February 9, 2011

Canada Takes on Spam, Spam, Spam, Spam, Spam[1]
Fighting Internet and Wireless Spam Act

The Federal government's legislation to control spam and other ills of the electronic age with the oh-so-catchy title of *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,* was passed in mid-December, 2010. This newly passed legislation was Bill C-28, otherwise known as the Fighting Internet and Wireless Spam Act, or "FISA" for short. It is generally expected to be proclaimed in force within 7-8 months. The delayed timing is intended to allow companies to accommodate the requirements of FISA into their operations and prepare for compliance. But there is no indication yet whether FISA will be proclaimed in force in full or in part.

The stated purpose of FISA is:

To promote the efficiency and adaptability of the Canadian economy by regulating commercial conduct that discourages the use of electronic means to carry out commercial activities, because that conduct (a) impairs the availability, reliability, efficiency and optimal use of electronic means to carry out commercial activities; (b) imposes additional costs on businesses and consumers; (c) compromises privacy and the security of confidential information; and (d) undermines the confidence of Canadians in the use of electronic means of communication to carry out their commercial activities in Canada and abroad. .

FISA introduces its own set of requirements with respect to electronic communications, and it empowers the Canadian Radio-television and Telecommunications Commission (the CRTC) to enforce the provisions in the act, including the imposition of significant monetary penalties. It also makes specific amendments to each of the *Competition Act* and *Personal Information Protection and Electronic Documents Act* and then requires each of the CRTC, the Commissioner of Competition and the Privacy Commissioner, to 'consult with each other to the extent that they consider appropriate' to ensure the effective regulation of FISA, the *Competition Act,* the *Personal Information Protection and Electronic Documents Act,* the *Electronic Documents Act* and the *Telecommunications Act*.

FISA is designed to stop (i) spam; (ii) hacking and phishing; and (iii) malware and spyware. It is a blunt instrument, though, and the penalties are extensive. Depending upon the evil prohibited by FISA, there are various routes to enforcement. If a company sends a message that is either

[1] With reverential acknowledgement to Monty Python's famous 1970 skit.

misleading or deceptive, the Competition Bureau will engage. If it is a question of spam, spyware or message misrouting – the CRTC is the place to go. If there is an improper 'harvesting' of personal information – the Privacy Commissioner takes over. And overlaying all of this is the right of private action.

Spam:

If you conduct an online business in Canada, or one that is targeted to Canadians, or if you communicate with customers via various electronic means, then you will need to comply with FISA requirements. FISA applies to any *commercial activity*, which is defined as any transaction, act or conduct or any regular course of conduct that is of a commercial character, whether or not the person carrying it out does so with an expectation of profit. Spam is a commercial electronic message sent to an electronic mail account, specifically including email, instant messaging and texting but also, because the definition is open-ended, capturing messages communicated through social media portals, message boards or similar media. Unless the recipient has consented, and the message contains certain prescribed information identifying the sender and how to unsubscribe, a sender is prohibited from sending the message. While there are some limited exceptions, essentially it is an 'opt in' system, where permission must first be given by the recipient, rather than an 'opt-out' system where the sender can send the message, as long as they honour the opt out requests of recipients.

There are exceptions to messages being defined as "commercial messages" for the purposes of FISA, which are if it: (i) is a message sent between individuals with a personal relationship (family); (ii) is sent to a person engaged in a commercial activity and consists solely of an inquiry or application related to that activity; (iii) solely provides a quote or estimate requested by the recipient; (iv) provides product recall, warranty or safety/security information about a product/service already purchased; (iv) provides notice of factual information concerning an ongoing subscription, membership, account or loan; (v) provides information concerning a recipient's employment relationship or benefit plan; or (vi) delivers a product, good or service, including upgrades or updates further to a previous transaction with a sender.

There are also certain matters that lead to a conclusion of implied consent to unsolicited messages: (i) if there is an existing business relationship between sender and recipient; (ii) if the recipient has 'conspicuously published' their email contact information; (iii) if the recipient has disclosed their e-mail contact information to the sender without indicating that they do not wish to receive communications; (iv) or other circumstances that may be set out in regulations. At present, no regulations have been introduced. An existing business relationship includes any commercial transaction, business or investment relationship between the parties in the past 2 years; an inquiry from the recipient in the past 6 months, or written consent of the recipient still in effect (or expired within the previous 2 years. For the purposes of non-profits – an existing relationship includes a donation of time or money by the recipient for a registered charity, political party, organization or

candidate or which arises because of membership by the recipient in a club, association or voluntary organization.

