



# PROPOSED CANADIAN FIGHTING INTERNET AND WIRELESS SPAM ACT

*By Bradley J. Freedman*

The Canadian Parliament is now considering Bill C-28 – the *Fighting Internet and Wireless Spam Act (FISA)* – which was introduced by the Government of Canada on May 25, 2010 with the stated purpose of prohibiting unsolicited commercial email (spam), deterring the most damaging and deceptive forms of online fraud (such as identity theft, phishing, and spyware) and helping to drive spammers out of Canada. *FISA* is a revised version of the proposed *Electronic Commerce Protection Act*, which was originally introduced to Parliament in April 2009 and was under consideration by the Senate when Parliament was prorogued in December 2009.

*FISA* would create a comprehensive regulatory regime of offences, enforcement mechanisms, and severe penalties, all designed to protect individuals and businesses engaged in electronic commerce. All businesses engaged in electronic marketing and software distribution in Canada should be familiar with *FISA* and be prepared to comply with its requirements if passed by Parliament.

## I Regulated Conduct

### (a) Commercial Electronic Messages – Spam

*FISA* would prohibit spam by prohibiting commercial electronic messages (including email, instant messaging, and messages to telephone accounts) unless: (1) the recipient has consented to receive the message; and (2) the message complies with required formalities, including information regarding both the actual and beneficial sender of the message, a sender's contact information, and an effective and timely unsubscribe mechanism.

The prohibition applies to the person who actually sends the message and all persons on whose behalf the message is sent. An electronic message is considered to be "commercial" if the message content, including hyperlinks to Web sites and contact information, makes it reasonable to conclude that a purpose of the message is to encourage participation in a commercial activity, including transactions for goods, services, or land, business, investment or gaming opportunities, or the promotion of a person involved in any of those activities.

# PROPOSED CANADIAN FIGHTING INTERNET AND WIRELESS SPAM ACT

---

The prohibition does not apply to noncommercial messages. There are also various exceptions for commercial messages, including messages between individuals with a personal or family relationship; messages that facilitate, complete, or confirm a commercial transaction; messages that provide warranty, recall, safety, or security information to appropriate recipients; factual information regarding subscription, membership, account, or similar information to appropriate recipients; messages relating to an employment relationship or related benefits; messages that deliver products or services (including updates or upgrades) to appropriate recipients. In addition, the prohibitions do not apply to commercial electronic messages that are interactive two-way voice communications between individuals, facsimile messages, or voice recordings to a telephone account.

Consent to receive a commercial electronic message may be express or implied. Express consent must be based upon the disclosure of prescribed information (including the purposes for which consent is sought and the identity of the person seeking the consent). Consent may be implied in limited circumstances, including a current or recent preexisting business relationship between the sender and recipient (including a current written contract between them or a commercial transaction within the previous 18 months) or a preexisting non-business relationship between the sender and recipient (including a donation by the recipient to a sender charity or political party within the previous 18 months). There is also a three-year transition provision that provides for implied consent in limited circumstances.

Notably, the requirements of informed consent and formalities also apply to an electronic message that seeks consent to send further commercial electronic messages.

## **(b) Fraudulent Data Collection – Phishing**

Phishing is a fraudulent technique that uses counterfeit Web sites or fake electronic messages to fool individuals into disclosing their personal, financial, and other sensitive information to unintended recipients. The victim intends to send the information to one recipient, but in fact it goes somewhere else.

*FISA* contains an anti-phishing provision that would prohibit a person, in the course of commercial activity, from altering the transmission data in an electronic message so that the message is delivered to a destination other than or in addition to the destination specified by the sender, without the sender's express consent. The consent must be informed (based upon prescribed information disclosure), and an effective and timely consent withdrawal mechanism must be provided as well.

## **(c) Software Distribution**

*FISA* would prohibit a person, in the course of commercial activity, from installing any computer program (not just spyware) on any other person's computer system, or causing that computer program to send an

# PROPOSED CANADIAN FIGHTING INTERNET AND WIRELESS SPAM ACT

---

electronic message from the computer system, without the consent of the owner or authorized user of the computer system. In most circumstances, the required consent must be express and informed (based upon prescribed information disclosures, including the function and purpose of the computer program), and an effective and timely consent withdrawal mechanism must also be provided. There are limited exceptions that permit implied consent to the installation of legitimate computer software. There is also a three-year transition provision that provides for implied consent to the installation of a software update or upgrade in limited circumstances.

*FISA* would also amend the *Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)* to prohibit the unauthorized collection of an individual's electronic address or personal information by use of a computer program designed for collecting that information or by unauthorized access to a computer system, or the use of an electronic address or personal information collected in that manner, without the individual's consent.

## (d) Misleading Electronic Messages

*FISA* would also amend the *Canadian Competition Act* to add new provisions prohibiting the sending of an electronic message that contains false or misleading information regarding the sender or subject matter of the message, false or misleading information in the content of the message, or false or misleading information regarding a source of data on a computer system (including a URL). The message recipient need not have been deceived or misled by the message for these provisions to apply, and they are not limited to commercial electronic messages.

## II Enforcement

### (a) Regulatory/Criminal Enforcement

*FISA* would give the Canadian Radio-television and Telecommunications Commission (CRTC) broad powers to investigate and impose substantial administrative monetary penalties for violations of *FISA* – up to \$1 million for an individual and up to \$10 million for an organization. The factors to be considered in assessing penalties include the nature and scope of the violation, past violations, the financial benefits of the violation, and ability to pay.

