FMC LAW

Focus on
Communications

JANUARY 2011

Canada's New Anti-Spam Legislation: Overview and Implications for Businesses

By Margot Patterson

A. Overview and Implications

The *Fighting Internet and Wireless Spam Act* ("*FISA*" or the "*Act*") received Royal Assent in December 2010, and will enter into force in the fall of 2011. A part of Canada's Strategy for the Digital Economy, *FISA* is intended to promote e-commerce by deterring spam, identity theft, phishing, spyware, viruses, and botnets (all defined below)[1], as well as misleading commercial representations online. *FISA* creates new offences, enforcement mechanisms and penalties to address these online threats. Canada is the last of the G-8 countries to introduce an over-arching legislative framework to address spam, which continues to represent approximately 80% of all global e-mail traffic.

FISA will affect how companies do business online in Canada. Proactive businesses can use the lead

---

[1] The following definitions are drawn from the Library of Parliament's Legislative Summary of Bill C-28, available online: Click here

- **Identity theft** is the collection and use of stolen personal information to impersonate someone, generally for financial fraud purposes.
- **Phishing is the impersonation of a trusted person or organization in order to steal a person's personal information, usually for the purposes of identity theft.**
- **Spyware is software that collects information about a user, or modifies the operation of the user's computer, without the user's knowledge or consent.**
- **A virus is hostile software (or "malware") that spreads by attaching itself to another resource on a computer such as e-mail.**
- **A botnet is a collection of "zombie" computers used to send spam or for another purpose. A "zombie" is a computer that runs malware so that the computer can be remotely controlled by the creator, distributor or controller of the malware.**

time prior to *FISA*'s entry into force as a transition period to prepare for compliance. For example:

- All organizations that send commercial email to clients or prospects will need to review their online marketing practices, to ensure they comply with new consent, disclosure, and "unsubscribe" requirements.
- Similarly, companies that distribute software and updates/upgrades to their customers will need to review their installation practices and software agreements to meet the new requirements.
- Advertisers and marketers will need to familiarize themselves with how the existing misleading and deceptive representations laws will apply online.

Recommended next steps for businesses are set out at the end of this article.

B. A Multi-Faceted Regulatory Regime: Communications, Competition and Privacy

FISA amends four *Acts* that regulate telecommunications, competition, and privacy: the *Canadian Radio-television and Telecommunications Commission Act*, the *Telecommunications Act*, the *Competition Act*, and the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"). The CRTC, the Competition Bureau, and the Office of the Privacy Commissioner will have expanded mandates to administer the new regulatory regime.

C. Application

FISA applies to "commercial activity" defined as "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**". The bolded language could potentially catch some third parties involved in commercial activities; it is unique to *FISA* and does not, for example, exist in *PIPEDA*. "Electronic message" and "electronic address" apply broadly to any means of telecommunication, including text, sound, voice, or image, via e-mail, instant messaging, telephone or "any similar account", which could include Facebook and Twitter postings. Broadcasting is expressly excluded.

D. Prohibitions

With some specific exceptions, *FISA* is based primarily on an "opt-in" approach, with express, permission-only consent. Anyone who alleges that they have consent to engage in an otherwise prohibited act has the onus of proving it.

1) Unsolicited Electronic Messages (Spam)

a) Overview

FISA (section 6) prohibits sending any commercial electronic message unless it is: (i) sent with the recipient's express or implied consent; and (ii) in a prescribed form. It must identify the person who sent the message, and (if different) the person on whose behalf it is sent, and provide accurate contact information for these persons. It must also provide a *FISA*-compliant unsubscribe mechanism.

