

Blakes Bulletin

Communications/Information Technology

Spammers Beware: Proposed E-Commerce Protection Act Prohibits Unsolicited Commercial Electronic Messages

TRICIA KUHL AND MARK MACNEIL

On April 24, 2009, what might become Canada's first anti-spam legislation was tabled in the House of Commons for first reading. If enacted, Bill C-27 would create the *Electronic Commerce Protection Act* (the ECPA), the primary purpose of which is to promote e-commerce in Canada by regulating commercial conduct that currently undermines Canadians' confidence in conducting business online. To this effect, the ECPA not only prohibits certain forms of spam, phishing and the use of spyware in commercial activities, it establishes hefty fines for any violation of the rules established thereunder. Surprisingly, the ECPA also sets out amendments to the *Telecommunications Act* which would dismantle the legislative framework of the recently established national do-not-call list relating to unsolicited telecommunications. It is important to note that the ECPA is only proposed legislation which may be amended during the legislative process, or may never become law.

SCOPE OF THE ECPA

What is a Commercial Electronic Message?

The ECPA only applies to the sending of a "commercial electronic message", which is defined under the ECPA as a message sent by any means of telecommunication, including a text, sound, voice or image (i.e., cellular phone text messages as well as e-mail) to an electronic address (i.e., an e-mail, instant messaging, telephone or similar account), the purpose, or one of the purposes of which, is to encourage participation in a commercial activity (an e-message). The definition includes an e-message that:

- (i) offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land or promotes or advertises any of the foregoing;
- (ii) offers to provide a business, investment or gaming opportunity or promotes or advertises any of the foregoing; or

- (iii) promotes a person as being a person who does, or intends to do, anything referred to in (i) or (ii) above.

Exceptions

The following types of e-messages are exempt from the reach of the ECPA:

- (i) a message sent by an individual to another individual with whom they have a personal or family relationship;
- (ii) a message sent to a person engaged in a commercial activity for the sole purpose of an inquiry or an application related to that activity;
- (iii) a voice recording sent to a telephone account;
- (iv) an interactive two-way voice communication between individuals;
- (v) a fax sent to a telephone account; and
- (vi) a message that is of a class or sent in circumstances that will be specified in the regulations (note: no draft regulations have yet been published).

Furthermore, telecommunications service providers who merely provide a telecommunications service that enables the transmission of the e-message will not, under the ECPA, be held liable for spamming. Finally, the ECPA does not apply to broadcasting by a broadcasting undertaking.

REQUIREMENTS AND PROHIBITIONS UNDER THE ECPA

1. Consent Required to Send Commercial Electronic Messages

Under the ECPA, no person is permitted to send an e-message without the recipient's prior consent. Consent is implied when the sender and the recipient have an existing business or non-business relationship. An "existing business relationship" is defined as a business relationship between the person who sent or caused the message to be sent (the sender) and a person who has:

- (i) purchased, leased or bartered a product, goods, a service, land or an interest or right in land from the sender, within the 18-month period immediately preceding the date on which the message was sent;

CONT'D ON PAGE 2

CONT'D FROM PAGE 1

(ii) accepted, within this 18-month period, a business, investment or gaming opportunity offered by the sender;

(iii) entered into a written contract with the sender in respect of another matter, if the contract is currently in existence or expired within this 18-month period; or

(iv) made an inquiry or submitted an application to the sender, within the six-month period immediately preceding the date on which the message was sent, in respect of anything mentioned in paragraphs (i) or (ii).

An "existing non-business relationship" is defined as a non-business relationship between the sender and the person to whom the message is sent (the recipient) where the recipient, within the 18-month period preceding the date on which the message was sent:

(i) has made a donation or given a gift to the sender, has performed volunteer work for the sender or attended a meeting organized by the sender, where the sender is a registered charity, a political party or organization, or a person who is a candidate for publicly elected office; or

(ii) has been a member of the sender, where the sender is a club, association or voluntary organization (as defined in the regulations).

If the sender does not have an existing business or non-business relationship with the recipient, the sender must obtain the express consent of the recipient prior to sending the e-message. To obtain such express consent, the sender must set out clearly and simply:

(i) the purpose or purposes for which the consent is being sought;

(ii) information identifying the person seeking consent and, if applicable, the person on whose behalf the consent is being sought; and

(iii) other information which may be set out in the regulations.

In all cases, the ECPA requires the sender to:

(i) set out information identifying the sender of the message as well as, if applicable, the identity of the person on whose behalf the message is sent;

(ii) set out contact information of the sender, or of the person on whose behalf the message is sent, which must be valid for at least 60 days; and

(iii) set out a mechanism allowing the recipient of the message to "unsubscribe" or otherwise withdraw his consent to receive future messages, which must include an electronic address or hyperlink by which the indication can be sent.

