What Businesses Should Know About Canada's New Anti-Spam and Anti-Spyware Laws: Implications for Electronic Communications

Jennifer McKenzie, Catherine Lovrics & Peter Woods

On December 15, 2010, anti-spam and anti-spyware legislation passed in Canada (Bill C-28, Fighting Internet and Wireless Spam Act). Expectations are that the law will be brought into force sometime this year. The law aims to deter the most damaging and deceptive forms of spam, such as identity theft, phishing and spyware, and to help drive spammers out of Canada. However, its reach is much broader, and it is likely to affect most businesses that market to Canadians. Businesses have a few months to prepare for the law's wide net, to set policies and shore up consent to sending emails, etc., to their marketing lists.

With few exceptions, any commercial electronic message sent without consent and that is not in the prescribed format will be considered spam. This includes emails, instant messages, messages sent through social media sites and texts.

Consent may only be implied in a narrow set of circumstances, and otherwise must be express (i.e. recipients need to opt-in). Generally a message requesting consent to send emails, texts, etc., will itself be considered spam. For express consent, the opt-in 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 other prescribed information. Consent may be implied where there has been an existing relationship in the past two years, and if an address is conspicuously published without a statement to not send unsolicited messages, and the communication relates to that person's business. If there is a personal relationship, communications are exempt, so viral marketing is not affected. Faxes, voice recordings and messages subject to Canada's "Do Not Call" legislation are also exempt. There are other exceptions, and some will be set out in the regulations.

Electronic messages must: (1) identify the person who sent the message; (2) provide contact information for the sender (that is valid for at least 60 days); and, (3) set out an unsubscribe mechanism. The unsubscribe mechanism must enable opt-outs using the same electronic means by which the message is sent, and give a link or address to opt-out.

Bill C-28 also prohibits false or misleading representations in electronic messages, including in subject lines and headers. So marketers will need to be mindful to ensure teasers in subject lines and headers do not over exaggerate.

In an effort to target malicious software, the act prohibits installing any computer program (good or bad) in the course of a commercial activity unless express consent has been given. Consent is deemed for the purposes of web functionality (such as in the case of cookies, HTML code, Java Scripts, etc.), but otherwise consent must be express. If the software meets certain spyware or malware criteria, then enhanced disclosure is required. Only express consent is valid under the anti-spyware provisions so this may have implications for online agreements such as web wrap agreements. One challenge will be determining the level of disclosure necessary based on the functionality of the software in question.

The new law also prohibits email harvesting, and altering transmission data to route a message to an unintended destination.

There are serious consequences to violating the law: fines of up to $10 million for corporations and $1 million for individuals. Liability extends to anyone who aids, induces or procures a prohibited act. Companies are vicariously liable for actions taken by their employees in the course of their duties. There is also a wide ambit for Officer and Director liability, including if they acquiesce to the prohibited act. Bill C-28 also grants a personal right of action to seek compensation and awards capped at $1 million per day for various violations and $1 million for each act of aiding, inducing, or procuring a breach, plus the daily liability. There is also a possibility of class actions.

Foreign companies should be aware that the Canadian law departs from anti-spam legislation in other countries in several ways. Since the anti-spam provisions apply to any commercial electronic message that is sent or received by a computer in Canada, foreign companies may attract liability under the new law.

Jennifer McKenzie, B.A., LL.B., is a partner with Bereskin & Parr LLP and heads the firm's Regulatory, Advertising & Marketing Practice group. She can be reached in Toronto at 416.957.1628 or jmckenzie@bereskinparr.com.

Catherine Lovrics, B.A, LL.B., is an associate lawyer in Bereskin & Parr LLP's Regulatory, Advertising & Marketing Practice group. She can be reached in Toronto at 416.957.1163 or clovrics@bereskinparr.com.

Peter Woods, is a Student-at-Law at Bereskin & Parr LLP, from the University of Western Ontario. He can be reached in Toronto at pwoods@bereskinparr.com.