Compliance and Enforcement Information Bulletin CRTC 2018-415

PDF version

Ottawa, 5 November 2018

Guidelines on the Commission's approach to section 9 of Canada's anti-spam legislation (CASL)

Introduction

- 1. The purpose of this information bulletin is to provide general compliance guidelines and best practices for stakeholders with respect to section 9 of Canada's anti-spam legislation (CASL). Specifically, this bulletin discusses the Commission's general approach to section 9 of CASL and provides examples of parties to whom section 9 of CASL may apply, activities that could result in non-compliance, and measures for managing associated risks. This bulletin builds on previous guidance and best practices outlined in Compliance and Enforcement Information Bulletin 2014-326.²
- 2. The information and guidance presented in this bulletin are guidelines only, and are not intended to be exhaustive. Further, the content of this bulletin is not intended to serve as legal advice. Those seeking legal advice regarding compliance with CASL should retain independent counsel.
- 3. The Commission recognizes that each organization is different. Depending on the size of the organization, its overall risk exposure, and the nature of the risks to be mitigated, measures to ensure compliance with CASL may vary, particularly in the case of small- to medium-sized businesses. The Commission will assess measures taken to ensure compliance on a case-by-case basis and recommends that each business adapt its own risk management and compliance strategies, including those described below, to its particular circumstances and the specific risks at hand.

Key definitions and interpretation

4. Section 9 of CASL states

It is prohibited to aid, induce, procure or cause to be procured the doing of any act contrary to any of sections 6 to 8.

² Other related documents are Compliance and Enforcement Information Bulletins 2012-548 and 2012-549.



¹ CASL, also commonly referred to as "Canada's anti-spam legislation," 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 Radiotelevision and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23, and the associated regulations made thereunder.

Section 9 of CASL addresses ways in which persons may contribute to contraventions of sections 6 to 8 of CASL without committing the violations directly. Section 9 of CASL identifies four ways in which these contributions may be made: by aiding, inducing, procuring, or causing to be procured. The Commission will consider the facts of each case to determine whether a person has violated one or more of the elements of section 9 of CASL. As an example, a person may contravene section 9 of CASL by giving assistance to or enabling a third party to carry out violations of sections 6 to 8 of CASL. This may take the form of providing access to the tools or equipment necessary to commit a violation. Alternatively, it may involve facilitating a violation by giving technical assistance or advice.

- 5. By contrast, violations of sections 6 to 8 of CASL typically involve a direct action related to
 - sending, causing, or permitting to be sent, commercial electronic messages (CEMs) without express or implied consent [paragraph 6(1)(a)] (e.g. email, short messaging service (SMS), or messages to any other electronic address);
 - altering, or causing to be altered, transmission data in electronic messages, in the course of a commercial activity,³ without express consent [paragraph 7(1)(a)] (e.g. unwanted redirection or phishing); and
 - installing, or causing to be installed, a computer program on another person's computer in the course of a commercial activity without express consent; or having so installed or caused to be installed a computer program, cause an electronic message to be sent [paragraph 8(1)(a)] (e.g. malware, viruses, and botnets).

Who does section 9 of CASL apply to?

- 6. CASL applies to all individuals and organizations who use electronic means to carry out commercial activities in or from Canada, or offer their products or services to Canadians. Section 9 of CASL may apply to individuals and organizations facilitating commercial activity, by electronic means, by providing enabling services, technical or otherwise. Section 9 of CASL could also apply to those who receive direct or indirect financial benefit from a violation of sections 6 to 8 of CASL. While not exhaustive, the following list features examples of intermediaries that may engage in activities placing them at risk of non-compliance with section 9 of CASL:
 - Advertising brokers

³ CASL defines "commercial activity" as any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, whether or not the person who carries it out does so in the expectation of profit, other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada.

