May 16, 2014

On December 15, 2010, Canada passed Canada's Anti-Spam Legislation ("CASL"), one of the world's most stringent anti-spam laws.[1] The scope of CASL is not limited to Canadian businesses—it regulates any commercial electronic messages that are sent, routed, or accessed using a computer system located in Canada.[2] Although delayed several times, the anti-spam provisions of CASL are set to become effective on July 1, 2014,[3] which means U.S. businesses need to act now in order to ensure that they are in compliance with the law by July 1.[4]

The anti-spam provisions of CASL prohibit the distribution of unsolicited commercial electronic messages unless (i) the message recipient has consented to receiving the message, and (ii) the content and form of the message comply with certain statutory requirements.[5] CASL also contains provisions which prohibit altering transmission data in an electronic message so that the message is delivered to a destination other than, or in addition to, the destination specified by the sender unless certain statutory requirements are met.[6] Such provisions are intended to prevent, or at least create disincentives, for malicious practices such as pharming.[7]

Failure to comply with CASL can result in substantial potential liability. The Canadian Radio-Television and Telecommunications Commission ("CRTC") is authorized to impose administrative monetary penalties of up to C$1 million per violation of CASL for individuals and C$10 million for businesses.[8] Officers, directors, and agents may be personally liable if they acquiesced in a violation of the law.[9] However, because CASL takes into account "honest mistakes," a company that has undertaken good faith efforts to comply will have an affirmative defense in the event the CRTC initiates action based on a violation of CASL.[10]

Recommendations

It is important for any U.S. companies that send, route, or access commercial electronic messages (CEMs) or alter transmission data using a computer system located in Canada, or that deliver CEMs to Canadian residents, to undertake clearly defined actions to comply with the anti-spam provisions of CASL.[11]

1. Make sure you understand what constitutes a "commercial electronic message." CASL defines a "commercial electronic message" or "CEM" as any electronic message that encourages participation in a commercial activity, regardless of whether there is an expectation of profit.[12] Electronic messages that encourage participation in a commercial activity may include messages that offer, advertise or promote goods, services, or business or investment opportunities; messages that advertise or promote a supplier or sponsor; and messages that direct the recipient to a location, telephone number, contact information or website that has a commercial purpose.[13] Examples of CEMs include e-newsletters that provide information that may not be commercial in nature, but that contain a link to a sponsor's website; an online client satisfaction survey; or a mass email providing general information about your business or organization.

The law does not apply to certain types of CEMs. For businesses, the most relevant exceptions are messages sent:

- To a person who is engaged in a commercial activity and your message consists solely of an inquiry or application related to that activity;[14]
- In response to a request, inquiry or complaint, or is otherwise solicited by the person to whom you send the message;[15]
- By your employee, representative, consultant, or franchisee to an employee, representative, consultant or franchisee of (1) your organization and the message concerns the activities of your organization, or (2) another organization if the organizations have a relationship and the message concerns the activities of the organization to which the message is sent;[16] or
- To a limited-access secure and confidential account that you provide in which only you can send messages to the person who receives the message.[17]

There is also an exception if you send a message and reasonably believe the message will be accessed in a listed foreign state[18] and the message conforms to the law of the foreign state that addresses conduct that is substantially similar to conduct prohibited under the CEM rules in CASL.[19]

2. You must obtain express consent before July 1, 2014 to send CEMs and alter transmission data. After July 1 an electronic message that requests such consent will itself be an unauthorized CEM, so it will no longer be possible to obtain express consent by sending such a request.[20] As a result, you should consider obtaining as many express consents as possible now, while you are still able to lawfully send a request for consent by email. Properly done, this can be a good opportunity to touch base with your customers.

