May 3, 2011

On December 15, 2010, Canada passed the Fighting Internet and Wireless Spam Act (also known as "Canada's Anti-Spam Law"), the world's most stringent anti-spam law.[1] Regulations implementing Canada's Anti-Spam Law are expected to be issued for public comment this spring, while the law is expected to take effect in September 2011.[2] Although there are many similarities between Canada's Anti-Spam Law and the U.S. CAN SPAM Act of 2003,[3] there are important differences that may result in liability for U.S. companies that fail to understand and address them in their electronic marketing policies and practices. These differences include the following:

1. The U.S. CAN-SPAM Act applies only to commercial *e-mail* messages that are "primarily promotional," but Canada's Anti-Spam Law applies to all *electronic* messages with any commercial content to an electronic address, including 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), delivered in connection with a commercial activity.

2. The U.S. CAN-SPAM Act regulates, but does not prohibit, unsolicited commercial e-mail, but Canada's Anti-Spam Law prohibits unsolicited commercial electronic messages within or into Canada unless the sender has obtained either explicit or implied consent from its intended recipients.[4]

3. The U.S. CAN-SPAM Act does not address malware or spyware, but Canada's Anti-Spam Law prohibits installing any computer program in the course of a commercial activity unless express consent has been given. If the software meets certain spyware or malware criteria, the sender must also bring its "foreseeable" impacts to the user's attention.

4. Canada's Anti-Spam Law imposes much higher potential liability on those who violate its provisions than the U.S. CAN-SPAM Act, with penalties ranging up to C$1 million for individuals and C$10 million for businesses. Officers and directors can also be liable under Canada's Anti-Spam Law if they directed, authorized, acquiesced in or participated in the offending conduct.

U.S. companies face potential liability under Canada's Anti-Spam Law if they are sending commercial electronic messages to users who reside in Canada. Since the Canadian law is not expected to become effective until the fall, U.S. companies should review their existing electronic marketing policies and practices now to ensure that they comply with the requirements of Canada's Anti-Spam Law.

Application

Unlike CAN-SPAM, which only covers email, Canada's Anti-Spam Law applies to electronic messages to an electronic address, including 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), delivered in connection with a commercial activity.[5] "Commercial activity" is defined as any 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 with the expectation of profit.[6]

Canada's Anti-Spam Law creates an "opt-in" system whereby prior consent must be obtained from the recipient in order to deliver a commercial electronic message, as opposed to the "opt-out" system used in the U.S. where the sender can send a message without prior consent as long as the recipient is able to "opt-out" of receiving future messages. As a result, the Canada law places

the burden on the sender to demonstrate it received consent prior to sending a commercial electronic message.

Implied consent

Consent is implied in the following cases:

1. Electronic communications where the sender and the recipient have an "existing business relationship" ("EBR") or a "non-business relationship" (e.g., membership in a club or the recipient made a donation), where the relationship arose within the past two years or is pursuant to a contract in effect in the past two years (there is however, a limited grandfather provision that provides that these two year time limits do not apply during the initial three year period after Canada's Anti-Spam Law takes effect, if the EBR included communications using commercial electronic messages);[7]

2. Where the recipient has conspicuously published, or has caused to be conspicuously published, his or her electronic address, the publication is not accompanied by a statement that the person does not wish to receive unsolicited commercial electronic messages at the electronic address, and the message is relevant to the person's business, role, functions or duties in a business or official capacity; or

3. Where the recipient has disclosed to the sender the electronic address to which the message is sent without indicating a wish not to receive unsolicited commercial electronic messages at the electronic address, and the message is relevant to the person's business, role, functions or duties in a business or official capacity.[8]

Consent is also assumed for other key categories, such as most normal business-to-business communications (e.g., providing a quote or estimate requested by the recipient; facilitating, completing or confirming an existing commercial transaction; providing warranty or similar information about a product or service that the recipient has purchased; providing factual information about an ongoing subscription or similar service; or delivering a product or services, including updates and upgrades, pursuant to an existing relationship).[9] If a business is sold, the purchaser assumes the existing business relationships of the seller for purposes of implied consent.[10] If there is a personal relationship, communications are exempt, so viral marketing is not affected by the new law.[11]

