

Canada introduces anti-spam legislation

On April 24, 2009, the Canadian government introduced Bill C-27, which would establish the *Electronic Commerce Protection Act* (ECPA) and make significant consequential amendments to other federal legislation, including Canada's *Competition Act*, *Telecommunications Act* and *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The primary purpose of Bill C-27, which incorporates a number of the legislative recommendations made in 2005 by the government-mandated "Task Force on Spam", is to cut down on spam (unsolicited junk e-mail). However, the proposed ECPA aims to regulate not only spam, but also counterfeit websites and spyware, among other issues. In the broadest sense, therefore, the legislation is intended to bolster consumer confidence in online commerce.

Canada is currently the only G8 country and one of only four OECD (Organisation for Economic Co-operation and Development) countries without specific spam legislation. The *Cisco 2008 Annual Security Report* estimated that messages sent from Canada accounted for 4.7% of the world's spam. That percentage landed Canada in fourth place on the list of countries with the most originating spam, behind only the U.S., Turkey and Russia. The government has characterized Bill C-27 as a necessary step in fulfilling an international duty to join global partners in passing laws to combat spam and related cyber-threats.

Having passed both First Reading and Second Reading in the House of Commons, Bill C-27 has been referred to the Standing Committee on Industry, Science and Technology for review. While almost everyone can agree that spam is a nuisance, concerns have been raised about the proposed legislation, as drafted. Thus, while initial predictions were that Standing Committee review would be completed before Parliament's summer recess, more recent estimates see the review continuing after Parliament returns in the fall, in order to ensure that the resulting legislative changes do not negatively affect legitimate business.

Main prohibitions

The anti-spam provisions would prohibit sending (or causing or permitting to be sent) a commercial "electronic message" (which is defined broadly to include a text, sound, voice or image message) to an electronic address, unless the recipient has given express or implied consent. As currently drafted, implied consent would be limited to situations in which there is an existing business or non-business relationship between the sender and recipient (although there is a provision that would permit future regulations to better define implied consent.) Both "existing business relationship" and

This newsletter was prepared by members of the Intellectual Property Group at Stikeman Elliott.

EDITOR: JUSTINE WHITEHEAD
jwhitehead@stikeman.com

“existing non-business relationship” are defined fairly narrowly, and would be restricted to situations in which the relevant parties had participated in a relevant transaction in the last eighteen months. Another aspect of the ECPA that appears to pose some practical difficulties is that it would prohibit the sending by email of any request for express consent to communications by email.

The ECPA also dictates some aspects of the form of permitted messages: the message must identify the person who sent the message (and, if it is different, the identity of the person on whose behalf the message was sent), along with contact information for those identified. Moreover, permitted messages must include an unsubscribe mechanism, which includes either a hyperlink (valid for at least 60 days after the message is sent) that the recipient can follow or a specified electronic address to which the unsubscribe indication can be sent. Unsubscribe requests must be given effect within 10 days.

The ECPA includes provisions directed to privacy and personal security concerns that are associated with counterfeit websites. Section 7 of the proposed ECPA would prohibit a person, in the course of a commercial activity, from altering or causing to be altered the transmission data in an electronic message “so that the message is delivered to a destination other than, or in addition to, that specified by the sender.” This provision appears to be directed at one aspect of “phishing”. Phishing, which is often undertaken in conjunction with a spoofed email, is the act of sending an email falsely claiming to be a legitimate business and directing the recipient to a specified counterfeit website, in an attempt to obtain sensitive information such as passwords, credit card numbers, and bank account information.

Section 8 of the proposed ECPA would prohibit a person, in the course of a commercial activity, from installing a computer program on another person’s computer system without express consent. After a presumably authorized installation, it would also prohibit a person, in the course of a commercial activity, from causing an electronic message to be sent from that computer system, without express consent. The government’s stated intent for the legislation is to prevent the collection of personal information through illicit access to computer systems (spyware), but as currently drafted, these provisions apply to all computer programs, and not just those with a harmful effect.

Requests for express consent must clearly and simply set out the purpose for which the consent is being sought, and identify the entity seeking consent. Moreover, consent in respect of the installation of a computer program must clearly and simply describe the function, purpose and impact of every computer program that would be installed if consent is given. There is some disagreement between the federal government and industry as to whether the drafting of the latter requirement could be considered to prevent current commercial practices that see some legitimate programs (such as anti-virus and anti-spyware programs) utilizing automatic updates to the software.

Administrative monetary penalties

The ECPA would subject any individual who violates any of the foregoing prohibitions to liability under an administrative monetary penalty (“AMP”) of up to \$1 million and corporate entities would be liable to an AMP of up to \$10 million. Officers, directors, agents of a corporation that violates the prohibitions could also be held liable for such actions if they directed, authorized or participated in the commission of the violation. At the same time, a defence of exercising due diligence to prevent the violation is available, although there is no indication of the types of action that would constitute due diligence.

