CAOB
CAROL ANNE O'BRIEN
BARRISTER & SOLICITOR

OFFICE 416·640·7270 MOBILE 416·399·6270 EMAIL caob@caobrienlaw.com FAX 416·368·5655 WEB caobrienlaw.com
151 Yonge Street, Suite 1500 Toronto, ON M5C 2W7

April 2011

(Published in the newsletter of the Ontario Bar Association, Information Technology and E-Commerce Section)

Prepare Now, to Comply with Federal Anti-Spam Legislation

Federal anti-spam legislation received royal assent on December 15, 2010 and is expected to come into force within the next few months, upon proclamation. The legislation prohibits a very broad class of commercial electronic communications, unless the recipient consents to receive it or an exception is available. As such, it will affect virtually all businesses that use any form of electronic communication, and will have a broad impact throughout the economy. Sending unsolicited commercial electronic messages without the recipient's consent can be penalized by administrative monetary penalties ("AMPs") of up to $1 million for an individual, and up to $10 million for corporations and others. As such, it is crucial that in-house and external counsel work with their clients to begin to do the analysis of operations necessary to prepare for compliance. In this article, the legislation[1] is referred by its former short title, the *Fighting Internet and Wireless Spam Act* ("FISA"). FISA was introduced as Bill C-28 on May 25, 2010. It is an updated version of the *Electronic Commerce Protection Act* ("ECPA"), Bill C-27, which died on the Order Paper with the prorogation of Parliament in December, 2009.

Prohibitions and "Commercial Electronic Messages"

The central prohibition of FISA is contained in s. 6, which states:

---

[1] The full title is: "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 Radio-television and Telecommunications Commission Act,* the *Competition Act,* the *Personal Information Protection and Electronic Documents Act* and the *Telecommunications Act*". Unusually, the short title provision was removed during Committee debate. Industry Canada currently refers to "Canada's Anti-Spam Legislation." See the Backgrounder http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00572.html and the Q&A document: http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00569.html. **[Update**: See also the Industry Canada web site, launched in August, 2011 at: http://www.ic.gc.ca/eic/site/030.nsf/eng/home.]

> "It is prohibited to send or cause or permit to be sent to an electronic address a commercial electronic message unless (a) the person to whom the message is sent has consented to receiving it, whether the consent is express or implied; and (b) the message complies with subsection (2)."

FISA also prohibits altering "transmission data" (s. 7) and installing a computer program on another person's computer without the express consent of the owner or an authorized user (s. 8), and provides that to "aid, induce, procure or cause to be procured the doing of any act contrary to any of [the foregoing]" is also a contravention.

This article focuses on compliance with the s. 6 prohibition against sending unsolicited commercial electronic messages. To ensure compliance, the starting point for businesses will be to review all procedures and forms relating to e-mail correspondence, including company newsletters and advertising materials, prior to FISA coming into force.

"Commercial Electronic Messages"

As the first step of analysis to prepare for compliance, one must refer to FISA's definitions. Under FISA, "Commercial activity" is defined more broadly than in the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). In FISA, there is an explicit statement that an activity can be commercial even in the absence of an expectation of profit:[2]

> "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, whether or not the person who carries it out does so in the expectation of profit, other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada".

"Electronic message" is also defined very broadly, as "a message sent by any means of telecommunication, including a text, sound, voice or image message"[3] such that it would

---

[2] The definition also differs by incorporating an exception relating to law enforcement and other government activities.

[3] At sections 89 – 90, FISA contains amendments to the *Telecommunications Act* that would result in the replacement of its current National Do No Call List provisions by FISA's broader prohibitions. However it is expected that these provisions will not be brought into force at the same time as the rest of FISA, but phased in at a later date. [**Update:** Industry Canada (in August 2011) indicates that FISA is expected to be brought into force in early 2012.]

apply not only to e-mail and text messages, but also to unsolicited voice mail messages left by telemarketers. A "commercial electronic message" is further defined in s. 1(2) as:

> "an electronic message that, having regard to the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message, it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity, including an electronic message that (a) offers to purchase, sell, barter or lease a product, goods, a service, land or an interest or right in land; (b) offers to provide a business, investment or gaming opportunity; (c) advertises or promotes anything referred to in (a) or (b); or promotes a person, including the public image of a person, as being a person who does anything referred to in any of paragraphs (a) to (c), or who intends to do so."

Having identified the categories of "commercial electronic messages" it generates, an organization must then move on to the second stage of analysis, to consider whether one or more exceptions will apply such that the recipient's consent is not required, or whether the situation is one in which the recipient's consent may be implied.

Exceptions and Implied Consent

As a business reviews its procedures with respect to consents, it is important to note that s. 13 provides that anyone relying on either express or implied consent has the burden of proving it in court, or before the regulator. As such, it will be important to create and maintain appropriate paper or electronic records as evidence of an exception under FISA, or the recipient's implied or express consent.

