AMSBIZLAW

ANALYSIS • OPINION • INSIGHT

ALLEN MCDONALD SWARTZ LLP
Business Lawyers

CANADA'S ANTI-SPAM LEGISLATION WILL ALLOW FOR CLASS ACTIONS ON JULY 1, 2017

IS YOUR ORGANIZATION AT RISK?

By Jillian Swartz, Partner,
Allen McDonald Swartz LLP

As a result of the potential for high damages awards, it is likely that CASL litigation will become the next trend in class action litigation.

Canada's anti-spam legislation (CASL), considered by many to be one of the most stringent anti-spam regimes in the world, came into effect on July 1, 2014. Since then, the Canadian Radio-television and Telecommunications Commission (CRTC) has issued a number of press releases reporting on its regulatory enforcement activities, including a fine of Cdn$1,100,000 that it issued to one entity that, in the CRTC's words, "flagrantly" violated the basic principles of the law.

On July 1, 2017, CASL's private right of action provisions, which provide for penalties of up to Cdn$1,000,000 per day, will come into effect. Class actions are almost a certainty. Any Canadian business (and any business that has customers, donors or contacts in Canada) that is not fully compliant with CASL must act now to develop and implement robust compliance strategies in order to mitigate its class action risk.

HIGH-LEVEL OVERVIEW OF THE LAW

CASL applies to any commercial electronic message (CEM) sent to or accessed by a computer system located in Canada. A CEM is an electronic message intended to encourage participation in a commercial activity; an electronic message can be any one of the following:

- email
- text message
- instant message
- direct message sent through a social-networking site

Commercial activity is defined in CASL as any conduct of a commercial character, whether or not there is an expectation of profit. Accordingly, CASL's prohibitions catch a wide range of electronic communications, including electronic messages that offer, advertise or promote any good, service, investment opportunity or gaming opportunity. Subject to certain exceptions, CASL prohibits:

- sending CEMs without consent
- altering transmission data without express consent
- installing computer programs without express consent
- making false or misleading representations in electronic messages, including in the sender and subject lines

- collecting e-mail addresses using computer programs without consent
- collecting personal information through unauthorized access to a computer system

This article discusses the class action risk created by CASL's private right of action regime and offers strategies for developing a robust compliance program to address this risk.

THE CLASS ACTION RISK

CASL provides for a private right of action. This means that, in addition to the risk that the regulators may bring an enforcement action against an organization that violates CASL, there is a potential for individuals, partnerships, corporations, organizations, etc. (or more aptly, a group of such persons) to bring a lawsuit against an organization that has breached CASL. There is a risk of high damages awards under CASL. The following chart summarizes the potential damages that a court may award.

Nature of the Violation	Potential Damages
Sending a CEM without consent and without an exemption	Cdn$200 per contravention, to a maximum of Cdn$1,000,000 for each day on which the contravention occurs **plus** actual damages
Failing to meet the form and content requirements	Cdn$200 per contravention, to a maximum of Cdn$1,000,000 for each day on which the contravention occurs **plus** actual damages
Failing to meet the unsubscribe requirements	Cdn$200 per contravention, to a maximum of Cdn$1,000,000 for each day on which the contravention occurs **plus** actual damages
Altering transmission data without express consent	Up to Cdn$1,000,000 for each day on which the contravention occurs **plus** actual damages
Installing computer programs without consent	Up to Cdn$1,000,000 for each day on which the contravention occurs **plus** actual damages

As a result of the potential for high damages awards, it is likely that CASL litigation will become the next trend in class action litigation. It is also important to note that the CRTC, because it has limited resources to pursue enforcement action, has been focusing on the worst offenders. Class action lawyers are not similarly restrained, so it is likely that they will aggressively pursue organizations that have allegedly violated CASL. The class action risk is heightened because CASL allows a court to impose a monetary award without any proof that actual damages have been sustained.

MITIGATING THE CLASS ACTION RISK – DEVELOPING A COMPLIANCE PROGRAM

In order to minimize the threat of class action litigation, and the size of the damages award, businesses that have customers, contacts or donors in Canada, should develop and implement a sophisticated compliance program.

