DECEMBER 2018

CASL BULLETIN

Borden Ladner Gervais

CRTC Issues Guidance for Avoiding Indirect Liability for CASL Violations

In November 2018, the Canadian Radio-television and Telecommunications Commission ("CRTC") issued an *Information Bulletin* regarding *Canada's Anti-Spam Legislation* (commonly known as "CASL"). The Bulletin indicates that the CRTC is taking an aggressive approach to the interpretation of the CASL provision that imposes liability on persons who "aid, induce, procure or cause to be procured" a CASL violation. The Bulletin explains that businesses that provide products or services that could be used to commit CASL violations must implement proactive measures to prevent identified risks, even if that means going beyond industry standards.

CASL

CASL creates a comprehensive regime of offences, enforcement mechanisms and potentially severe penalties designed to prohibit: (1) sending, or causing or permitting to be sent, unsolicited commercial electronic messages ("CEMs") without consent (express or implied) or compliance with prescribed formalities; (2) altering, or causing to be altered, transmission data in an electronic message, in the course of a commercial activity, without express consent; and (3) installing, or causing to be installed, a computer program on another person's computer system, or using the computer program to send an electronic message, without express consent. CASL imposes liability not only on persons who directly commit a CASL violation, but also on persons who "aid, induce, procure or cause to be procured" a 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, which is not in force.

The CRTC is primarily responsible for enforcing CASL, 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).

In December 2017, the House of Commons Standing Committee on Industry, Science and Technology recommended changes to CASL to clarify the scope and application of CASL and to reduce the cost of compliance and better focus enforcement. The government has indicated an intention to make some clarifying amendments to CASL.

Past Enforcement Action for Indirect CASL Violations

The CRTC has taken enforcement action against organizations and individuals based on indirect or vicarious liability for CASL violations committed by other persons:

- **Liability for Aiding the Distribution of Malvertising:** In July 2018, the CRTC issued notices of violation imposing administrative monetary penalties against two online advertising businesses for allegedly aiding their customers' installation of malicious computer programs through the distribution of online advertising. The businesses allegedly adopted practices that permitted and encouraged anonymity by their customers, formed relationships with customers known for distributing malvertising, and failed to implement safeguards after they were warned that their services were being used to distribute malvertising.
- **CEO Personal Liability for Non-compliant CEMs:** In June 2017, the CRTC accepted a voluntary undertaking by a group of companies and their chief executive officer to settle alleged CASL violations for sending CEMs without the recipients' consent and without a compliant unsubscribe mechanism. The CRTC alleged that the chief executive officer was personally liable for the CASL violations committed by his companies.
- **Organization Liability for CEMs sent by Service Providers:** In September 2016, the CRTC announced a voluntary settlement with an organization regarding the alleged sending of unlawful CEMs by the organization and its service providers.

CRTC's Approach to Section 9

CASL section 9 provides that "it is prohibited to aid, induce, procure or cause to be procured" a violation of CASL's rules for sending CEMs, altering transmission data in a message, or installing and using computer software on another person's computer.

In November 2018, the CRTC issued *Compliance and Enforcement Information Bulletin CRTC 2018-415* titled "Guidelines on the Commission's approach to section 9 of Canada's anti-spam legislation (CASL)" for the stated purpose of providing general compliance guidelines and best practices regarding CASL section 9. The Bulletin explains the CRTC's approach to section 9, includes examples of organizations to whom section 9 could apply and activities that could result in non-compliance, and provides guidance for organizations seeking to manage associated risks.