Express consent can be obtained orally[21] or in writing, including electronically. However, the burden will be on you to prove that you received such consent. You should keep a record of the time of receipt of consent.[22] Examples of acceptable consent include checking a box on a web page to indicate consent where a record of the date, time, purpose, and manner of that consent is stored in the database, or filling out a consent form at the point of purchase.[23] The end-user must make a positive action to indicate consent, such as checking a box to indicate consent or typing in his or her email address. Mechanisms such as an unchecked opt-out box or a pre-checked opt-in box cannot be used to obtain express consent. Likewise, silence or inaction on the part of the end-user cannot be construed as providing express consent.[24]

Unless you obtain express consent, you should no longer send, route, or access CEMs from computer systems located in Canada, or to users located in Canada, except in the following limited cases in which consent will be implied: (1) where the sender and the recipient have an "existing business relationship" or an "existing non-business relationship" where the relationship arose within the two year period immediately before the day on which the message was sent or is pursuant to a contract in effect in the two year period immediately before the day on which the message was sent (there is a limited grandfather provision that these two year time limits do not apply during the initial three year period after July 1, 2014, if the existing relationship included communications using CEMs);[25] (2) where the recipient has conspicuously published, or caused to be conspicuously published, his or her electronic address, the publication is not accompanied by a statement that the person does not wish to receive unsolicited CEMS at the electronic address, and the message is relevant to the person's business, role, functions or duties in a business or official capacity;[26] or (3) where the recipient has disclosed to the sender the electronic address to which the message is sent without indicating a wish not to receive unsolicited commercial electronic messages at the electronic address, and the message is relevant to that person's business, role, functions or duties in a business or official capability.[27] Consent is also assumed for certain other categories, such as most normal business-to-business communications; providing factual information about an ongoing subscription or similar service; or delivering a product or service, including updates and upgrades, pursuant to an existing relationship.[28] Although not specifically addressed in CASL, the CRTC has taken the position that requests for express consent must not be subsumed in, or bundled with, website terms of use or similar online agreements. The underlying objective is that the specific requests for consent must be clearly identified. For example, users must be able to grant their consent to the website terms, but deny consent to receive CEMS or alter transmission data.[29]

The requirements for obtaining express consent to alter transmission data are the same as the requirements for sending CEMs. However, separate consents to send CEMs and to alter transmission data are required.[30]

3. Make sure that you clearly, prominently and simply identify yourself, and anyone else on whose behalf the message is sent in all CEMs and requests to alter transmission data. In addition, you must state your reason for altering transmission data when seeking consent to alter such data. The identification required by CASL must include:

- Your name or the name by which you conduct your business, if different from your name.[31]
- If you are sending the message on behalf of another person, the name of that person, or the name by which that person conducts its business, if different from that person's name.[32] If you are sending the message on behalf of multiple senders, such as affiliates, all senders must be listed.[33]
- If the message is sent on behalf of another person, a statement indicating which person is sending the message and which person on whose behalf the message is sent.[34]
- The mailing address, and either a telephone number providing access to an agent or a voice messaging system, an email

address or a web address of the person sending the message or, if different, the person on whose behalf the message is sent.[35] The address must be valid for a minimum of 60 days after the message is sent.[36]

If it is not practical for you to include all the above information directly in your message (for example, if you are sending a communication by short message service (SMS)), you can post the information on a web page that the recipient can readily access at no cost. The link to the web page must be clearly and prominently set out in the message.[37]

In addition to stating your identity, or the identity of the person on whose behalf the message is sent, you should also state why you are requesting consent to alter transmission data when seeking such consent.[38]

4. Make sure that all CEMS or consents to alter transmission data include an unsubscribe mechanism. Every CEM that you send and every request for consent to alter transmission data must also include a mechanism by which the user may withdraw consent. You must ensure any withdrawal of consent to receive CEMs or alter transmission data becomes effective within 10 business days after your receipt of such request.[40]

