Blaney McMurtry
BARRISTERS & SOLICITORS LLP

EXPECT THE BEST

New Law That Limits Sales Tactics Scheduled to Take Effect Soon

by H. Todd Greenbloom and Varoujan Arman
Originally published in *Blaneys on Business* (June 2011)

Todd Greenbloom is a partner in Blaney McMurtry's corporate/commercial group. His active general business law practice intersects with a host of competition and restrictive trade practices issues. Todd is a recognized authority on all aspects of franchising and licensing. His clients come from a wide variety of industries, including restaurants, food service, hospitality, recreation, trade shows, retailing, manufacturing, advertising and service.

Todd may be reached directly at 416.593.3931 or tgreenbloom@blaney.com.

Varoujan Arman, a graduate of The University of Windsor law school, is an articling student at Blaney McMurtry, and will be joining Blaney McMurtry as an associate in the corporate commercial litigation group in September, 2011.

New federal law that prohibits businesses from transmitting spam – electronic messages that are not wanted and that have not been requested – is expected to take effect later this year or early next.

Businesses and other organizations that send electronic messages as part of their marketing efforts, or for other uses, will want to conduct a careful review of their practices and evaluate whether they run afoul of the new legislation.

The legislation, known as FISA (*Fighting Internet and Wireless Spam Act*), was passed last December. It will be enforced by three federal agencies – The Office of the Privacy Commissioner of Canada (OPC), the Canadian Radio-Television and Communications Commission (CRTC), and Industry Canada – and will amend other legislation, including related computer privacy matters under the federal Personal Information Protection and Electronic Documents Act (PIPEDA).

One purpose of FISA is to regulate the transmission of commercial electronic messages. The term "electronic messages" has a broad definition and is not limited to e-mails. Text messages, sound, voice, or image messages, "tweets", and instant messages will all be subject to regulation. The Act will prohibit the sending of commercial electronic messages unless recipients have provided their consent, which in some instances can be implied.

Two-way voice communications, fax transmissions sent to a telephone account, or a voice recording sent to a telephone account are excluded from the prohibitions. At this time two-way voice communications, fax transmissions sent to a telephone account or a voice recording sent to a telephone account are covered under the National Do Not Call List (DNCL). Currently, Bell Canada has a contract with the CRTC to maintain the DNCL.

One significant loophole is that the Act only applies where the computer used to send or access the electronic message is located in Canada.

Unlike its American counterpart, which targets predominantly unsolicited spam e-mails, FISA also aims to regulate several other related areas. For instance, it prohibits the unauthorized installation of spyware or other similar software, the alteration of transmission data, the transmission of false or misleading information, and the unauthorized access to a user's computer to collect personal information or other e-mail addresses. The latter suggests that the widespread use of cookies, that retain for a vendor personal customer information and that are sometimes used without the consent of the user, may fall under the scrutiny of the new Act.

"Phishing" may also fall under the regulation of FISA. "Phishing" is the attempt to collect personal information by having users enter their information or passwords onto web pages where the user is led to believe the page is from an authentic source, but is not. Because the information is entered voluntarily, one could argue that consent is given and there is accordingly no violation. However, FISA's prohibition on sending false or misleading information may overcome that argument and protect the user.

Under the Act, when seeking express consent to send an electronic message, a business will be obliged to clearly and simply set out the purpose for which the consent is being sought and identify itself as the party requesting the consent.

A best practice for online forms is to always include an opt-out check-box where the user can decline to receive any future communications. Similarly, all messages sent must include an unsubscribe option.

As indicated earlier, FISA contains some exceptions to its rules. The recipient providing consent to receive information is one. Consent might be given or inferred through ongoing subscriptions to a website or blog, or transactions of an ongoing nature where there is an existing relationship. Other more specific exceptions are also provided in the Act.

There are circumstances in which consent to receiving messages need not be given expressly. Businesses and other organizations may be taken to imply consent based on the established relationship described above. The period of implied consent expires after two years from the date of the transaction, dealing, or termination of the relationship.

FISA begins to encounter some inevitable grey areas when it comes to implied consent. For instance, how will the Act treat businesses that advertise through Facebook, Twitter, blogs, or other computer-based billboard-type locations which the user must first actively seek out and then "join," "like", or follow?

Even more unclear would be a situation where a company "tweets" (through Twitter) about something popular but unrelated to its basic business in order to attract and "sign up" a large number of followers, only to then change the use of the account to begin sending or posting advertising or promotional materials. What remains to be determined is what level of informed consent from the recipient will be required to bring an activity within the implied consent exception.

FISA will be good news-bad news for many people who are businessmen and women and consumers at the same time. As individuals, most users of computers and other electronic devices find spam annoying. They will therefore applaud the government and Parliament for the new Act. As people who work in businesses or organizations that use electronic messaging, however, they may not like the new level of regulation, or the severe penalties that go with it. These penalties range up to a $1 million fine in the case of an individual, and up to $10 million in the case of a corporation.

What can businesses and other organizations do in response to the new legislation? They should become familiar with the Act, understand it, and determine which, if any, of their practices they need to change to ensure compliance with the Act.

As some grey areas already exist and, where a "tie" situation seems likely, businesses should err on the side of caution instead of pushing the envelope.

It remains to be seen how aggressively the three enforcing agencies will pursue offenders. Advice of legal counsel will be of critical importance in establishing and maintaining compliance with FISA. ■