Various exceptions apply to a commercial electronic message that:

- is sent between individuals with a **personal or family relationship**
- is sent to a person who is engaged in a commercial activity, and consists solely of an **inquiry or application** related to that activity
- solely provides a **quote or estimate** requested by the recipient
- facilitates, completes or confirms a **pre-existing commercial transaction**
- provides **warranty, product recall, or safety/security information** about a product, goods or a service already used or purchased
- provides notice of **factual information** concerning an ongoing **subscription, membership, account or loan** with the sender (or about that relationship itself)

- provides ongoing information about the recipient's **employment relationship or benefit plan**
- **delivers a product, good or service**, including updates/upgrades, further to a previous transaction with the sender

Notably, the prohibition does not apply to a telecommunications service provider merely because the provider provides a service that enables the transmission of the message. In subsection 6(8), *FISA* also exempts telemarketing, which is currently covered by the Do Not Call List ("DNCL") administered by the CRTC under the *Telecommunications Act*. However, section 68 of *FISA* provides for the repeal of subsection 6(8), and the DNCL itself. At some point in the future, for example, when VOIP and other technologies blur the distinction between "calls" and "commercial electronic messages", the government may make *FISA* apply directly to telemarketing activities. Telemarketers should take note, as the *FISA* consent standards are higher than those for the DNCL and those of the *U.S. CAN-SPAM Act*, both of which take an overall "opt-out" approach.

A person contravenes the spam prohibition only if the computer system used to send or receive the message is located in Canada.

b) Consent

FISA does contain specific exceptions to the express, "opt-in" consent model. Consent is **implied** for unsolicited communications if there is an "existing business (or non-business) relationship" between the sender and recipient; if the recipient has "conspicuously published" their e-mail contact information; if the recipient has disclosed their e-mail contact information to the sender without indicating that they do not wish to receive communications; or in circumstances set out in regulations (to be established).

An existing business relationship includes:

- a commercial transaction with the recipient within the previous two years
- a business, investment or gaming opportunity with the recipient within the previous two years
- any kind of inquiry from the recipient in the previous 6 months on the above two points
- a written contract with the recipient, still in effect or expired within the previous two years

The purchaser of a business inherits the above business relationships from the vendor.

An existing non-business relationship includes, during the previous two years:

- a donation or gift, or volunteer work, by the recipient for a registered charity, political party, organization or candidate or
- membership by the recipient in a club, association or voluntary organization.

The unsubscribe requirements for spam include enabling the recipient to withdraw consent to receive communications: at no cost to them, using the same means of communications (e.g. reply email) or another effective means, to a contact for the sender that is accessible for at least 60 days.

2) **Intercepting and Re-directing Communications (Hacking and Phishing)**

a) Overview

FISA (section 7) prohibits altering the transmission data in an electronic message so that the message is sent or copied to a destination other than the one intended by the sender. Any alterations must be made with the express consent of the sender or the recipient, as set out in the *Act*, or in accordance with a court order. Telecommunications service providers are exempt from the prohibition for alterations made for network management purposes. A person contravenes the prohibition only if a computer system used to send, route or access the message is located in Canada.

b) Overview

Anyone altering transmission data with express consent must provide the recipient with an address to send notice to withdraw consent, which must be carried out by the sender within 10 business days.

3) Installing Computer Programs Without Consent (Malware and Spyware)

a) Overview

FISA (section 8) prohibits installing or causing to be installed a computer program on anyone else's computer system, or cause an electronic message to be sent from that system, without obtaining the express consent of that person pursuant to the *Act*, or a court order. The prohibition applies only where the computer system, the person installing the program or sending the message, **or** the person directing this activity, is located in Canada.

b) Consent

The requirements for obtaining express consent are outlined in detail in the *Act*, and include information on the function of the program and in certain specific circumstances, a description of the material operating elements and their foreseeable impact on the system. Some exceptions to the express consent provisions apply in respect of updates and upgrades. In addition, express consent is deemed if the program is a cookie, HTML code, Java Script, operating system, a program that can be executed only through the use of another program for which consent has been given previously, or any other program specified in the regulations, **and** it is reasonable to believe that the recipient consents.

E. Enforcement of *FISA* and Penalties

The CRTC is the primary regulatory agency to enforce and pursue administrative monetary penalties ("AMPs") for *FISA* violations. The maximum penalty for an individual is $1 million, and for an organization, $10 million, per violation. The factors to determine the penalty include the purpose of the penalty, the nature and scope of the violation, any history of violations, the financial benefit obtained from the violation, and ability to pay.

