CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CHARITY LAW BULLETIN NO. 238

JANUARY 27, 2011

EDITOR: TERRANCE S. CARTER

NEW RULES FOR SPAM IMPACTS REGISTERED CHARITIES AND NOT-FOR-PROFITS

By Ryan M. Prendergast*

A. INTRODUCTION

On December 14, 2010, Bill C-28, the *Fighting Internet and Wireless Spam Act* ("FISA")[1] received Royal Assent.[2] FISA is a revived version of Bill C-27, the Electronic Commerce and Protection Act, which died on Order Paper during the 2nd Session of the 40th Parliament due to the prorogation of Parliament on December 30, 2009. FISA creates a new regulatory scheme for spam and related unsolicited electronic messages, as well as amending four existing statutes dealing with privacy and telecommunications. These include the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), of which organizations with existing privacy obligations may already be aware. However, FISA will also expand on the privacy and confidentiality obligations of registered charities and not-for-profits, particularly if they carry out commercial activities.

This *Charity Law Bulletin* provides an overview of FISA, along with the impact it may have on registered charities and not-for-profit organizations.

* Ryan M. Prendergast, B.A., LL.B., is an associate of Carters Profession Corporation, Orangeville, Ontario, Canada.

[1] While commonly referred to as the *Fighting Internet and Wireless Spam Act*, it is interesting to note that Bill C-28 does not itself contain a short title. In this regard, the name *Fighting Internet and Wireless Spam Act* was removed from Bill C-28 on November 2, 2010 by the Standing Committee on Industry, Science and Technology. It remains to be seen how the bill will be referred to once it comes into force.

[2] More information regarding FISA as well as the text of the legislation, can be found online at: http://www2.parl.gc.ca/Sites/LOP/LEGISINFO/index.asp?Language=E&query=7019&Session=23&List=toc.

B. OVERVIEW OF FISA

1. Definitions

FISA contains a broad definition of "commercial activity" meant to capture a wide range of activities. In this regard, FISA defines "commercial activity" 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, other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada." It is important to note that this definition expands on the definition for "commercial activities" in PIPEDA, which defines "commercial activity" as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists." However, this expanded definition does not modify the existing definition in PIPEDA.

FISA defines a "commercial electronic message" as one where it would be "reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity..."[3] This reasonable conclusion would take into consideration the content of the message, any hyperlinks contained in the message, as well as the contact information contained in the message. Therefore, even if the message itself did not contain information that would expressly lead one to conclude that it was a "commercial electronic message," a hyperlink to a webpage that could lead the reader to infer it is encouraging participation in a commercial activity could catch message in the prohibition described below.

FISA also broadly defines "electronic address," which applies not only to e-mail addresses, but also to instant messaging accounts, telephone accounts or any similar account. This could include an individual's Facebook or Twitter account, in order to ensure that spam messages to such accounts are caught by the prohibition as well.

[3] FISA, section 2.

2. The general prohibition against "commercial electronic messages" without consent

It is an offence under FISA to "send or cause or permit to be sent" a "commercial electronic message" without the person who receives it having provided consent.[4] However, several exemptions are provided for, which include but are not limited to where the message is being sent to an individual with whom the sender has a personal or family relationship. The prohibition also does not apply if the message sent is to provide information such as a quote, warranty information, updated product information, or similar content related to on-going business relationships.

Even where the receiver has consented to receive the "commercial electronic message", the content of the message must still contain certain prescribed requirements under FISA. The "commercial electronic message" must: set out information that identifies the person who sent the message or the person on whose behalf it was sent; information enabling the person to whom the message is sent to readily contact the sender; and a means by which the receiver can unsubscribe from receiving further "commercial electronic messages." The contact information must also be valid for 60 days following the sending, or causing to be sent, of the "commercial electronic message." According to subsection 11(1) of FISA, the mechanism through which the receiver can unsubscribe from receiving further "commercial electronic message" must enable the receiver to indicate that they no longer wish to receive any messages from the sender, either through the same e-mail which they received, or any other electronic means. Additionally, a request from an individual to no longer receive messages from the sender must be acted upon no later than 10 business days after the request has been sent.

