Blakes
CANADIAN LAWYERS

CASL UPDATE: LESSONS LEARNED AND NEW RULES FOR SOFTWARE INSTALLATIONS

By Wendy Mee and Pei Li, Blake, Cassels & Graydon LLP

On July 1, most of the provisions of Canada's Anti-Spam Legislation, known as CASL, came into effect. CASL is regarded as one of the strictest anti-spam laws in the world, requiring prior consent for the sending of "commercial electronic messages" and requiring all such messages to comply with specific form and content requirements. As of October 2014, the Canadian Radio-television and Telecommunications Commission received over 120,000 complaints. This article focuses on enforcement efforts so far and discusses additional provisions regulating the installation of computer programs, which take effect January 15, 2015.

ENFORCEMENT OF CASL'S ANTI-SPAM PROVISIONS

In the first few months after Canada's Anti-Spam Legislation (CASL) took effect on July 1, 2014, the agency charged with its enforcement, the Canadian Radio-television and Telecommunications Commission (CRTC), received more than 120,000 complaints, including more than 1,000 in the first three days. Complaints can be submitted online or by email to the government's newly established Spam Reporting Centre (Centre) at www.fightspam.gc.ca. The Centre clearly states that not all submissions will be investigated. Rather, the information provided through the Centre will be used as an intelligence gathering tool and to identify enforcement targets.

Blakes
CANADIAN LAWYERS

On October 7, 2014, the CRTC made its first announcement regarding a completed investigation under CASL. Soon after the law took effect, the CRTC began receiving numerous complaints about spam messages that were being routed through a Saskatchewan-based Internet service provider (ISP), Access Communications. Preliminary investigations showed that the messages were actually coming from the server of a small computer reseller, which used Access Communications as its ISP. The server had become infected with malware, which had caused it to send millions of spam messages without the computer reseller's or Access Communication's knowledge. Once alerted to the problem, Access Communications and the computer reseller worked together to remove the malware. The CRTC did not fine either company in this instance.

While only a single investigation, this matter is an important piece of the puzzle as we try to understand what to expect from the CRTC in terms of enforcement. So far, the results appear positive for businesses that are attempting to comply with the law. Once alerted to the violation, the ISP and the computer reseller took swift steps to correct the situation and were not hit with an administrative monetary penalty (AMP). Those who have worried that the CRTC would come down hard on honest mistakes may be able to breathe a bit easier.

The CRTC continues to investigate complaints. Although each case may be different, the CRTC's first step in the investigation process appears to be issuing a Notice to Produce the following information and documentation:

- For every email address identified in the Notice, documentation on the method the email address was obtained, the kind of consent obtained, the nature of the relationship which supports such consent, and the date on which that consent was obtained.
- Policies and procedures for obtaining, recording and tracking consent for sending of CEMs.
- All templates used for CEMs sent during the period of time identified in the Notice.
- Policies and procedures for scrubbing email contact lists, including documentation on how the unsubscribe mechanism works.
- Documents with third parties who have sent CEMs on behalf the organization.
- Audited financial statements (or unaudited if audited statements are not available).
- Information relating to restrictions on use of assets, credit facilities, amounts due to or from owners or shareholders.

The organization may contest the Notice, but on limited grounds. The complaint(s) forming the basis of the investigation are not identified.

The first few requirements in the Notice are easy to understand. CASL stipulates prior consent (whether express or implied) to send a CEM, so being able to demonstrate the method, kind and date of consent from each recipient makes sense, as does the nature of the relationship between the sender and recipient since consent to send CEMs is implied in respect of certain relationships.

The request for information relating to policies and procedures is also understandable because CASL allows for a due diligence defense. Having appropriate policies and procedures in place to ensure compliance with CASL may support such a defense. Similarly, appropriately drafted CEM templates may demonstrate due diligence on the part of the organization.

Contracts with third parties can also be used to show that the organization exercised due diligence, for example, by ensuring that all email service providers were aware of and agreed to comply with CASL. These contracts may also be useful to the CRTC in its investigation, as they may allow the CRTC to follow a path to the source of an issue. As an example, understanding the relationship between Access Communications and the Saskatchewan-based computer reseller led the CRTC to find the root of the problem in the CRTC's first announced completed investigation discussed above.

While it may be surprising that the CRTC requests financial statements and asset restrictions, AMPs under CASL are to be based (at least in part) on the organization's ability to pay. This information may be being requested as background to determine the amount of the AMP, should one be levied.