Express consent required

Except as set forth above, express consent is required before a commercial electronic message can be sent. The consent must (1) identify why consent is being sought, and (2) identify the person seeking consent as well as the person on whose behalf consent is being sought, along with (3) any other requirements which may be prescribed by regulation.[12] An electronic message that contains a request for consent is also considered to be a commercial electronic message subject to the act, so express consent cannot be obtained by sending a request for consent by email.[13]

Form and content of commercial electronic messages

Commercial email messages must be in a form that will be prescribed in the regulations to be issued pursuant to Canada's Anti-Spam Law, identify the sender or senders, provide contact information for the sender(s), and include an "unsubscribe" mechanism. The unsubscribe mechanism must enable opt-outs using the same electronic means by which the messages are sent, or, if using those means is not practicable, any other electronic means that will enable the person to indicate the wish.[14] In addition, the sender must specify an electronic address, or link to a web page that can be accessed through a web browser, where the recipient can express his or her desire to unsubscribe.[15] The electronic address of the web page where the recipient can express the desire to unsubscribe must be valid for at least 60 days after the message is sent.[16] Upon receiving notice of a desire to unsubscribe, the

sender must unsubscribe the address within no more than ten business days.[17]

Canada's Anti-Spam Law also prohibits false or misleading representations in electronic messages, including in subject lines and headers, email harvesting, and altering transmission data to route a message to an unintended destination.

Anti-spyware, anti-malware provisions

In an effort to target malicious software, Canada's Anti-Spam Law prohibits the installation of any computer program in the course of a commercial activity unless express consent has been given. Consent is deemed to have been given for the purposes of web functionality (such as in the case of cookies, HTML code, Java Scripts, operating systems, patches and add-ons and other programs which may be listed in regulations issued pursuant to the new law),[18] but otherwise must be express.[19] When consent to install is required, it must "describe clearly and simply the function and purpose of every computer program that is to be installed."[20] If the software meets the following spyware or malware criteria, the sender must also bring its "foreseeable impacts" to the user's attention:

1. collecting personal information stored on the computer system;
2. interfering with the user's control of the computer system;
3. changing or interfering with settings or preferences on the computer system without the user's knowledge;
4. changing or interfering with access to or use of that data on the computer system;
5. causing the computer system to communicate with another computer system without the user's authorization;
6. installing a computer program that may be activated by a third party without the user's knowledge; or
7. performing any other function specified in regulations issued pursuant to Canada's Anti-Spam Law.[21]

These requirements apply to computers and computer servers, as well as any electronic device that allows for the installation of third party programs, such as tablets and smartphones. Because express consent is required under the anti-spyware provisions, this may have implications for online agreements such as web wrap agreements.[22]

Penalties

The Canadian Radio-television and Telecommunications Commission (CRTC) can impose administrative monetary penalties of up to C$1 million per violation of the Anti-Spam Law for individuals and C$10 million for businesses.[23] Officers, directors and agents may be personally liable if they acquiesced in a violation of the law. Unlike the CAN-SPAM Act, which does not provide a general cause of action for persons that receive commercial e-mail messages, Canada's Anti-Spam Law also provides statutory damages of C$220 per commercial electronic message (up to a maximum of C$1 million per day), C$1 million per day for altering transmission data, and C$200 for each collection (or subsequent use) without consent of an electronic address using "address harvesting" software (up to a maximum of C$1 million per day). These statutory damages, coupled with a private right of action which allows individuals to sue anyone who violates the law, provide powerful incentives for litigation and potentially open up the door to class action proceedings.

Recommendations

Canada's Anti-Spam Law takes into account "honest mistakes," and therefore it is important for any businesses that are subject to it to undertake clearly defined actions to comply.[24] As a result, we recommend that U.S. based businesses that may be sending

commercial electronic messages to Canadian residents, whether intentionally or not, take the following steps:

1. Collect consents. Develop internal systems to request, collect and store individual consents. Update your website to ensure you are obtaining express consent for email and newsletters. Review and update procedures for consents, opt-out requests, update unsubscribe requests within the required time frame.