Section 6(5) contains a number of exceptions to the requirement for consent, such that the consent of the recipient is not required to send the commercial electronic message. Specifically, ss. 6(5)(a), (b) and (c) create exceptions for commercial electronic messages that are sent to: an individual in a "personal or family relationship, as defined in the regulations" [4]; a "person who is engaged in a commercial activity and consists solely of an inquiry or application related to that activity;" or "that is of a class, or is sent in circumstances, specified in the regulations". Furthermore, s. 6(6) provides an exception from the requirement to obtain consent (but not the requirements of s. 6(1)(b) and (2) with respect to form and content) for a long list of categories of commercial electronic

[4] This is one of a number of provisions in which specific requirements for compliance remain to be determined in FISA's Regulations. **[Update**: Two sets of draft Regulations have now been issued for comment, by the CRTC on June 30, 2011 and by Industry Canada on July 9, 2011.]

messages, which include (a) a quote or estimate that was requested by the recipient; (b) a message that facilitates, completes or confirms a commercial transaction that has previously been entered into; and (c) a warranty, product recall, or safety or security information. Additional categories in this provision include (at s. 6(g)) those that communicate "for a purpose specified in the regulations".

Two important areas for analysis for compliance will involve circumstances where consent to receive commercial electronic messages can be implied, where there is either an "an existing business relationship or an existing non-business relationship", as provided for in s. 10(9)(a). The definition of an "existing business relationship," in s. 10(10) provides that a business relationship between the person sending or causing the message to be sent and the recipient, sufficient for an implied consent, can arise from:

> (a) the purchase or lease of a product, goods, a service, land or an interest in land, within the prior two years,
> (b) the acceptance by the recipient of a business, investment or gaming opportunity, within the prior two years;
> (c) bartering anything mentioned in (a);
> (d) a written contract, in respect of a matter not referred to in (a) to (c), if the contract is currently in existence or expired within the prior two years; or
> (e) an inquiry or application made by the recipient, in respect of anything mentioned in (a) to (c), within the prior six months.

When a business is sold, s. 10(12) provides that the purchaser is considered to have the same "existing business relationships" as its predecessor.

Through the definition of an "existing non-business relationship" in s. 10(13)(a) and (b), consent can also be implied where the recipient has, within the prior two years, made a donation or gift to, or volunteered with, the sender of the message, which is a registered charity, a political party, or a political candidate. Clubs, associations and voluntary organizations, benefit from s. 10(13)(c).

Consent may also be implied in certain circumstances involving business listings and business cards. Specifically, s. 10(9)(b) and (c), provide for implied consent where a recipient has either conspicuously published or disclosed (to the person who sends the message, the person who causes it to be sent or the person who permits it to be sent) his

or her e-mail contact information and, at the same time, has not posted a disclaimer that the e-mail may address not be used for unsolicited electronic commercial messages. Where consent is implied in these circumstances, it applies only to messages that are "relevant to the person's business role, functions or duties in a business or official capacity."

Consents to Receive Commercial Electronic Messages

Where no exception exists and where consent cannot be implied, it will be necessary for the business to ensure that its procedures include mechanisms to solicit each recipient's express consent, before any commercial electronic messages are sent. When express consent is required, s. 10(1) provides that the sender must "clearly and simply" set out: (a) the purpose or purposes for which the consent is being sought; (b) prescribed information that identifies the person seeking consent and, if the person is seeking consent on behalf of another person, prescribed information that identifies the other person; and (c) any other prescribed information."

Mandatory Contents of Commercial Electronic Messages

Even where the sender can rely on an implied consent, s. 6(1)(b) and s. 6(2) specify that commercial electronic messages must set out prescribed information, identifying the sender and if different, the person on whose behalf it is sent. In addition, each message must provide information enabling recipients to readily contact either of those persons, and include an unsubscribe mechanism. As provided for by s. 11(1), the unsubscribe mechanism must enable the person to whom the commercial electronic message is sent "to indicate, at no cost to them, the wish to no longer receive any commercial electronic messages, or any specified class of such messages, from the person who sent the message or the person – if different – on whose behalf the message is sent." This may be done using the same electronic means by which the original message was sent, or if this is not practicable, by any other electronic means that will enable the person to indicate the wish. In addition, the unsubscribe mechanism must specify an electronic address or link to a web page, to which the indication may be sent, and this address or web page must be valid for a minimum of 60 days after the message is sent.

Conclusion

To avoid the risk of significant AMPs, it is important for organizations to begin the process of reviewing and adapting their procedures relating to commercial electronic messages. Because of FISA's particular requirements, this process could be time-intensive, and so starting sooner rather than later is advisable.

Please address any questions about the new federal anti-spam legislation to Carol Anne O'Brien at caob@caobrienlaw.com, or (416) 640-7270.

Carol Anne O'Brien's law practice is focused on regulatory matters including communications law (broadcasting and telecommunications), competition law, advertising and marketing, Internet domain names and privacy.