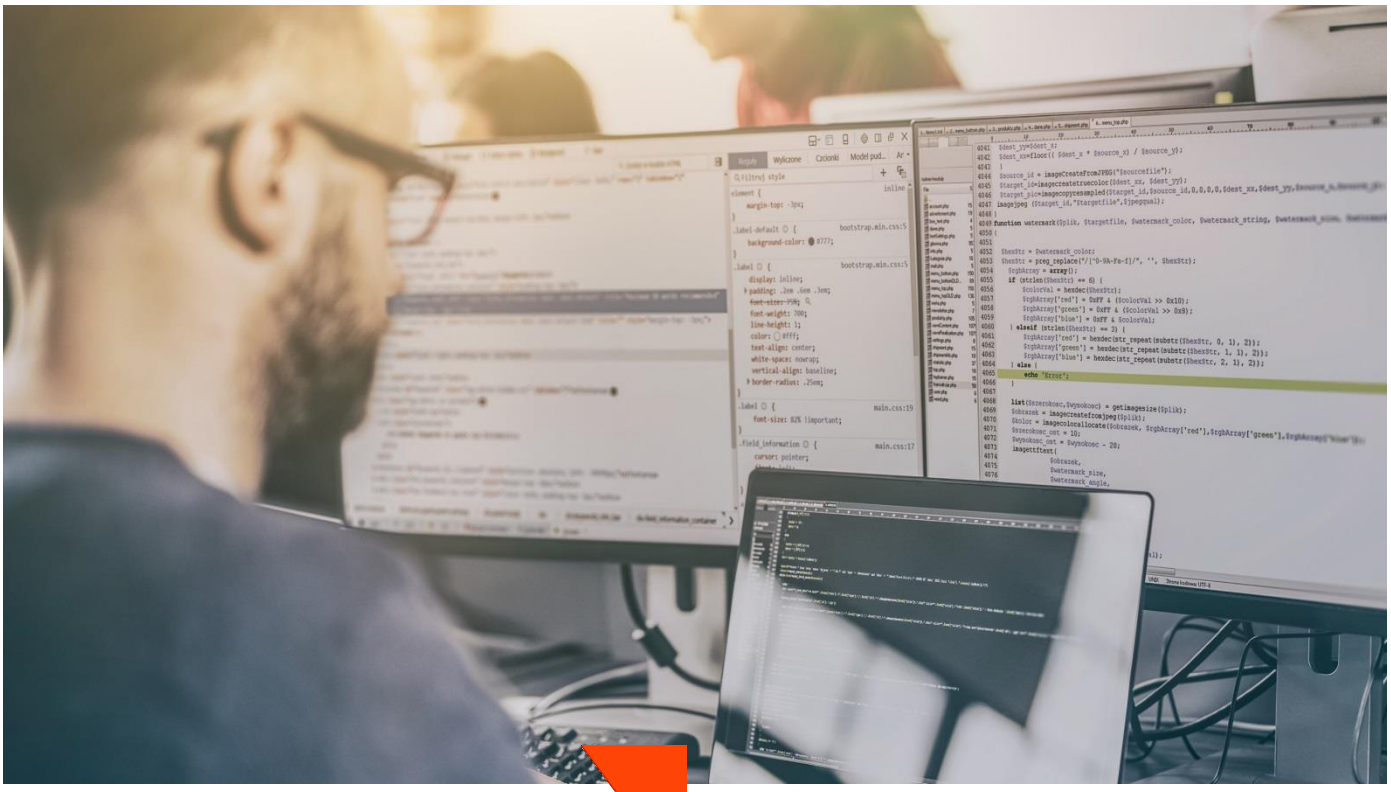
FASKEN



New CASL Ruling: CRTC Provides Guidance on B2B Messaging and the Due Diligence Defence

Privacy and Information Protection Bulletin

On October 19, 2017, the Canadian Radio-television and Telecommunications Commission (CRTC) issued two key decisions in a contested enforcement proceeding brought by Compu.Finder. These recent decisions stem from an earlier CRTC enforcement proceeding against Compu.Finder, which resulted in the first administrative monetary penalty (AMP) issued under Canada's anti-spam legislation (commonly referred to as CASL).

In the first of the two recent decisions, the CRTC rejected Compu.Finder's arguments that CASL was unconstitutional. In the second decision, which is the subject of this bulletin, Compu.Finder's challenge of the AMP was partly successful, reducing the AMP from $1.1 million to $200,000.

This second decision also sheds further light on the way the CRTC interprets and applies certain provisions of CASL and highlights the importance of proper documentation in invoking the due diligence defence. In particular, this decision outlines (i) how the CRTC interprets the business-to-business exemption; and (ii) what factors the CRTC considers in assessing the applicability of the due diligence defence available under CASL.

Background and Decision

On March 5, 2015 the CRTC issued a Notice of Violation to Compu.Finder regarding four violations of CASL and imposed a combined AMP of $1.1 million. The initial investigators' report identified 451 messages sent without consent over approximately a two and a half month period.