Following is a summary of key aspects of the Bulletin:

- **Application:** Section 9 may apply to individuals and organizations that facilitate electronic commerce by providing enabling services, technical or otherwise, used to commit a CASL violation, and may also apply to individuals and organizations who "receive direct or indirect financial benefit from" a CASL violation. The Bulletin include a non-exhaustive list of "intermediaries" that might be liable under CASL section 9: advertising brokers, electronic marketers, software and application developers, software and application distributors, telecommunications and internet service providers and payment processing system operators.
- **Considerations:** The CRTC will consider various factors when assessing the potential section 9 liability of an individual or organization for a CASL violation committed by another person, including: (a) the level of control the individual or organization had over the violation, and the extent to which they had the ability to prevent or stop the violation; (b) the degree of connection between their actions and the violation; and (c) whether they took reasonable steps, including precautions and safeguards, to prevent or stop the violation.
- **Strict Liability:** An individual or organization may be liable for violating CASL section 9 "even if they did not intend to do so or were unaware that their activities enabled or facilitated" CASL violations by other persons. The Bulletin explains: "While awareness of violations may be a factor when assessing section 9 violations, it is not necessary to be found liable...Businesses are expected to understand the non-compliance risks associated with the nature of their respective industries and take certain precautionary measures to mitigate those risks, thereby reducing their potential liability under section 9 of CASL."
- **Examples:** A person may violate CASL section 9 by giving assistance to or enabling another person to commit a CASL violation (e.g. by providing access to tools or equipment necessary to commit the violation or by facilitating the violation by giving technical assistance or advice). The Bulletin includes examples of potential violations of CASL section 9: (a) an online marketing services company provides a messaging template that does not include required sender information or an unsubscribe mechanism and does not ensure that individuals consented to be on its mailing lists; (b) a web hosting services company does not include CASL compliance obligations in its terms of service, or have a process for ensuring CASL compliance, and does not take action to stop CASL violations after being alerted to the violations; and (c) an online app store operator fails to stop the distribution of an app that has undisclosed functionalities (e.g. push advertisements) and is installed without proper express consent after receiving complaints about the app.
- **Due Diligence:** CASL section 33 provides that an individual or organization will not be liable for a CASL violation if they establish that they exercised due diligence to prevent the commission of the violation. Organizations may demonstrate due diligence by having documented measures in place to mitigate non-compliance risks, but a "set it and forget it" CASL compliance program is not sufficient. Organizations must establish suitable compliance measures tailored to relevant CASL risks, and take reasonable steps (including ongoing management and active oversight) to ensure the effective operation of the compliance measures. Organizations should "take steps to maintain a high standard of awareness and take decisive, prompt, and continuing action to prevent CASL violations from occurring, or to stop them once identified".
- **CASL Compliance Program:** The Bulletin encourages individuals and organizations to implement "a robust compliance program" that is suitable for identified risks based on all relevant circumstances. The Bulletin includes examples of recommended components of a CASL compliance program: regular threat and risks assessments; validating client identities; implementing written agreements that require clients to comply with CASL; auditing clients' use of services, and reporting possible CASL violations to relevant authorities; and taking prompt measures to respond to CASL violations and to prevent similar violations from occurring in the future. The Bulletin cautions that "simply following industry standards may be insufficient", and that steps must be taken to address identified threats and vulnerabilities "even if that means going beyond industry standards".

Comment

The Bulletin is an important reminder that CASL imposes liability not only on persons who directly commit a CASL violation, but also persons who cause or contribute to a CASL violation by aiding, inducing or procuring the violation, including by providing products and services used to commit the violation.

The Bulletin indicates that the CRTC is taking an aggressive approach to CASL section 9. The Bulletin explains the CRTC's view that CASL section 9 imposes strict liability on persons who "aid, induce, procure or cause to be procured" a CASL violation, and that businesses that provide products or services that could be used to commit CASL violations must implement proactive measures to identify and prevent risks, even if that means going beyond industry standards. In many circumstances, compliance with the Bulletin's recommended due diligence practices might be burdensome, costly and impracticable.

Some of the concerns arising from the Bulletin might be addressed through clarifying amendments to CASL made in response to recommendations by the House of Commons Committee. In the meantime, businesses that provide products or services that could be used to commit CASL violations should consider revising their CASL compliance programs to be consistent with the Bulletin and previous CRTC guidance. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's national CASL Group includes lawyers, located in BLG's offices across Canada, with expertise in CASL, privacy law, cyber risk management and class action litigation. We provide both proactive CASL compliance advice and legal advice to help respond to a CASL contravention. Additional information about BLG's national CASL Group and our services is available at blg.com/CASL.

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com