July 5, 2011

Canada’s Anti-Spam Law Coming Into Force

Author(s): Michael Fekete, Nicole Kutlesa, Patricia Wilson

By enacting what may be the most comprehensive anti-spam law in the world, Canada’s Parliament has placed new and significant obligations on businesses that communicate and market electronically.

Known as Canada’s Anti-Spam Law, or CASL, the new rules go much further than restricting bulk, unsolicited e-mail messages, by creating an express consent regime that applies to almost all e-mails and other electronic messages sent for a commercial purpose. And unlike the U.S. CAN-SPAM Act, which applies only to e-mail, CASL’s anti-spam provisions also apply to other forms of electronic communication, such as text messages, instant messaging and social media messaging.

CASL was passed in December 2010 and is awaiting proclamation. Draft regulations that provide rules important to ensuring compliance regarding the content of notices and consents were published for comment by the Canadian Radio-Television and Telecommunications Commission (CRTC) on June 30, 2011 (and in the Canada Gazette on July 2, 2011) and are subject to a comment period until August 29, 2011. Finalization of the regulations and the coming into force of CASL could happen as early as September 2011, although December 2011 or early winter 2012 is a more likely timeframe.

CASL OVERVIEW

CASL enacts rules to restrict spam (unsolicited commercial electronic messages), spyware (installation of computer programs on another person’s computer), and certain practices, such as pharming and address harvesting. The anti-spam rules will require express, opt-in consent from recipients, subject to limited exceptions. The CASL consent regime is stricter than existing requirements under Canada’s privacy law, Personal Information Protection and Electronic Documents Act (PIPEDA), which generally permits opt-out consent for marketing messages and allows for reliance on implied consent in broader circumstances than does CASL.

CASL’s opt-in consent requirement will require businesses that communicate by e-mail with customers, subscribers or others to revisit their practices for obtaining and documenting consent. In many cases, businesses will need to obtain “new” or “refreshed” consent from individuals on an opt-in basis.

CASL provides limited exceptions to its opt-in consent requirement. Businesses can rely on implied consent to send e-mails to recipients when there is an “existing business relationship,” although this exception is largely limited to specific categories of customers who have been active within the prior two year or six month period. A three year transitional period after CASL comes into force has been provided.
for both active customers and inactive customers with whom there is a qualifying business relationship, allowing electronic messages and requests for consent to be sent to customers during this time period. In addition, there are business card and address publication exclusions from the express consent requirement for sending commercial electronic messages to recipients who have published or provided their electronic address without stating they do not wish to receive messages, where the message is relevant to recipients’ business or professional role.

The anti-spyware provisions of CASL include an express consent requirement for the installation of computer programs and prescriptive disclosure and notice requirements. Although the principal policy objective of these provisions is to deter the distribution of “spyware,” the consent and notice provisions will apply to most computer programs and regardless of whether the program is installed for a malicious purpose. Both “basic” and “function-specific” disclosure notices (including reasonably foreseeable impacts on the user’s computer and email contact information) must be given to end users in advance of installation of a program.

Exceptions from the anti-spyware consent requirement are provided for certain categories of computer programs, including cookies, Java Script, HTML and operating systems, but only where the person’s conduct makes it reasonable to believe that they consent. In addition, to allow for automatic update services offered by many software publishers, the installation of an update or upgrade to a computer program will be exempted from the express consent and “basic” disclosure requirements if: (i) the program was initially installed in accordance with those requirements; (ii) the initial consent entitles individuals to receive the update or upgrade; and (iii) the installation is made in accordance with the initial consent. A transition period of three years, or until consent is withdrawn, is provided for the installation without express consent of updates or upgrades to programs installed on a user’s computer prior to CASL coming into force.

STIFF PENALTIES

CASL imposes significant monetary penalties for non-compliance and creates new violations and offences for false or misleading subject lines, e-mail address harvesting and pharming. The new anti-spam and anti-spyware rules will be enforced with stiff penalties, including administrative monetary penalties of up to $10,000,000 for corporations ($1,000,000 for individuals). As well, a private right of action will allow consumers and businesses to commence enforcement proceedings and recover damages, including statutory damages of up to $1 million a day.

WHAT BUSINESSES NEED TO DO TO PREPARE FOR CASL

Businesses and non-profit organizations using e-mail, text, instant messages or other electronic messaging, such as social media messaging or Twitter, to communicate with customers, subscribers, clients or prospects should:

- review all categories of electronic communications to identify those that are “commercial electronic messages” (CEMs) under CASL;
- develop CASL compliant contact and consent notices, as well as opt-out mechanisms for CEMs;
- determine if opt-in consent has been obtained from CEM recipients;
- identify whether consent of recipients can be implied based on an “existing business relationship” under CASL, or whether the recipient’s electronic address was provided or published without a refusal to receive CEMs (the “business card” and “publication” exceptions);
refresh or renew consents from recipients by securing opt-in consent
before CASL comes into effect or where no existing business relationship exists; or
where it applies, during the three (3) year transition period for existing business relationships;
cull e-mail and subscription lists of CEM recipient addresses where express consent is required but
cannot be established;
establish opt-in consent and consent renewal mechanisms on web pages, agreements, terms of use or
applications in accordance with CASL requirements;
refresh e-mail and electronic message marketing lists on a rolling basis to obtain consent from or
removal of customers who are not active for two (2) years;
develop consents, disclosures and notices to computer users about the installation of computer
programs;
implement procedures for operationalizing opt-out requirements “without delay” but within 10
business days in any event; and
establish internal guidelines, training and operational controls to ensure compliance with CASL.

CASL is likely to change electronic marketing in Canada significantly by developing opt-in, consent-based
marketing and more targeted promotion methods. Organizations must be innovative and take action
now and during the three year transition period (where it applies) to implement new, CASL-compliant e-
mail and electronic direct marketing strategies and computer program installation practices or face
significant regulatory and legal liability.

For our earlier article on Canada’s Anti-Spam Legislation, visit the February 2011 issue of Osler’s

Save the Date! Join Osler partners Patricia Wilson, Michael Fekete, and Nicole Kutlesa on September
15, 2011, for a one hour webcast on Canada’s Anti-Spam Law, its impact on businesses and a discussion
of CASL compliance strategies. Registration information will be provided shortly.

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 our commercial activities, S.C. 2010, c.
23, formerly referred to as the “Fighting Internet and Wireless Spam Act.”

2 “Pharming” is a practice whereby a website user is redirected to a bogus website upon clicking on a link
within an email message that appears to be from a legitimate company.
CONTACT US

For more information, please visit osler.com or contact the following individual(s):

TORONTO
Michael Fekete, Partner,
Technology
National Innovation Leader
416.862.6792
mfekete@osler.com

© Osler, Hoskin & Harcourt LLP. This content is for general information purposes only and does not constitute legal or other professional advice or an opinion of any kind. You can subscribe to receive updates on a range of industry topics at osler.com/subscribe.