In its representations contesting the Notice of Violation, Compu.Finder raised several procedural issues and defences for some of the messages, reducing the number of messages being considered by the CRTC to 317. Of these 317 messages, 87 contained two unsubscribe mechanisms, one functioning and one faulty. Although Compu.Finder asserted that the working unsubscribe mechanism rendered the messages compliant, the CRTC found that these messages were still in violation of CASL, as the broken unsubscribe mechanism caused sufficient confusion to make the functioning mechanism not "able to be readably performed" as required by the regulations under CASL.

Compu.Finder also argued that it had implied consent to send 132 of the messages, as it was able to provide links to public listings where the contact details of the recipients were published. However, the CRTC found that publication of contact details alone is insufficient to meet the requirements for implied consent under CASL. Specifically:

- some of the contact details were from a third-party directory where there was no indication that the contact details were submitted by the intended recipients for publication; and
- some of the contact details were obtained from websites whose terms of use contained a disclaimer against the use of the directory for marketing purposes.

"Business -to-Business" Exemption

The Compu.Finder decision provides much needed clarity on the "business-to-business" exemption included in the regulations under CASL. The regulations provide that in order for the business-to-business exemption to apply: a) the message must be between employees, representatives, consultants or franchisees of the sending and receiving organizations; b) these organizations must have a "relationship"; and c) the content of the message must concern the activities of the receiving organization. If this exemption applies to a message, that message is not subject to CASL's requirements.

In discussing and applying this exemption in the decision, the CRTC has articulated new interpretative principles for the first two elements of the exemption.

Messages Between Organizations

Demonstrating that a message is sent to an employee, representative, consultant or franchisee of an organization may be as simple as demonstrating that the email is sent to a domain that belongs to the recipient organization. This is based on the assumption that it would be "highly unusual for someone who was not an employee, or a representative of some other sort, to have an email address associated with the organization." As a result, this element of the exemption will in many cases be easily satisfied. However, as an example of an instance in which the assumption would not apply, the CRTC pointed to universities, where students and alumni are also likely to have university email accounts, but could not be treated as employees or representatives for the purposes of this exemption.

Relationship Between Organizations

The CRTC decision articulated a new principle in interpreting this exemption – it is not enough for the sending organization to have "any" relationship with the recipient; rather, the relationship should have such a character as to "demonstrate that the organization had, or intended to create, a relationship that would allow for a complete exemption from [CASL's anti-spam regime]."

Compu.Finder sought to demonstrate such a relationship with the recipient organizations by showing either a contractual relationship or some history of correspondence.

- To demonstrate a contractual relationship, Compu.Finder produced invoices and proof of payments for one-off transactions with individual employees within the recipient organization.
- To demonstrate a history of correspondence, Compu.Finder produced a list of individuals it had corresponded with; however, the list had no indication of the period, frequency or content of these messages, or whether such communications were reciprocated.

The CRTC found these stand-alone transactions and history of correspondence insufficient to demonstrate a relationship that would support a presumption that the receiving organization intended to receive messages outside of CASL's anti-spam regime.

The CRTC also found that there was insufficient evidence that the messages sent by Compu.Finder concerned the activities of the recipient organizations.

Due Diligence Defence

Subsection 33(1) of CASL provides that "a person must not be found to be liable for a violation if they establish that they exercised due diligence to prevent the commission of the violation."

The Compu.Finder decision references and underscores prior CRTC guidance on the importance of written CASL policies, ongoing audit and monitoring mechanisms, procedures for dealing with third parties to confirm compliance, and adequate employee training. Compu.Finder did not produce evidence that any of these were in place during the period in which the violations occurred, and so was unable to avail itself of the due diligence defence.

As Compu.Finder decision demonstrates, it is not enough to comply with CASL; an organization must also be able to demonstrate its compliance through documented policies and procedures, and records that support any exemptions.

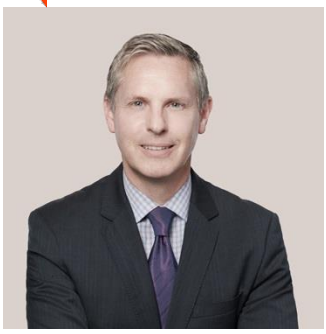
For a discussion of advisable practices and the results of a recent survey on organizational compliance with CASL, see the Fasken Martineau CASL Survey Report "Bridging the Gaps in Understanding and Compliance".

Conclusions

The Compu.Finder case provides welcome guidance on the position of the CRTC in respect of key aspects of CASL. It includes a number of useful lessons for organizations subject to CASL as noted above, and shows that organizations can successfully challenge (and significantly reduce) AMPs in appropriate cases. It is also notable that the decisions come at a time when CASL is under review by the Canadian government and may undergo

amendment. While it remains to be seen whether any drastic changes will be made to the law, the Compu.Finder experience may be viewed as a relevant development in the review of how CASL is functioning.

Authors



Daniel Fabiano

PARTNER

Alex Cameron

PARTNER

Andrew S. Nunes

PARTNER