A compliance program should include the following:

• **An understanding of all of CASL's requirements.** CASL is not only about "spam". While a failure to obtain the necessary consent to send CEMs is perhaps the most obvious act of non-compliance, businesses will also breach the law if CEM does not include the required contact information; if the unsubscribe mechanism included with each CEM is not "clearly and prominently" set out; if the unsubscribe mechanism cannot be "readily performed"; if organizations fail to remove contacts from their mailing lists within 10 business days from an unsubscribe request; and if organizations send CEMs containing false or misleading information.

- **A system to categorize electronic messages.** By categorizing the electronic messages that an organization sends by type and recipient, an organization can obtain a better understanding of how CASL will impact its electronic messaging practices. It can then consider the categories of messages that are (i) exempt from CASL entirely, (ii) for which consent is not required, and (iii) for which consent may be implied.

- **Standard templates for electronic messages.** Creating standard templates will help to ensure that the required identifying information and a compliant unsubscribe mechanism is included in every electronic message.

- **A central contact database.** A central contact database will assist the organization in tracking consents and demonstrating that it has obtained the required consent to send CEMs to its contacts. In addition, a database can effectively keep track of unsubscribe requests. Systems should also be introduced to ensure that opt-out requests are effected within the prescribed time frames.

- **Record retention policies.** In recent enforcement actions, the CRTC has focussed on ensuring that organizations that send CEMs maintain appropriate records by requiring alleged violators to prove that they have complied with each of CASL's requirements for each CEM. The CRTC has imposed fines on businesses that could not prove that they had secured consent from each person to whom the organization had sent a CEM.

- **A CASL policy and employee training programs.** An organization's CASL policy should be an internal document; as a result, it should be kept separate from the organization's privacy policy, which is a customer-facing document. Proper policies and regular training of all employees will assist organizations to create a culture of compliance and will assist in building a due diligence defense.

- **An audit program.** CASL compliance is not a one-time event. In order to maintain compliance with CASL over the long-term, on-going effort is required, particularly given employee turnover and conflicting organizational priorities. Instituting an audit program will not only ensure that systems are working appropriately, but it will also support a due diligence defense in the event that an organization's compliance is challenged.

USING UNDERTAKINGS AS A SHIELD

It should be noted that CASL prohibits a court from issuing a monetary award against an organization that has entered into an undertaking with the CRTC. An undertaking is an agreement between an individual, partnership, corporation, or organization and the regulator that identifies every breach of CASL. Undertakings may also include such conditions as the regulator considers appropriate, which often include a promise by the organization to develop and implement a robust compliance program and pay a fine.

If you are concerned that your organization has violated CASL, you may wish to consider reaching out to the CRTC to canvass the possibility of entering into an undertaking with the regulator. The issue of when and how an organization approaches the regulator is a strategic one and legal advice should be sought before doing so.

VICARIOUS AND DIRECTOR LIABILITY

An employer can be held liable where an employee violates CASL while acting within the scope of his or her employment, unless the employer can show that it exercised due diligence to prevent the violation. In addition, it is an offense to aid, induce, procure or cause to be procured the sending of CEMs in violation of CASL.

CASL also provides for vicarious liability for directors and officers resulting from a company's failure to comply with CASL where they directed, authorized, assented to, acquiesced or participated in the non-compliance, subject to a due diligence defence. Creating a robust compliance program will assist an organization to create its due diligence defence.

CONCLUSION

If your organization needs assistance to develop or enhance its compliance program or to assess the effectiveness of its current compliance program, please contact Jillian Swartz at jswartz@amsbizlaw.com or by phone at 416.642.2524.

Allen McDonald Swartz LLP periodically provides materials on our services and developments in the law to interested persons; these materials are intended to be for informational purposes only and do not constitute legal advice or a legal opinion on any issue.

Please contact the author for permission to reproduce, display or reprint this article.

This article was first published on July 19, 2016.