Organizations would be well advised to ensure that if requested, they would be able to provide the requested information and documentation noted above.

COMPUTER PROGRAMS PROVISIONS TO TAKE EFFECT

On January 15, 2015, CASL's provisions regulating the installation of computer programs will take effect. Though the main intent of these provisions is to fight bots, viruses and other malware, given the broad scope of the legislation, the prohibition has potentially wide implications for legitimate businesses. As a result, many businesses (including those outside of the software industry) will need to review their practices and develop compliance strategies in order to comply with these provisions.

Subject to limited exceptions, the computer programs provisions of CASL prohibit installing, or causing to be installed, a computer program (including any updates or upgrades) on any other person's computer system, in the course of commercial activity, without the express consent of the owner or authorized user.

As with CASL's anti-spam provisions, express consent must be obtained in the prescribed manner and any request for express consent must provide certain information. Additional enhanced disclosure requirements will apply if the person seeking consent to install the computer program knows and intends that the program will cause the computer system to operate in a manner that is contrary to the reasonable expectations of the owner or authorized user and the computer program performs one or more prescribed functions (for example, collects personal information stored on the computer system, interferes with the owner's or an authorized user's control of the computer system, or causes the computer system to communicate with another computer system or device without the authorization of the owner or an authorized user of the computer system).

Express consent is not required for an update or upgrade to a computer program that was installed with express consent provided the person who gave the consent is entitled to receive the update or upgrade under the terms of the express consent previously given and the update or upgrade is installed in accordance with those terms. Note that this does not apply if the update or upgrade involves a computer program that performs a function for which enhanced notice would be required. CASL's transitional provision also provides that if a computer program was installed before January 15, 2015, consent to the installation of an update or upgrade to the program is implied until the earlier of January 15, 2018, or when the person gives notification that they no longer consent to such installation.

Express consent is deemed to have been obtained if the computer program falls under a prescribed category (for example, a cookie, HTML code, operating system, program necessary to correct a failure in the operation of the computer system) and the person's conduct is such that it is reasonable to conclude that they consent to the program's installation.

The potential penalties for non-compliance under CASL are substantial and include administrative monetary penalties of up to C$1-million for individuals and C$10-million for other persons. Provisions creating a private right of action under CASL will come into force on July 1, 2017.

On November 10, 2014, the CRTC posted its first substantive guidance on the computer programs provisions of CASL, which provide some insight into the CRTC's interpretation of these provisions. For example, there has been much speculation about when software is considered to be installed or caused to be installed on another person's device. In response, the CRTC has indicated that CASL does not apply to self-installed software (e.g. when a person downloads software from a website or app store or installs software using a CD or DVD). However, if the software subsequently installs an update without prompting from the user, CASL would apply. Furthermore, if the software contains a concealed program that is automatically executed when the software is installed, CASL will apply. While these guidance materials provide clarity on some key issues, much uncertainty still remains regarding the application and enforcement of the computer programs provisions.

CONCLUSION

In some ways, the six months since CASL came into effect seemed action-packed, with a massive number of complaints filed. In other ways, little is known about the CRTC's enforcement priorities since the CRTC only made a public announcement regarding one completed investigation. However, that investigation did deliver some good news about the CRTC's attitude—at least toward cooperative organizations and inadvertent misdeeds. With additional provisions taking effect in January 2015, many in the technology industry are waiting to see whether a similar attitude will be taken with respect to enforcement of CASL's computer programs provisions.

ABOUT THE AUTHORS

Wendy Mee and Pei Li, Blake, Cassels & Graydon LLP

WENDY MEE is an associate in the Blakes Toronto office. She practices primarily in the area of privacy law, where she advises a wide range of clients, including those in the life sciences, financial services, education, retail, food and consumer goods sectors, on a variety of privacy and data protection issues. Wendy also advises clients on marketing and advertising issues generally, including in respect to Canada's Anti-Spam Legislation, the CRTC's do not call rules, misleading advertising and contests and promotions.

PEI LI is an associate in the Blakes Toronto office. Her practice focuses on health, drugs, marketing and advertising regulatory matters, as well as privacy and access-to-information law. She advises clients on such matters as product labelling, food and consumer product law, drug and medical device regulation and promotional contests. Pei also helps clients understand and comply with Canada's Anti-Spam Legislation.

ABOUT THE FIRM

As one of Canada's top business law firms, Blake, Cassels & Graydon LLP (Blakes) provides exceptional legal services to leading businesses in Canada and around the world.