Messages sent to a recipient who has given express consent is also permitted, but, query how you get the consent, when the first email without such prior express consent (unless it just so happens to fall into one of the implied consent categories, or perhaps during the transitional period exceptions) would in and of itself constitute a breach of the spam provisions.

Messages have to meet certain prescribed formalities, both as to the 're-line', content, and as to the method for allowing a recipient to unsubscribe. For organizations that communicate in a number of different formats (e.g. posting messages on LinkedIn™, Facebook™ postings, email messages), policies will have to be developed to ensure compliance with each method. Although there is a transitional period following enactment of FISA, businesses that communicate via email with their customers and potential customers will have to devise methods of obtaining consent or otherwise cull their own email lists, and they will have to ensure that communications meet the prescribed requirements.

In addition to the above, amendments to the *Competition Act* provide that electronic messages sent with false or misleading representations, and whether such false or misleading representations are in the subject line or the body of the text (or in a locator) is prohibited. The *Competition Act's* existing provisions on misleading advertising is otherwise applicable, and the Competition Bureau's penalties for misleading advertising generally will apply, including the potential for substantial fines. *PIPEDA* is amended to prohibit the unauthorized collection or use of a person's email address or personal information if it was collected through a computer program designed for collecting addresses, or, in the case of personal information, which was an illegal manner.

Spyware and Malware

FISA prohibits the installation, without consent of a recipient, of any computer program on such recipient's computer system. Further, if a computer program is installed, it is a prohibited act to cause the program to send an electronic message. There are no implied consents and only express consents are valid. So a clickwrap agreement will work but express consent must meet prescribed requirements, that include a clear description of the purpose for which the consent is sought and that identifies the party seeking the consent. If installed, the party installing the program must provide an email address for the recipient to send a message for removal or disabling of the installed program if the recipient believes that the program does not meet the function or purpose described in the request for consent, or that the impact of installation was not properly described.

For the purposes of FISA, express consent is deemed for cookies, HTML code, Java Script, operating systems and for computer programs that can only be executed through the use of a different program for which consent has been obtained previously.

Hacking and Phishing

Unless a sender or the person to whom a message is sent provides express consent, or an alteration is made by court order, any alteration of 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 is prohibited. Seeking consent requires disclosure of prescribed information including the purpose for which the consent is sought, the identification of the person seeking consent and other information that may be required.

What Happens if you Run Afoul?

The CRTC is empowered to designate persons to enforce FISA, including issuing demands for production and preservation of documents and to seek injunctive relief or issue 'notices of violation' which can include the imposition of an administrative monetary penalty. The maximum penalty is $1 million for an individual contravening FISA and $10 million for a corporation or other similar entity.

A 'violation' is not an offence under the *Criminal Code* but failure to abide by a notice of violation, or misleading a designated person and other similar matters is an offence, punishable on summary conviction and a fine of $10,000 for a first offence, or $25,000 for subsequent offences in the case of an individual, and $100,000 first offence, $250,000 subsequent offences in the case of a corporation or other similar entity. As well, an employer can be held liable for a violation by an employee, and directors and officers can be held liable for a violation by their corporation, unless that person can establish that they exercised due diligence to prevent a violation.

In addition, FISA, the *Competition Act* and *PIPEDA* all provide for a private right of action. A person (whether individual or corporation) that has been affected by a violation may seek a court order for compensation for their loss. On application, the court may order compensation of $200 per contravention, up to a maximum penalty of $1 million per day.

What Next?

The months ahead prior to the proclamation in force of FISA provide an opportunity for organizations to prepare and introduce to employees FISA compliance policies, to review and cull email lists, to provide for a methodology for obtaining consents, and ensuring that messages have templates to address the prescribed requirements such as unsubscribe functions.

For more information, contact **Valerie C. Mann** at 604.631.9173 or vcmann@lawsonlundell.com.