The process for imposing liability under the AMP is a fairly expedited administrative process. A notice of violation (which must include details of the alleged violation and the amount of the AMP) will be issued and served upon an offender if the CRTC believes that there are reasonable grounds on which to believe that a person has committed a violation under the ECPA. The person served with the notice of violation then has 30 days to make representations to the CRTC regarding the allegations or the amount of AMP, failing which that person will be deemed to have committed the violation. If representations are made, the CRTC will evaluate them on the civil balance of probabilities standard, and may then impose the penalty set out in the notice of violation or reduce or waive the penalty. Appeal of decisions of the CRTC in respect of notices of violation can be made to the Federal Court of Appeal. The CRTC can also agree to an undertaking, which is in essence an agreement to settle an alleged violation on terms acceptable to both the CRTC and the offender.

Private right of action

One of the most controversial provisions of the ECPA is that it would establish a private right of action for persons who allege that they have been affected by a contravention of the anti-spam, anti-phishing and anti-spyware provisions of the ECPA. Such persons may apply for an order for compensation for actual loss or damages suffered or expenses incurred, as well as a maximum of \$200 for each contravention of the breached provisions (with a limit of \$1 million for each day on which a contravention occurred). Again, officers, directors or agents of corporations would be subject to this private right of action, if it could be proved that they directed, authorized or participated in the commission of the contravention.

That same private right of action would apply to persons who allege that they have been affected by breaches of the new provisions of PIPEDA and the *Competition Act* that would be brought into effect by Bill C-27 (discussed in the next section).

Changes to PIPEDA, the Competition Act and the Telecommunications Act

Bill C-27 would establish new prohibitions under PIPEDA in relation to collecting personal information, including a ban on (i) collecting an individual's electronic address through a computer program designed or marketed for use in generating (or searching for) and collecting electronic addresses, or using any address collected by the foregoing means; and (ii) collecting personal information through any means of telecommunications if the collection involves accessing a computer system (or causing one to be accessed) without authorization, or using any personal information that is collected that way.

Bill C-27 also proposes numerous amendments to the *Competition Act*, including the addition a new section 52.01, which broadens the criminal "false or misleading representation" provisions of the *Competition Act* by prohibiting activities such as knowingly or recklessly sending, for business promotion purposes (i) a false or misleading representation in the sender or subject matter information of an electronic message or (ii) an electronic message that contains a materially false or misleading representation. Under the proposed new section 74.011 of the *Competition Act*, such actions would also qualify as reviewable conduct, thus permitting the Commissioner of Competition to apply to court or the Competition Tribunal for an order prohibiting the conduct and/or imposing AMPs under the *Competition Act*.

Bill C-27 would also amend the *Telecommunications Act* to permit the government to either maintain the current "Do Not Call" list in such a way that it would not overlap with the ECPA regime, or to have the responsibility for regulating telemarketing fall under the ECPA entirely.

Other anti-spam bills

Bill C-27 is not the only bill with anti-spam implications currently moving through Parliament. Bill C-355, a private member's bill which aims to amend the Criminal Code to make cyberbullying an offence, proposes as part of that effort to make it an offence to make repeated telephone calls or to send repeated electronic messages to any person with intent to harass.

Bill S-220 also purports to be anti-spam legislation, introducing an offence for sending an unauthorized commercial electronic message, as well as a right of civil action for those adversely affected. Unlike Bill C-27, however, it does not propose to amend other statutes. Having been introduced in the Senate, Bill S-220 would also need to pass through the House of Commons before it could be enacted, which seems unlikely given the status of Bill C-27.

For further information, please contact your Stikeman Elliott representative, the editor, Justine Whitehead (jwhitehead@stikeman.com), or any member of our Intellectual Property Group listed on the following page.

**Stikeman Elliott's
Intellectual Property Group:**

OTTAWA

Stuart C. McCormack
smccormack@stikeman.com
Kim D.G. Alexander-Cook
kalexandercook@stikeman.com
Nicole Brousseau
nbrousseau@stikeman.com
D. Jeffrey Brown
jebrown@stikeman.com
Craig Collins-Williams
ccollinswilliams@stikeman.com
Eugene F. Derényi
ederenyi@stikeman.com
Randall Hofley
rhofley@stikeman.com
Nicholas McHaffie
nmchaffie@stikeman.com
Ryan Sheahan
rsheahan@stikeman.com
Alexandra Stockwell
astockwell@stikeman.com
Vivien Tzau
vtzau@stikeman.com
Justine M. Whitehead
jwhitehead@stikeman.com

TORONTO

Kathryn I. Chalmers
kchalmers@stikeman.com
Martin Langlois
mlanglois@stikeman.com

MONTREAL

Jonathan Auerbach
jauerbach@stikeman.com
Bruno Barrette
bbarrette@stikeman.com
Marc-André Coulombe
macoulombe@stikeman.com
Mortimer Freiheit
mfreiheit@stikeman.com
Benoît Huart
bhuart@stikeman.com
Caroline Plante
cplante@stikeman.com

CALGARY

Nick J. Kangles
nkangles@stikeman.com

www.stikeman.com

STIKEMAN ELLIOTT

To subscribe or unsubscribe to this publication, please contact us at info@stikeman.com

This publication provides general commentary only and is not intended as legal advice. © Stikeman Elliott LLP