Bulletin | Cybersecurity, Privacy and Data Protection

January 2020

Canada's Anti-Spam Legislation – 2019 Year in Review

In 2019, the Canadian Radio-television and Telecommunications Commission continued to enforce Canada's Anti-Spam Legislation (commonly known as "CASL") and issue guidance for CASL compliance.

CASL

CASL creates a comprehensive regime of offences, enforcement mechanisms and potentially severe penalties designed to prohibit the sending of unsolicited or misleading commercial electronic messages ("CEMs"), the unauthorized commercial installation and use of computer programs on another person's computer system and other forms of online fraud.

For most organizations, the key parts of CASL are the rules for CEMs. Subject to limited exceptions, CASL creates an opt-in regime that prohibits the sending of a CEM unless the recipient has given consent (express or implied in limited circumstances) to receive the CEM and the CEM complies with prescribed formalities (i.e. information about the sender and an effective and promptly implemented unsubscribe mechanism) and is not misleading.

CASL also prohibits, subject to limited exceptions, the installation and use of a computer program on another person's computer system, in the course of a commercial activity, without the express consent of the owner or authorized user of the computer system. The computer program rules apply to almost any computer program (not just malware, spyware or other harmful programs) installed on almost any computing device (including mobile phones) as part of a commercial activity (regardless of expectation of profit).

CASL imposes liability not only on an organization that directly violates CASL (e.g. by sending a prohibited CEM or installing a prohibited computer program), but also on an organization that causes or permits a CASL violation, or who aids, induces or procures a CASL violation. CASL also provides that an organization is vicariously liable for CASL violations by its employees and agents (e.g. digital marketing service providers) within the scope of their employment or authority, and corporate directors and officers are personally liable if they direct, authorize or assent to, or acquiesce or participate in, a CASL violation. Organizations, directors and officers might avoid liability if they exercise due diligence to prevent the CASL violation.

CASL violations can result in potentially severe administrative monetary penalties – up to $10 million per violation for an organization and $1 million per violation for an individual – in regulatory enforcement proceedings. CASL includes a private right of action that is not in force.

The Canadian Radio-television and Telecommunications Commission ("CRTC") is responsible for enforcing CASL's rules regarding CEMs and computer programs, and has various enforcement tools for that purpose. Since CASL came into force in 2014, the CRTC has taken enforcement action against organizations and individuals who have violated CASL, and has issued enforcement decisions and accepted voluntary undertakings (settlements).

Regulatory Enforcement

- **CEO Liable for Company's CASL Violations:** On April 23, 2019, the CRTC issued a decision imposing a $100,000 administrative penalty against the President/CEO of a corporation known as "nCrowd" for CASL violations (i.e. sending promotional emails without the recipients' consent and without a properly functioning unsubscribe mechanism) committed by nCrowd and its subsidiaries. The CEO was held personally liable because he "acquiesced", which the CRTC interpreted to mean "agreeing to something tacitly, silently, passively, or without protest", in nCrowd's CASL violations. No order was made against nCrowd because it had been dissolved. (more information)
- **Notice of Violation for Aiding Malware Distribution:** On December 10, 2019, the CRTC issued a notice of violation imposing penalties totalling $115,000 against two individuals operating a partnership known as "Orcus Technologies" for allegedly developing, selling and promoting malware known as "Orcus RAT", which enables hackers to install the program and take control of a victim's computer without their knowledge or consent. In addition, one of the individuals operated a dynamic domain name server service used by hackers to install malware on computer systems and to communicate with the infected computer systems in Canada and abroad. (more information)

Regulatory Guidance

- **Social WiFi:** In August 2019, the CRTC issued *Enforcement Advisory – Notice for businesses collecting customer data with in-store WiFi* to explain the "Social WiFi" business model, and remind businesses and consumers of CASL requirements for sending marketing messages to individuals who subscribe to Social WiFi.
- **Web Hosting Providers:** In October 2019, the CRTC issued *Enforcement Advisory – Notice for Web Hosting Service Industry* to remind web hosting providers and operators of other networked infrastructure that they must not contravene CASL by aiding, inducing, procuring or causing to be procured the distribution of malware, and to encourage those organizations to exercise due diligence and establish a CASL compliance program.

For more information about CASL, see BLG bulletins *CASL – Year in Review 2018*, *CASL – Year in Review 2017*, *CASL – Year in Review 2016* and *CASL – Year in Review 2015*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

blg.com | Canada's Law Firm
Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.

This document provides general information only, and does not constitute legal or other professional advice. Readers are encouraged to obtain legal advice from a competent professional regarding their particular circumstances.

© 2020 Borden Ladner Gervais LLP. BD9496–01–20

Borden Ladner Gervais