BULLETIN
Technology and Intellectual Property

FASKEN MARTINEAU
www.fasken.com

January 28, 2011

FISA: Legal Obligations and Business Strategies

By: Constantinos Ragas | Montréal

The *Fighting Internet and Wireless Spam Act* ("**FISA**") was passed into law by the federal government on December 15, 2010. The law comes into force later this year, and is the product of several years' worth of research into spam-combating best practices from across the globe.

The main purpose of the 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."

In general terms, FISA is aimed at fighting (i) unsolicited electronic commercial messages (ie. spam); (ii) software that transmits information about a person, or a person's online activities, without his or her consent; (iii) altering the transmission of electronic communications; and in a more general sense, (iv) identity-theft.

This bulletin reviews the principal legal obligations under FISA and highlights business strategies for compliance with the law[1].

Principal Legal Obligations

Unsolicited Electronic Messages

Generally speaking, the FISA prohibits the sending of a commercial electronic message (a "**CEM**") to an "electronic address" (which includes email, instant messaging and telephone accounts) unless the recipient has given his or her express or implied[2] consent. In addition, a CEM must include: (i) prescribed information which identifies the sender and, if different, the person on whose behalf the message was sent (the "originator"); (ii) information enabling the recipient to contact either the sender or originator of the message; and (iii) an unsubscribe mechanism.

The contact information of the sender or originator must be valid for a period of at least 60 days following the time at which the message was sent.

An unsubscribe mechanism must: (i) enable a recipient to indicate, at no cost, that he or she no longer wishes to continue to receive CEMs; and (ii) specify an electronic address or link to a website where the recipient can communicate this wish. The electronic address or link to the website must be valid for a period of at least 60 days following the time at which the message was sent. Once the recipient has expressed his or her wish to unsubscribe, the sender or originator has up to 10 business days to ensure that no further CEMs are sent to the recipient.

Installation of Computer Programs

The FISA makes it illegal to install a computer program on a person's computer without their express consent, or where a computer program has been installed, cause a message from that computer to be sent without the person's express consent. The FISA does not distinguish between malicious spyware and software used for legitimate business purposes; the installation of all computer programs must comply with the law.

The person to whom such consent was granted must ensure, for a period of 1 year[3], that the owner or authorized user of the computer on which the program is installed is provided with an electronic address by which he or she can send a request to remove or disable the computer program. In addition, if the consent was originally based on an inaccurate description of the material elements of the computer program, the owner of the computer or authorized user must be provided with assistance, at no cost, to remove or disable the computer program.

Express Consent

When seeking to obtain the express consent of a person, the request must clearly set out the purposes for which the consent is being sought, the prescribed information regarding the identity of the person requesting the consent and the person on whose behalf the consent is being obtained, and any other information which may be set out in the regulations.

The FISA includes certain additional requirements where a computer program performs certain functions stipulated in the legislation or regulations. Under these requirements, these functions, and their reasonably foreseeable impact on a computer system, must be described

and the computer owner's or authorised user's consent must be obtained separately from the license agreement of the software. These functions include: (a) collecting personal information stored on the computer system; (b) changing or interfering with settings, preferences or commands already installed or stored on the computer system without the knowledge of the owner or an authorized user of the computer system; and (c) causing the computer system to communicate with another computer system, or other device, without the authorization of the owner or an authorized user of the computer system.

Altering Transmission Data

Most people have experienced a virus which intercepts data transmitted across a web browser, or which redirects the web browser to a different website. This process of rerouting and intercepting data is often employed in "phishing" scams which seek to acquire certain confidential information like online banking passwords and account numbers, or redirect users to a look-a-like online banking page in order to acquire this information directly.

In an effort to restrict such activities, the FISA generally prohibits the alteration of transmission data[4] so that a message is delivered to a destination other than, or in addition to, the destination specified by the sender. Such alteration of transmission data is permitted with the express consent of the sender, provided that the person to whom such consent was granted ensures that (a) the sender can withdraw such consent and is provided with an electronic address by which he or she can withdraw such consent; and (b) any such withdrawal of consent is effected within 10 business days after receipt. As highlighted in the Business Strategies section below, the FISA transmission data provisions may apply to businesses in unexpected ways.

Supervision and Enforcement

The FISA grants broad and sweeping powers to the Canadian Radio-television and Telecommunications Commission (the "**CRTC**"), the organization responsible for supervising compliance with the Act. Persons designated by the CRTC can cause a notice to be served on any person to ensure compliance with the FISA, including an order to produce a copy of a document, prepare a document based on data, or to produce any other information. In addition, a CRTC designee can obtain a warrant from a justice of the peace to enter into the premises of any person or business in order to verify compliance with the FISA. Subject to the conditions set out in the warrant, the CRTC designee may examine anything found on the premises, use any means of communication or computer system, prepare or copy documents, remove anything found on the premises for copying or examination, and even prohibit or limit access to all or part of the premises. The CRTC designee can also ask the court to order an injunction to stop a person who is violating, or is likely to violate, the FISA.