Sections 7 to 9 also contain further prohibitions against the altering of the transmission data of a message, as well as against installing malware such as bots, viruses and spyware, or any other computer program without consent on an individual's computer.

3. Consent Provisions of FISA applicable to registered charities and not-for-profit organizations

For registered charities and not-for-profit organizations that maintain lengthy donor or member lists to which they send regular e-mails that fit within the definition of "commercial electronic message," consent to receive such message can be implied only if certain conditions under FISA are met. These

[4] FISA, section 6.

conditions include where the person who sends the message and the receiver have an "existing business relationship" or an "existing non-business relationship."

An "existing non-business relationship" can arise were a donation or gift was made by the person to whom the "commercial electronic message" was sent within the two-year period "immediately before the day on which the message was sent..." and the person who sent the message was a charity. The same exemption and time period also applies where a person has done volunteer work with the charity within the past two year period. An "existing non-business relationship" can also arise in the context of not-for-profit organizations where the person is a member of a "club, association or voluntary organization." In this regard, the time period of two years commences on the day that the membership terminates.[5] It is interesting that registered charity is defined by reference to the *Income Tax Act* (Canada)("ITA") but membership in a club, association or voluntary organization which bears a striking resemblance to "club, society, or association" under 149(1)(l) of the ITA, is to be defined by regulation.

The consequence of these provisions is that a person who was once a donor to a registered charity or member of a not-for-profit organization will not always be so for the purpose of sending them a message that may be considered a "commercial electronic message."

In this regard, in order to avoid the need to monitor the expiry of an existing "non-business relationship," it would be ideal for the organization to obtain the receiver's express consent. Where the registered charity or not-for-profit organization wishes to obtain the express consent of a person to send them a "commercial electronic message," the message must set out the purposes for which the consent is being sought and prescribed information that identifies the person seeking the consent. It is important to note that an electronic message that contains a request for consent to send a "commercial electronic message" is itself deemed to be a "commercial electronic message."[6] This would prevent an organization from sending a request for consent to send an "commercial electronic message" to an individual where there is no pre-existing relationship, whether it be an "existing business relationship" or "existing non-business relationship." In this regard, section 66 of FISA will provide for a 3 year transitional period once FISA comes into force where a person's consent to receive a "commercial

[5] FISA, para. 10(14)(b)
[6] FISA, ss. 1(3).

electronic message" is implied from an "existing business relationship" or an "existing non-business relationship" as defined in FISA.

4. Consequences of failure to comply with FISA

Violation of section 6 or other prohibitions contained within FISA can result in monetary penalties of up to $1,000,000 for individuals and $10,000,000 for corporations. The threat of such heavy fines is somewhat measured by subsection 20(2) of FISA which states that, "The purpose of a penalty is to promote compliance with the Act and not punish." This presumably indicates that monetary penalties are not to be issued in a punitive manner.

In addition, section 47 of FISA also allows for a private right of action by an individual who alleges that they were affected by any act or failure to act that lead to a breach of the prohibitions contained in sections 6 to 9 of FISA. FISA will empower the court to award to a successful applicant of a private right of action compensation for any actual loss or damage suffered, as well as further monetary amounts for each day on which the breach occurred.

Furthermore, Section 52 of FISA also provides that an "officer, director, agent or mandatary of a corporation" that commits a contravention of sections 6 to 9 of FISA, as well as certain provisions of PIPEDA and the *Competition Act*, is liable for the contravention if they "directed, authorized, assented to, acquiesced in or participated in the commission of that contravention." Subsection 53 also makes a person vicariously liable for breaches committed by their employees. However, FISA also provides a statutory due diligence defence under subsection 54(1) which may provide some relief against third-party claims for a person, whether they be an individual or a corporation.

C. CONCLUSION

Although FISA is not yet in force, registered charities and other not-for-profit organizations will want to review their privacy and electronic communications policies to comply with FISA when it does come into force, and that they are keeping appropriate records of all donors, volunteers and members prior to sending them a "commercial electronic message." It is expected that FISA will come into force potentially during the summer of 2011. It will also be important to monitor when the regulations are made available as they will add considerable definition to the statute.