2. Seek express consent now. After Canada's Anti-Spam Law becomes effective, an electronic message that contains a request for consent will be considered as a commercial electronic message subject to the law, so it will not be possible to obtain express consent by sending a request for consent by email. As a result, you should consider obtaining as many express consents as possible now, while you are still able to lawfully send a request for consent by email.

3. Use commercial electronic messaging in your existing business relationships. In order to take advantage of the grandfathering provision of Canada's Anti-Spam Law, during which the two (2) year time limits applicable to EBRs will not apply, make sure that you are using commercial electronic messaging with these customers before the law becomes effective.

4. Extend form and content requirements for commercial e-mails to other commercial electronic messages. Although U.S. companies who are in compliance with CAN-SPAM will not have much work to do related to the form and content of commercial e-mail messages, you will need to extend such practices to all electronic messages with any commercial content, including those sent via instant message, social media or mobile text messaging.

5. Installation of software in the course of a commercial activity. Ensure that you have a procedure for obtaining express consent before any computer program that is distributed in the course of a commercial activity is installed. Review web-wrap agreements to ensure they are compliant with the applicable provisions of Canada's Anti-Spam Law.

6. Ensure compliance with the amended PIPEDA. Review existing practices regarding the collection of personal information to ensure that they are compliant with the amendments to Personal Information Protection and Electronic Documents Act ("PIPEDA"), which prohibit the collection of personal information by means of unauthorized access to computer systems, and the unauthorized compiling of lists of electronic addresses.

7. Develop a compliance policy that addresses the key issues under Canada's Anti-Spam Law. Distribute the policy to relevant employees and provide training. This will support your assertion of the due diligence defense in Canada's Anti-Spam Law.

8. Representations regarding compliance with Canada's Anti-Spam Law. If you are purchasing or renting email or other electronic messaging lists, obtain representations from your vendor that consents have been obtained or that there are no Canadian addresses included on the lists. If you are acquiring another company, ensure that the representations and warranties included in any acquisition agreement include a provision regarding compliance with Canada's Anti-Spam Law.

9. Review regulations. The full impact of Canada's Anti-Spam Law will not be known until the implementing regulations are published. These regulations should be reviewed when they are published.

Notes

1 Fighting Internet & Wireless Spam Act, S.C., chapter 23.

2 According to Section 91 of the Act, the provisions of the Act will come into force on a day or days to be fixed by order of the Governor in Council.

3 15 U.S.C. §7701.

4 There is a 36 month transition period for existing business relationships in effect prior to the Act coming into force. §§ 66, 67.

5 §1(2).

6 §1(1).

7 §10(10)

8 §10(9).

9 §6(6).

10 §10(12).

11 §6(5)(a).

12 10(1).

13 A sender who has received the express consent of a recipient to receive commercial electronic messages must, for the period covered by the consent, ensure that the recipient is provided with an electronic address to which he or she may send notice of the withdrawal of consent and ensure that effect is given to withdrawal of consent no more than ten business days after it is received.

14 §11(1)(a).

15 §11(1)(b).

16 §11(2).

17 11(3).

18 The new law does not address whether beacons are exempt from these requirements, although this may be addressed in the regulations.

19 §10(8).

20 §§10(1), 10(3).

21 §10(5).

22 A person who has received the express consent of a user to the installation of a computer program must, for a period of one year after any program that performs one or more of the functions described in §10(5) ensure that the person is provided with an electronic address to which he or she may, if he or she believes the function, purpose or impact of the software was not accurately described before he or she gave consent, send a request to remove or disable, and if the consent was based on an inaccurate description of the material elements of the function, on receipt within that one year period, assist him or her in the removal or disabling of the program without cost and as soon as feasible.

23 The Competition Bureau, through application to the Competition Tribunal, may also seek administrative monetary penalties under the current regime in the Competition Act, which allows for penalties of up to C$750,000 for individuals and C$1 million per subsequent violation, and up to C$10 million for businesses and C$15 million per subsequent violation.

24 §33(1).

Key Contacts

Adam Ruttenberg Washington, DC	aruttenberg@cooley.com +1 202 842 7804