NOVEMBER 12, 2018

Whose Liability Is It Anyway? CRTC Issues New Guidance Regarding Liability for Aiding or Inducing CASL Non-Compliance

Authors: Zain Rizvi, Anita Banicevic and David Feldman

Perhaps the most controversial feature of Canada's anti-spam legislation (CASL)[1] is its broad approach to liability for various actors and intermediaries involved in electronic communications. As we have previously explained, persons may be liable under CASL if they "cause" or "permit" a violation of sections 6 to 8 of CASL (which prohibit, respectively, sending commercial electronic messages that fail to comply with certain form and consent requirements, altering transmission data in an electronic message without consent and installing computer programs without consent). In addition, section 9 of CASL prohibits any person from "aiding or inducing" others to engage in conduct that violates these provisions.

On November 5, 2018, the Canadian Radio-television and Telecommunications Commission (CRTC) issued Compliance and Enforcement Information Bulletin 2018-415 (the Bulletin), providing guidance regarding the CRTC's interpretation of section 9. The CRTC takes an expansive view of the provision's scope as a critical component of the CASL compliance ecosystem. From a practical perspective, the CRTC's position regarding the scope of liability under section 9 of CASL creates significant compliance burdens and challenges for businesses involved in digital marketing or communications in Canada. While the Bulletin provides the CRTC's perspective as to the scope of potential liability for the actions of third parties under CASL, this approach has yet to be endorsed or adopted by any court.

Key Aspects of the CRTC's Bulletin

The Bulletin sets out the following five key points:

1. **Section 9 can apply to almost any intermediary or provider of digital products or services.** The CRTC's position is that section 9 can apply to a wide range of individuals and organizations "facilitating commercial activity, by electronic means, by providing enabling services, technical or otherwise," as well as to "those who receive direct or indirect financial benefit from a violation of sections 6 to 8 of CASL." The Bulletin's "non-exhaustive list" of intermediaries that may be at risk of liability includes advertising brokers, electronic marketers, software and app developers and distributors, telecommunications and Internet service providers, payment processing system providers and web hosting service providers.

2. **Section 9 liability does not require intent to aid in or knowledge of the contravention of CASL.** The Bulletin states that individuals and organizations "engaging in regulated activities, such as those relating to electronic commerce" are responsible for ensuring that their actions or omissions are not aiding or inducing a third party to violate sections 6 to 8 of CASL. For example, a provider of online mass marketing services may be liable under section 9 if its messaging template does not include sender information or a CASL-compliant unsubscribe mechanism. Similarly, a provider of web hosting services may be liable for a fake banking website used to carry on a phishing campaign using its servers.

3. **Liability and enforcement action regarding potential section 9 violations will be assessed in light of several factors.** According to the Bulletin, when assessing potential section 9 liability, the CRTC will consider (i) the level of control the aiding party has over the conduct that violates sections 6 to 8, including its ability to prevent the conduct; (ii) the degree of connection between the actions taken by the aiding party and those that contravene sections 6 to 8 (e.g., merely selling a computer, which is then used

to violate CASL, indicates a weak connection, whereas distributing malicious software for use may suggest a stronger connection); and (iii) evidence that reasonable steps were taken to prevent or stop violations from occurring. Following a determination that a section 9 violation has occurred, the CRTC's choice of enforcement action will typically be based on considerations such as (i) the likely effect of such action on compliance; (ii) the nature and scope of the violation; (iii) the degree of harm associated with the violation; (iv) the level of cooperation by the alleged violator; and (v) any history of prior violations.

4. **A due diligence defence is available but may be difficult to establish.** Section 33 of CASL provides that an individual or organization will not be found liable for a CASL violation if it establishes that it exercised due diligence to prevent the commission of the violation. However, the Bulletin contemplates an extremely high standard for due diligence in the section 9 context. The Bulletin provides that the adoption of well-documented "reasonable steps" to prevent, detect and remediate potentially offending conduct engaged in by third-party clients would be required, including (i) validating clients' identities and researching their reputations and avoiding doing business with those seeking total anonymity; (ii) reviewing the products or services of potential clients for CASL compliance; (iii) auditing existing clients' use of services; (iv) allocating resources to take down threats, to address security vulnerabilities and to implement changes in a timely manner to prevent similar future threats; and (v) assisting users whose devices and accounts have been compromised.

5. **Industry compliance standards may not be good enough.** Perhaps most surprisingly, the Bulletin states that it expects intermediaries to engage in compliance steps that may surpass industry-accepted standards where necessary: "Simply following industry standards may be insufficient. Where a threat or vulnerability has been identified, steps should be taken to address it, even if that means going beyond industry standards."

The CRTC's view appears to be that section 9 requires intermediaries and other suppliers of products or services that may be used to violate CASL to ensure that their clients do not engage in improper conduct, failing which they may be held liable. The consequences of non-compliance may be significant, as violations of section 9 are subject to the same administrative penalties as violations of sections 6 to 8 (and, with the enactment of further regulations in the future, may one day include the possibility of significant administrative monetary penalties that may be assessed on a daily basis).

It is worth noting that the prospect of liability under section 9 of CASL is not merely theoretical. In July 2018, the CRTC issued a Notice of Violation to an advertising network broker and its related provider of real-time bidding services after concluding that the broker's customers had used the broker's systems to install "malvertising" in contravention of section 8 of CASL. While the facts in that case were egregious, the Bulletin confirms that the CRTC does not intend that the application of section 9 be limited to cases of deliberate or flagrant non-compliance.

Implications

The Bulletin raises significant questions about the burden and practicality of the CRTC's compliance expectations and possible liability for legitimate businesses engaged in digital communications in Canada. The CRTC's approach to this issue is surprising given recently expressed stakeholder concerns regarding the costs and burdens of CASL compliance. We expect that the CRTC's Bulletin will create renewed concerns and possible calls for further clarity and the need for legislative amendments to CASL.

For the time being, businesses involved in the provision of digital communications in Canada should consider reviewing their compliance processes (including in respect of third parties and clients) and take proactive steps where any compliance deficiencies arise in order to avoid the risk of CASL liability.

[1] CASL refers to *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23, and its associated regulations.

Key Contacts: Anita Banicevic, Elisa K. Kearney and Elliot A. Greenstone

This information and comments herein are for the general information of the reader and are not intended as advice or opinions to be relied upon in relation to any particular circumstances. For particular applications of the law to specific situations the reader should seek professional advice.

© 2024 DAVIES WARD PHILLIPS & VINEBERG LLP