Furthermore, the FISA provides individuals with a private right of action against violators of the legislation as well. For example, spammers can be sued for $200 per contravention, up to a maximum of $1,000,000 per day. Software-makers and data interceptors can be sued for a maximum of $1,000,000 per day that software is installed without a user's consent or data is being rerouted or intercepted. Those who aid, induce, procure or cause to be procured any of the aforementioned acts are, in addition to the amounts listed above, also liable to be sued up to a maximum of $1,000,000. Other offences are also included for violations of the *Personal Information Protection and Electronic Documents Act* and the *Competition Act*.

Violations and Offences

Separate from the private right of action noted above, the FISA imposes administrative monetary penalties to persons who send unsolicited CEMs, alter transmission data or install computer programs without obtaining the appropriate consent. The maximum penalty for any such violation committed by an individual is $1,000,000, and $10,000,000 in the case of a corporation or any other person.

The FISA also provides for certain offences, namely failure to comply with a demand or notice from a CRTC designee, or failure to assist a CRTC designee during the execution of a warrant. Obstructing, hindering, or knowingly misleading a CRTC designee is also an offence. These offences are punishable on summary conviction and a person convicted is liable to a fine of: (i) not more than $10,000 for a first offence or $25,000 for a subsequent offence in the case of an individual; and (ii) not more than $100,000 for a first offence or $250,000 for a subsequent offence in the case of a corporation or any other person.

Business Strategies

Regarding Spam

Many businesses outsource email and electronic marketing functions to third parties. One of the key considerations arising from the FISA is the joint liability of both senders and the businesses on behalf of which email communications are sent. In other words, a business could find itself liable for the negligence of its email marketing service provider if that company does not provide an unsubscribe mechanism in its emails. As a result, businesses that have existing commercial relationships with third-party email marketing firms would be well-advised to have their services contracts reviewed and updated.

Be Mindful When Transmitting Data

Many businesses will use contact forms to enable their customers to communicate with the customer service department. Often times, such contact forms will send an email to the customer service department and the quality control department as well in order to ensure a follow-up on the sources of customer complaints. Failing to notify the customer that the contact form is directed at both the customer service and quality control departments would be a violation of the FISA.

Obtaining Consent

With the new rules on obtaining consent, software license agreements will need updating and separate consent forms will need to be established. Depending on the functionality of the software, these consent forms will need to specify additional details concerning any of functions prescribed by the Act. For example, a consent form would need to specify whether the software (a) collects or transmits personal information, (b) changes or interferes with settings, preferences or commands already installed or stored on the computer system without the knowledge of the owner or an authorized user of the computer system; or (c) causes the computer system to communicate with another computer system, or other device, without the authorization of the owner or an authorized user of the computer system.

In light of the significant consequences of non-compliance with FISA, it is widely expected that many businesses will need to improve their current record-keeping practices in respect of tracking consents. In order to effectively respond to complaints and in order to ensure a high level of confidence when engaged in activities that are regulated by FISA, businesses must ensure, among other things, that an appropriate and defensible audit trail of consents is maintained.

Be Proactive

The best way to remain in compliance with the legislation is to be proactive and take the appropriate steps to ensure explicit consent is obtained for all forms of communication and interaction with customers and prospects. Unsubscribe mechanisms should be easy and hassle-free for users, and the language used in all forms of communication should be clear and simple to understand.

Read the full text for the *Fighting Internet and Wireless Spam Act*

For more information on the subject of this bulletin, please contact the author:

Constantinos Ragas
514 397 5244
cragas@fasken.com

---

[1] The author would like to thank Charles Lupien, Stéphane Caïdi, Alex Cameron, Daniel Fabiano and Jimmy Triassi for their assistance in preparing this bulletin.

[2] Implied consent is possible in certain limited circumstances, which include existing business relationships.

[3] This period starts at the time which the computer program begins to perform certain functions specified in the legislation or regulations, like collecting personal information.

[4] The definition of "transmission data" in FISA excludes data that reveals the substance, meaning or purpose of the communication. In other words, the content of an electronic communication is excluded, but the destination IP or email address is included.

FASKEN MARTINEAU
www.fasken.com

Contacts

VANCOUVER

Bruce Tattrie
604 631 4753
btattrie@fasken.com

TORONTO

John P. Beardwood
416 868 3490
jbeardwood@fasken.com

C. Ian Kyer
416 865 4396
ikyer@fasken.com

MONTRÉAL

Julie Desrosiers
514 397 7516
jdesrosiers@fasken.com

Stéphane Gilker
514 397 7608
sgilker@fasken.com

QUÉBEC CITY

Isabelle Chabot
418 640 2020
ichabot@fasken.com

LONDON

Ralph Cox
+44 207 917 8622
rcox@fasken.co.uk

PARIS

Jérôme Richardot
+33 1 44 94 96 98
jrichardot@fasken.com