2. Prohibition on Phishing

The ECPA prohibits, in the course of a commercial activity, the altering of transmission data in an e-message so that the message is delivered to a destination other than, or in addition to, the destination specified by the sender. This prohibition will not apply:

(i) if the sender has provided express consent to such type of phishing;

(ii) if transmission data is altered in accordance with a court order; or

(iii) to telecommunications service providers, if the alteration is made for the purposes of network management.

3. Spyware Prohibited

Installing a computer program on another person's computer system or, after having installed such a program, causing an e-message to be sent from that computer system, in the course of a commercial activity, is also prohibited under the ECPA. However, this prohibition does not apply in certain cases, for example, where the owner or authorized user of the computer system has provided express consent to such installation or message sending, or where the computer program is installed or message sent in accordance with a court order.

4. False or Misleading Representations Prohibited

The ECPA amends the *Competition Act* to prohibit persons from, knowingly or recklessly, sending or causing to be sent a:

(i) false or misleading representation in either the "sender information" (the part of the e-message that identifies the sender) or the "subject matter information" (the part of the e-message that summarizes the content of the message); or

(ii) representation in an e-message that is false or misleading in a material respect.

CONT'D ON PAGE 3

CONT'D FROM PAGE 2

LIABILITY UNDER THE ECPA

Administrative Fines

In order to effectively enforce the ECPA, the CRTC is given the power to investigate violations of the ECPA and to impose fines on ECPA violators of up to C\$1-million in the case of an individual, and up to C\$10-million in the case of any other person.

Civil Liability

A private right of action is also created under the ECPA for any person affected by a contravention of the ECPA. The affected person may apply to a court for an order that would require violators to pay (i) compensation for any loss or damage suffered by the applicant; and (ii) a maximum of C\$200 for each contravention, which may not exceed C\$1-million for each day on which any contravention occurred.

Penal Offences

The ECPA also sets forth certain penal offences which are punishable on summary conviction and subject to fines of up to C\$25,000 in the case of an individual, and of up to C\$250,000 in the case of any other person.

Directors' Liability

An officer, director, agent or mandatary of a corporation may be held liable for a violation of the ECPA if they are found to have directed, authorized, assented to, acquiesced or participated in the breach regardless of whether legal action is taken against the corporation. However, officers, directors, agents and mandataries of the corporation may not be held liable for contravening the ECPA if they establish that they exercised due diligence to prevent the violation.

AMENDMENTS TO PRIVATE SECTOR PRIVACY LEGISLATION

The ECPA amends the *Personal Information Protection and Electronic Documents Act* (PIPEDA) by adding a provision that will override the exception allowing personal information to be collected without the knowledge or consent of the individual concerned in certain circumstances. Specifically, the amendments will require consent to be obtained from the individual

concerned to collect and use the individual's electronic address if the e-address is collected by the use of a computer program that is designed or marketed for use in generating or searching for and collecting e-addresses.

Furthermore, pursuant to the amendments, consent will be required to collect and use an individual's personal information through any means of telecommunication, if the collection is made by accessing a computer system without authorization.

AMENDMENTS TO TELECOMMUNICATIONS ACT

The ECPA also sets out amendments that would repeal the legislative framework of the national do-not-call list (DNCL) recently established pursuant to the *Telecommunications Act*. The DNCL is a nationwide registry allowing Canadian consumers to opt-out of receiving unsolicited telemarketing calls by registering themselves on this list. For further information on the DNCL, please refer to our previous Blakes Bulletins on the subject:

- April 2009 [Blakes Bulletin on Communications: CRTC Expands Exemptions to Do Not Call List](#)
- August 2008 [Blakes Bulletin on Communications: Is Your Business Ready for the Launch of Canada's National Do Not Call List?](#)

If you have any questions about this or other aspects of the bill, please contact:

Sunny Handa	514-982-4008
Tricia Kuhl	514-982-5020
Mark MacNeil	514-982-5063

or another member of our [Communications Group](#) or our [Information Technology Group](#).

Go to blakes.com/english/subscribe.asp to subscribe to other Blakes Bulletins.

Blakes periodically provides materials on our services and developments in the law to interested persons. If you do not wish to receive further bulletins or other materials from Blakes, please contact Blakes Marketing Department at 416-863-3036 or dorothy.byers@blakes.com. For additional information on our privacy practices, please contact us at privacyofficer@blakes.com. *Blakes Bulletin* is intended for informational purposes only and does not create a lawyer-client relationship. The transmission of this information does not suggest Blakes or any of its lawyers are practising law of any jurisdiction other than Canada. The information provided in this bulletin is summary in nature and does not constitute legal advice. We would be pleased to provide additional details or advice about specific situations if desired. For permission to reprint articles, please contact Blakes Marketing Department at 416-863-2403 or lynn.spencer@blakes.com. ©2009 Blake, Cassels & Graydon LLP.