believes the message will be accessed in a foreign state that is listed in the schedule and the message conforms to the law of the foreign state that addresses conduct that is substantially similar to conduct prohibited under the CEM rules in CASL.

### **OPT-IN CONSENT REQUIREMENTS**

Under CASL, CEMs can be sent only with the express (opt-in) consent of the recipient, unless the sender can demonstrate that there is a statutory exception. Examples of exceptions include messages that solely:

- provide a requested quote or estimate;
- facilitate, complete or confirm a commercial transaction; and
- provide warranty information, product recall information, or safety or security information about a product that the message recipient has used or purchased.

There also will be limited instances in which consent can be implied, including where there is an “existing business relationship” between the sender and the recipient. Generally speaking, such a relationship will exist if the sender can demonstrate that:

- there is a business relationship arising from the purchase or lease of a product, goods or a service within the prior two-year period;
- there is a written contract with the recipient (other than in respect of the purchase or lease of products, goods or services and certain other subject matter) until two years following termination of the contract; or
- there was an inquiry or application made by the recipient within the prior 6 months regarding certain commercial activities, including purchases of goods or services.

Note, however, that these time periods will not apply during the initial three years after the anti-spam rules come into force if the existing business relationship includes communications using CEMs and the recipient has not opted-out of receiving them.

## CONSENT DISCLOSURE REQUIREMENTS

When requesting consent for the sending of CEMs, businesses will need to set out clearly and simply the purpose for which consent is being sought, a statement that consent can be withdrawn and prescribed “identity” and “contact” information. The identity information is the name under which the person requesting consent carries on business and, if applicable, a statement indicating that this person is requesting consent on behalf of another person (together with the name under which the other person does business). The required contact information is a mailing address and either a telephone number providing access to an agent or a voice messaging system, an email address or a web address for the person requesting consent or, if different, the person on behalf of whom consent is being sought.

## FORM AND CONTENT REQUIREMENTS

CEMs will need to include an unsubscribe mechanism that meets requirements prescribed in regulations and allows a message recipient to opt out of all electronic messages or specified categories. In addition, CEMs will need to include the sender’s contact information, identify the person who sent the message, identify the person on whose behalf the message is sent (if different from the sender), and set out other information prescribed in regulations.

## CRITICAL LEGAL ISSUES

There is no shortage of legal issues that businesses will need to consider in the context of their compliance planning activities. Perhaps the three most significant issues applicable to the electronic messaging rules are:

- deciding if a message is a CEM:
  - *CASL defines CEM by reference to whether it would be reasonable to conclude the message has as its purpose, or one of its purposes, to encourage participation in a commercial activity; a non-binding Regulatory Impact Analysis Statement issued by the Minister of Industry includes commentary that suggests the scope of CEMs does not apply to certain types of messages (such as surveys, newsletters and messages involving a pre-existing commercial relationship or activity that is already underway), but it is uncertain if the CRTC – which has regulatory enforcement powers – agrees with this interpretation);*
- deciding whether consent can be obtained through a license or consumer agreement or terms of use document:
  - *although there is nothing in CASL that addresses this issue, the CRTC has suggested through non-binding enforcement guidelines that consent cannot be bundled with requests to confirm agreement with a license or other consumer agreement (such as privacy policies or general terms and conditions of sale); rather, the CRTC wants*

*consumers to be given the opportunity to accept the agreement terms, but separately have the ability to refuse to provide consent for CEMs; and*

- deciding whether consent can be obtained through the use of a pre-checked box:
  - *although there is nothing in CASL that addresses this issue, the CRTC has suggested through non-binding enforcement guidelines that valid consent cannot be obtained using pre-checked boxes or other forms of opt-out consent.*

## **OTHER PROHIBITED CONDUCT**

### **Address Harvesting**

The Personal Information Protection and Electronic Documents Act (PIPEDA) has been amended to restrict “address harvesting,” or the unauthorized collection of email addresses through automated means (i.e., using a computer program designed to generate or search for, and collect, email addresses) without consent. The use of an individual’s email address collected through address harvesting also is restricted.

### **Misleading Advertising**

The Competition Act has been amended to make it an offence to provide false or misleading representations in the sender information, subject matter information, or content of an electronic message. The same conduct will be “reviewable conduct” pursuant to the rules governing deceptive marketing practices.

### **Pharming**

The alteration of “transmission data” in an electronic message without the consent of the sender or the recipient is prohibited. This provision is intended to address the practice of “pharming” whereby a website user is redirected to a bogus website upon clicking on a link included in an email message which appears to be from the legitimate company.

For more information about how Osler can help you with your compliance activities, please contact:

**Michael Fekete**

mfekete@osler.com

416.862.6792

**Andraya Frith**

afrith@osler.com

416.862.4718

**Dominic Mochrie**

dmochrrie@osler.com

416.862.5994

**Pat Wilson**

pwilson@osler.com

613.787.1009

This memorandum is a general overview of the subject matter and cannot be regarded as legal advice. Subscribe to a full range of updates at [osler.com](http://osler.com). You can unsubscribe at any time at [osler.com](http://osler.com) or <http://unsubscribe.osler.com>. © Osler, Hoskin & Harcourt LLP

[counsel@osler.com](mailto:counsel@osler.com)  
[osler.com](http://osler.com)

Toronto  
Montréal  
Calgary  
Ottawa  
New York