- Electronic marketers
- Software and application developers
- Software and application distributors
- Telecommunications and Internet service providers⁴
- Payment processing system operators

Potential for violation

- 7. 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.
- 8. When assessing the role individuals, businesses, or other entities play in potential section 9 violations, the Commission will consider a variety of factors. These include, but are not limited to.
 - the *level of control* that an individual or organization has over the activity that violates sections 6 to 8 of CASL, and the extent to which they have the ability to prevent or stop that activity (as required by the situation);
 - the *degree of connection* between the actions that could constitute a violation of section 9 of CASL, and those that contravene sections 6 to 8 of CASL. For example, selling a computer, which is then used to commit an unlawful activity, would not create a strong degree of connection between parties. However, selling malicious software to unsuspecting parties would suggest a stronger degree of connection; and
 - evidence that *reasonable steps* were taken, including precautions and safeguards to prevent or stop violations from occurring.

⁴ While subsection 6(7) of CASL provides that section 6 of CASL (relating to CEMs) does not apply to a telecommunications service provider merely because the service provider provides a telecommunications service that enables the transmission of a message, the same exception does not apply to sections 7 to 9 of CASL. There is an expectation that service providers enact prevention strategies and other safeguards to reduce their potential direct or indirect role in contraventions of CASL.

Examples – Potential violations of section 9 of CASL

Example 1

Company A specializes in online marketing and sells a bundle of services to Company B, which includes a messaging template and a collection of email addresses and mobile phone numbers for the purpose of mass marketing. The messaging template does not include sender identification information or an unsubscribe mechanism, and no attempt has been made to ensure the express or implied consent of the persons whose contact information appears on the list, all of which are required under section 6 of CASL. In this scenario, Company B may be in violation of section 6 of CASL if it uses the messaging template and contact lists provided by Company A to send commercial electronic messages (e.g. email or SMS). Even though Company A is not the sender of the messages, it could be violating section 9 of CASL by providing the tools that were used to violate section 6 of CASL.

Example 2

Company A offers web hosting services. Its client, Company B, uses Company A's services to launch a phishing campaign that redirects unsuspecting Canadians to a fake banking website created to obtain their personal data – a violation of section 7 of CASL. Company A was alerted to the malicious activity by a cyber security firm, but took no action to stop it. In addition, there is no statement in its web hosting terms of service requiring clients to be compliant with CASL, nor does it have processes to ensure compliance. Therefore, while it was Company B that launched the phishing campaign, Company A may be responsible pursuant to section 9 of CASL for having "aided" the doing of the section 7 violation.

Example 3

An individual visits an online app store and downloads a video game, which comes bundled with a custom browser toolbar. Not all toolbar functions, such as the pushing of advertisements, are described during the installation process, and consent for the toolbar is sought through a pre-checked box – contrary to the requirements of section 8 of CASL. During an investigation, it is determined that several customers had previously complained to the online app store about the toolbar. Although the video game developer may be the responsible party for a section 8 violation, the online app store may have violated section 9 of CASL for having "aided" the doing of the section 8 violation.

Caveat: While awareness of violations may be a factor when assessing section 9 violations, it is not necessary to be found liable. Determination of section 9 violations will depend on the exact context and circumstances surrounding each case.

Managing risks for compliance

Know your liabilities

- 9. With regard to strict liability violations, it is possible for an individual or organization to be held liable and face administrative monetary penalties for violating section 9 of CASL, even if they did not intend to do so or were unaware that their activities enabled or facilitated contraventions of sections 6 to 8 of CASL by a third party. When engaging in regulated activities, such as those relating to electronic commerce, individuals and organizations must comply with the associated legislative and regulatory requirements. With respect to section 9 of CASL, compliance includes ensuring that an individual's or organization's actions and/or omissions are not aiding or inducing a third party to violate sections 6 to 8 of CASL.
- 10. When issuing a notice of violation, the designated person⁵ is required to prove that the actions or omissions of the party resulted in a violation of section 9 of CASL. Pursuant to section 33 of CASL, however, an individual or organization will not be found liable if they establish that they exercised due diligence to prevent the commission of the violation.