False and misleading electronic messages would be subject to administrative enforcement by the Competition Bureau or criminal prosecution, with severe penalties – an unlimited fine and up to 14 years in jail for conviction on indictment, or a fine not exceeding \$200,000 and up to one year in jail for summary conviction.

# PROPOSED CANADIAN FIGHTING INTERNET AND WIRELESS SPAM ACT

---

Regulations may have the effect of substantially increasing maximum fines by providing that a contravention of *FISA* constitutes a separate violation for each day that it continues.

A *FISA* violation is not a criminal offence, and is not punishable by imprisonment. Corporate officers and directors can be held personally liable for corporate violations, and employers can be held liable for violations committed by their employees or agents acting within the scope of their employment or authority. Due diligence to prevent the commission of the violation is a defence.

## **(b) Private Enforcement**

*FISA* would give a private right of civil action to businesses and consumers affected by a violation of *FISA*, the unlawful collection, use, or disclosure of personal information in violation of *PIPEDA*, or misleading electronic messages in violation of the *Competition Act*. The action may be brought against the persons who committed the violation and all other persons liable for the violation (including corporate directors and officers and persons whose employees or agents committed the violation within the scope of their employment or authority). A private right of action is not available if the violation is already subject to an undertaking or a notice of violation issued by the CRTC.

The remedies available in a private action include compensation for loss, damage, and expense plus an additional payment of up to \$200 for each contravention to a maximum of \$1,000,000 for each day a contravention occurred. The private action remedy is modeled on similar legislation in the United States, where courts have issued multimillion-dollar judgments against spammers.

## **(c) Consultation and Coordination**

*FISA* would permit the CRTC, the Commissioner of Competition, and the Privacy Commissioner to consult with each other and to coordinate their enforcement activities. *FISA* would also permit the disclosure of personal information to foreign governments and institutions and international organizations to assist in an investigation or proceeding regarding unlawful activities that would constitute violations of *FISA* or related laws.

The Government of Canada has also announced that Industry Canada will act as a national coordinating body in order to increase consumer and business awareness and education, to coordinate work with the private sector regarding voluntary guidelines, and to conduct research. Also, the Government intends to create a Spam Reporting Centre to receive reports of spam and related threats.

# PROPOSED CANADIAN FIGHTING INTERNET AND WIRELESS SPAM ACT

---

## Impact on Canadian Businesses

If FISA becomes law, many Canadian businesses will have to change their Internet marketing practices. Commercial electronic messages will have to disclose prescribed information and provide recipients with an easy-to-use way to opt out of future messages. Businesses will also have to ensure that commercial electronic messages are sent only to persons who have given express or implied consent to receive the message, and have not opted out of future messages. Computer software businesses will also have to ensure that electronic distribution of software (including software updates) complies with disclosure and consent requirements.

### Bradley J. Freedman

604 640-4129

[bfreedman@blgcanada.com](mailto:bfreedman@blgcanada.com)

*This bulletin is prepared as a service for our clients and other persons dealing with information technology issues. It is not intended to be a complete statement of the law or an opinion on any subject. Although we endeavour to ensure its accuracy, no one should act upon it without a thorough examination of the law after the facts of a specific situation are considered. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP.*

*This bulletin has been sent to you courtesy of Borden Ladner Gervais LLP. We respect your privacy, and wish to point out that our privacy policy relative to bulletins may be found at <http://www.blgcanada.com/home/website-electronic-privacy>. If you have received this bulletin in error, or if you do not wish to receive further bulletins, you may ask to have your contact information removed from our mailing lists by phoning 1-877-BLG-LAW1 or by emailing [subscriptions@blgcanada.com](mailto:subscriptions@blgcanada.com).*

© 2010 Borden Ladner Gervais LLP

**Borden Ladner Gervais LLP**  
Lawyers • Patent &  
Trade-mark Agents

### Calgary

1000 Canterra Tower  
400 Third Avenue S.W.  
Calgary, Alberta, Canada  
T2P 4H2  
tel: 403 232-9500  
fax: 403 266-1395

### Montréal

1000 de La Gauchetière  
Street West  
Suite 900, Montréal,  
Québec, Canada H3B 5H4  
tel: 514 879-1212  
fax: 514 954-1905

### Ottawa

World Exchange Plaza  
100 Queen St., Suite 1100  
Ottawa, Ontario, Canada  
K1P 1J9  
tel: 613 237-5160  
1-800-661-4237  
legal fax: 613 230-8842  
IP fax: 613 787-3558

### Toronto

Scotia Plaza,  
40 King Street West  
Toronto, Ontario, Canada  
M5H 3Y4  
tel: 416 367-6000  
fax: 416 367-6749

### Vancouver

1200 Waterfront Centre  
200 Burrard Street,  
P.O. Box 48600  
Vancouver, British Columbia,  
Canada V7X 1T2  
tel: 604 687-5744  
fax: 604 687-1415

### Waterloo Region

Waterloo City Centre  
100 Regina Street South,  
Suite 220  
Waterloo Ontario N2J 4P9  
tel: 519 579-5600  
fax: 519 579-2725  
IP fax: 519 741-9149

[www.blgcanada.com](http://www.blgcanada.com)

**Borden Ladner Gervais LLP**  
is an Ontario Limited  
Liability Partnership