Violations of *FISA* are not criminal offences, however, they can give rise to vicarious liability. Directors and officers can be held liable for a violation by their corporation (piercing the corporate veil), and an employer can be held liable for a violation by an employee. A person cannot be found liable if they can establish that they exercised due diligence to prevent the violation – which is a key reason for corporations and employers to develop a *FISA* Compliance Policy.

FISA also creates a private right of action for an individual or corporation that has been affected by a contravention, to obtain a court order for compensation. Private actions may be brought, for example, for an act or omission that breaches the prohibitions on spamming, hacking, and malware and spyware (under *FISA*); for false or misleading electronic messages (under the *Competition Act*), or certain forms of unauthorized online collection of personal information (under *PIPEDA*). Remedies include

compensation for loss or damage suffered or expenses incurred, and a maximum penalty of: $200 per contravention, or $1 million per day for the spam prohibition; and $1 million per day for the hacking, malware and spyware prohibitions.

F. Amendments to the Competition Act, PIPEDA, and the Telecommunications Act

The *Competition Act* is amended through *FISA* to mandate the Competition Bureau and the Commissioner to investigate and enforce the online communications prohibitions. For example, the *Competition Act*'s existing misleading and deceptive representations provisions would extend to on-line activity, including knowingly or recklessly sending an electronic message that is false or misleading in a material respect, in respect of either the sender, the subject line, the message itself, or the locator (e.g. the URL). Proof of that the recipient was deceived is not required to establish this new offence. In addition, the definition of "telemarketing" is expanded to cover promotion "by any means of telecommunication" to update and broaden the regime under the *Competition Act*.

PIPEDA is amended to introduce new measures against unauthorized collection of personal information by hacking or unauthorized trading of electronic address lists. New definitions are added to co-ordinate with *FISA*, including "computer program", "computer system" and "electronic address". *FISA* specifies that most of the *PIPEDA* exceptions that currently permit the collection and use of personal information without consent (e.g. journalistic purposes, life-threatening emergency) are *not* available where an individual's electronic address was obtained via data mining or other automated crawling, or if personal information was illegally accessed by a computer system.

The *Telecommunications Act* would be amended to permit the CRTC to disclose information that is designated as confidential, when it is carrying out its mandate under *FISA*. As mentioned in the section on spam earlier in this note, *FISA* puts in place a framework to replace the current Do Not Call List with a new regime at a later date. This is intended to reflect both technological neutrality (VOIP is overtaking wire-line communications) and a perceived need for more effective tools to combat spam (the consent standard for telemarketing will be raised when the new regime is activated).

G. Three-Year Transition

For three years after the date the anti-spam provisions come into force, there will be implied consent for commercial electronic messages **where there is an existing business or non-business relationship with the recipient.** The same applies for the installation of computer program updates or upgrades. In all cases, the recipient can still withdraw consent at any time. Businesses must obtain express consent during the three-year transition period, to continue afterwards.

H. Next Steps for *FISA*

Regulations to be enacted under *FISA* will add more detailed requirements, and are expected to be issued for public comment in February or March of 2011. The Act and regulations are anticipated to come into force in the fall of 2011.

I. Next Steps for Businesses

1) Conduct an **audit** of online communications with clients, prospects, and third parties, including:
    - bulk email, automated messages, periodic client newsletters and updates
    - (for software developers) processes for installation of software updates/upgrades
2) Develop a **FISA checklist**, including:
    - consent, unsubscribe, and disclosure requirements and available exceptions
3) Develop a **FISA Compliance Policy** that:

- addresses applicable legal provisions (*FISA* and regulations, *Competition Act, PIPEDA, Telecommunications Act*)
- meets the prescribed requirements for the organization's forms and procedures that document consent
- covers the unsubscribe requirements and timeframes
- confirms or updates email address and personal information collection practices, and the organization's Privacy Policy and Website Terms of Use
- provides required information for software update/upgrade installation (where applicable);
- updates existing customer service processes
- includes information or training for employees, management and Board of Directors

Contact Us

For further information, please contact a member of our National Communications Group.