Due diligence

- 11. The most effective way to demonstrate due diligence is to ensure that measures are in place to mitigate non-compliance risk. Individuals and 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. A 'set it and forget it' compliance program or policy is an ineffective strategy. The key to due diligence is not just establishing a proper system to prevent the occurrence of violations, but, more fundamentally, taking reasonable steps to ensure the effective operation of the compliance measures, such as through ongoing management and active oversight, including audits and the monitoring of activities carried out by third parties. Further, compliance measures should not be generic in nature, but should instead specifically address identified non-compliance risks.
- 12. Individuals and organizations engaged in electronic commerce should seek legal and other expert advice⁶ to ensure they fully understand their rights, responsibilities, risks, and liabilities under CASL.

⁵ Pursuant to section 14 of CASL, for the purposes of any of sections 15 to 46 of CASL, the Commission may designate persons or classes of persons appointed under section 8 of the <u>Canadian Radio-television</u> <u>and Telecommunications Commission Act</u> to exercise powers in relation to any matter referred to in the designation.

⁶ Possible resources include industry associations or cyber security and information technology experts. Stakeholders are encouraged to consult with specialists relevant to their respective industries or technology.

Preventions and safeguards

13. Individuals and organizations should identify their vulnerabilities based on the nature of their business, activities, or technology used. The Commission encourages the implementation of a robust compliance program along with preventions and safeguards, which may be taken into consideration when reviewing cases of noncompliance. The Commission considers the following to be examples of reasonable steps, which may vary based on individual circumstances:

Prevention

- Incorporating regular threat and risk assessments into compliance or information technology security programs to identify vulnerabilities and risks.
- Validating the identity of clients, including company name and address, previous or current aliases, length of time in operation, primary corporate directors, or other relevant company stakeholders.
- Being cognizant of location discrepancies (e.g. clients doing business in one region while incorporated, banking, or having online registration in another, unrelated region).
- Obtaining further proof of identity, such as incorporation records, government-issued identification, or tax records, as appropriate in the given situation.
- Avoiding doing business with those seeking total anonymity through the use of aliases, post office boxes as mailing addresses, or cryptocurrency for transactions.
- Researching the reputation of potential clients, including any malicious activity associated with them.
- Reviewing the products or services of potential clients for legal compliance prior to doing business with them.
- Implementing written agreements that bind clients and their downstream clients to comply with CASL.

Detection, notification and information sharing

- Auditing how existing clients are making use of services.
- Detecting and reporting possible violations to relevant authorities.
- Where appropriate, sharing lessons learned and best practices within the industry to reduce the risks to other potential victims.

• Ensuring regular monitoring to detect threats and notifying stakeholders.

Remediation and recovery

- Allocating resources to take down threats, address security vulnerabilities, and implement sustainable changes in a timely manner to prevent similar threats from occurring in the future.
- Providing assistance to users whose devices and accounts have been compromised.

Documentation

- Documenting any measures taken to prevent the occurrence of CASL violations.
- 14. It should be recognized that 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.

Potential enforcement action

- 15. Following a determination that a section 9 violation has occurred, a variety of enforcement actions may be used by the Commission to promote compliance. The choice of enforcement action is typically based on considerations such as
 - the likely effect on compliance;
 - the nature and scope of the violation;
 - the degree of harm associated with the violation;
 - the level of co-operation by the alleged violator; and
 - the history of prior violations.

Related documents

- Guidelines to help businesses develop corporate compliance programs, Compliance and Enforcement Information Bulletin CRTC 2014-326, 19 June 2014
- Guidelines on the use of toggling as a means of obtaining express consent under Canada's anti-spam legislation, Compliance and Enforcement Information Bulletin CRTC 2012-549, 10 October 2012

• Guidelines on the interpretation of the Electronic Commerce Protection Regulations (CRTC), Compliance and Enforcement Information Bulletin CRTC 2012-548, 10 October 2012