

CASL-READY

by J. Andrew Sprague, Associate, Miller Thomson LLP

2015-06-01, canadianunderwriter.ca

The country's regulators are taking corrective actions and issuing penalties related to Canada's Anti-Spam Legislation, which took effect last July. The serious consequences arising from breaching related requirements, though, make clear that companies need to take steps to develop corporate compliance programs.

On July 1, 2014, the anti-spam provisions of Canada's Anti-Spam Legislation, known as CASL, became enforceable law. Several months later - on January 1, 2015 - CASL's installation of computer program provisions became enforceable law. They regulate the unsolicited installation of computer programs, including mobile applications for smartphones and smart devices.

CASL applies to more than just those types of messages that one might traditionally consider to be "spam" and its anti-spam provisions have broad application, applying to more than just email messages. As well, the definition of "commercial" under CASL, as it applies to commercial electronic messages, is very broad and catches many activities that might not readily come to mind.

CASL also regulates the following additional activities:

- the altering of transmission data in electronic messages;
- engaging in fraudulent or misleading practices through electronic messages or websites;
- the automated collection of electronic addresses (email harvesting) and subsequent uses; and
- the unauthorized use of computers to collect personal information and subsequent uses.

A simple reading of the legislation will not disclose everything that one needs to know about this new law. The interpretation guidance, both verbal and written, provided by CASL's regulators is an important component in understanding obligations under the law.

SHOULD CASL BE TAKEN SERIOUSLY?

In 2014, many individuals and organizations speculated whether CASL was just another "Y2K" or if it would become like the perceived unenforced National Do Not Call List (DNCL) and the Unsolicited Telecommunications Rules. Is CASL something they really need to worry about?

In 2015, the answer is CASL is, indeed, something that individuals and organizations should be concerned about and with which they should be compliant.

ENFORCEMENT ACTION

This past March 5, the Canadian Radio-television and Telecommunications Commission's (CRTC) chief compliance and enforcement officer issued a Notice of Violation to a Quebec company, which included a \$1.1 million penalty for violating CASL. The company had sent commercial electronic messages to recipients without their consent, as well as emails in which the unsubscribe mechanisms did not function properly. The imposed penalty - the first issued by the CRTC pursuant to its authority under CASL - was based on four alleged violations.

Three weeks later, on March 25, the CRTC announced that a company that operates a user-driven website had paid a penalty of \$48,000 as part of an undertaking for an alleged CASL violation.

It is alleged the company sent commercial emails to registered users of its website with an unsubscribe mechanism that was not clearly and prominently set out, and which could not be readily performed, as required by CASL.

And on March 11, the Competition Bureau announced it has taken action against two of Canada's largest rental car companies, alleging that the companies have engaged in deceptive marketing practices relating to false or misleading price representations. The bureau is seeking both \$30 million in administrative monetary penalties (AMPs) and refunds for consumers.

The action marks the bureau's first proceedings under the new provisions of the Competition Act that came into force on July 1, 2014 as part of CASL. It is reported the companies used electronic messages to disseminate the alleged false or misleading representations.

Notwithstanding the false perception that the CRTC is not enforcing the DNCL and the Unsolicited Telecommunications Rules, the commission is, indeed, engaged in enforcement and is actively issuing related monetary penalties. Like CASL, compliance in this area is also highly recommended.

PENALTIES AND CONSEQUENCES

Individuals or organizations that do something for which CASL requires consent - and they do so without the appropriate consent or they cannot rely upon an exemption - could be subjected to a number of significant consequences and penalties.

These include the following:

- AMPs of as much as \$1 million per violation for individuals and \$10 million per violation for any other person (i.e., any legal entity that is not an individual);
- corporate officers, directors and agents may be held personally liable for corporate violations;
- vicarious liability may arise for violations committed by employees or agents;
- private right of action, starting July 1, 2017, including class-action lawsuit risk; and
- reputational risk.

CASL COMPLIANCE STRATEGIES

A due diligence defence is available under CASL against claims of non-compliance. In 2014, the CRTC issued guidelines to help businesses develop corporate compliance programs, the stated purpose of which is to provide general guidance and best practices on the development of corporate compliance programs to facilitate compliance with CASL, and also the CRTC's Unsolicited Telecommunications Rules.

The CRTC acknowledges in the compliance guidelines no two organizations are the same and that every organization has different risks. As a result, compliance programs will vary depending on the size of an organization, its risk profile and its available resources.

In the guidelines, the CRTC expressly states the following:

Commission staff may take into consideration the existence and implementation of an effective corporate compliance program if the business presents the program as part of a due diligence defence in response to an alleged violation of the Rules or CASL. Although the pre-existence of a corporate compliance program may not be sufficient as a complete defence to allegations of violations under the Rules or CASL, a credible and effective documented program may enable a business to demonstrate that it took reasonable steps to avoid contravening the law. Thus, the program may support a claim of due diligence.

As well, Commission staff can take the existence of such a program into consideration when determining whether a violation of the Rules or CASL is an isolated incident or is systemic in nature, and whether sanctions against a business should include AMPs.

If individuals and organizations take proactive steps to establish appropriate policies, procedures and processes relating to activities prohibited under CASL - as well as properly enforce them - such individuals and organizations may be able to use their efforts as an aid to a due diligence defence. In addition, such efforts may be a factor in determining liability or damage awards arising out of a CASL non-compliance claim.

Given the potential for serious consequences under CASL, developing a corporate compliance program, if one has not already been developed, should be on any company's "to do" list, especially in light of the CRTC's aforementioned comments and the fact that the CRTC is clearly enforcing CASL.



YOUR ACCESS TO JUSTICE

Unsure about CASL's requirements or if all your electronic messages are CASL compliant?

DAS offers a comprehensive insurance solution to business owners trying to manage their CASL legal risk. Among other common business legal issues, the *DASbusiness* solution covers legal expenses to respond to alleged CASL violations. It also gives you unlimited access to DAS's telephone legal advice helpline, a toll-free advice line available 24/7, which allows you to prevent or reduce potential exposure to litigation.

Contact your DAS Broker Consultant today!

www.das.ca