The unsubscribe mechanism in CEMs must be set out clearly and prominently.[41] In addition, it must be "readily performed" which means it must be accessed without difficulty or delay, and should be simple, quick, and easy for the consumer to use.[42] In the case of a SMS, the user should have the choice between replying to the SMS message with the word "STOP" or "Unsubscribe" and clicking on a link in the SMS message that will take the user to a web page where he or she can unsubscribe from receiving all or some types of commercial electronic messages from the sender.[43]

For consents to alter transmission data, you must provide the person who gave his or her consent with an electronic address to which he or she may send notice of the withdrawal of such consent.[44]

NOTES

1. 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, S.C., chapter 23, formerly referred to as the "Fighting Internet and Wireless Spam Act."
2. §8 of CASL which deals with the installation of computer programs becomes effective on January 15, 2015. This section requires the consent of an end-user before either installing a computer program on the end-user's computer system or having an installed program send an electronic message from the end-user's computer system.
3. Order 81000-2-1795 (SI/TR), available at http://fightspam.gc.ca/eic/site/030.nsf/eng/00272.html.
4. Further details about CASL, including differences between CASL and the U.S. CAN-SPAM Act, are described in our prior Cooley Alert, which is available at https://www.cooley.com/canadas-anti-spam-law-how-it-may-affect-your-US-based-business.
5. CASL, *supra* note 1, §6.
6. CASL, *supra* note 1, §7.
7. Pharming is a form of cyber-attack in which a user requests a certain website but is then redirected to a fraudulent website.
8. CASL, *supra* note 1, §20(4). §47 of CASL that provides a private right of action will become effective on July 1, 2017. Class actions are anticipated. Also on July 1, 2017, §51 of CASL will become effective. §51 of CASL provides statutory damages of C$200 per commercial electronic message (up to a maximum of C$1 million per day) and C$1 million per day for altering transmission data. The penalties also apply to anyone aiding, inducing or procuring, or causing to be procured a violation of CASL. In addition, for each occurrence of conduct reviewable under the Competition Act, there is also a penalty of C$200 for each occurrence of the conduct, not exceeding C$1,000,000 for each day on which the conduct occurred.
9. CASL, *supra* note 1, §31.
10. CASL, *supra* note 1, §33(1).
11. The alteration of transmission data may also be made in accordance with a court order or by a telecommunications service provider for the purposes of network management pursuant to §7(1)(b) and §7(2) of CASL.
12. CASL, *supra* note 1, §1(2).
13. CASL, *supra* note 1, §1(2).
14. CASL, *supra* note 1, §6(5)(b).
15. Electronic Commerce Protection Regulations (SOR/2013-221), April 16, 2014, §3(b), available at http://laws-lois.justice.gc.ca/eng/regulations/SOR-2013-221/FullText.html.

16. *Id.* §3(a).
17. *Id.* §3(e).
18. The list of foreign states is set forth in the schedule to the Electronic Commerce Protection Regulations (SOR/2013-221), April 16, 2014, available at http://laws-lois.justice.gc.ca/eng/regulations/SOR-2013-221/page-4.html#h-8.
19. *Id.*, §3(f).
20. CASL, *supra* note 1, §1(3).
21. If you are obtaining consent orally, it must be verified either by an independent third party or a complete, unedited audio recording. Compliance and Enforcement Information Bulletin, CRTC 2012-548, October 10, 2012, available at http://www.crtc.gc.ca/eng/archive/2012/2012-548.htm.
22. CASL, *supra* note 1, §13.
23. Compliance and Enforcement Information Bulletin, CRTC 2012-548, *supra* note 21.
24. Compliance and Enforcement Information Bulletin, CRTC 2012-549, October 10, 2012, available at http://www.crtc.gc.ca/eng/archive/2012/2012-549.htm.
25. CASL, *supra* note 1, §10(9)(a), §10(10), and §66.
26. CASL, *supra* note 1, §10(9)(b).
27. CASL, *supra* note 1, §10(9)(c).
28. CASL, *supra* note 1, §6(6). For more information about implied consent see our prior *Cooley Alert*.
29. *Id.*
30. Compliance and Enforcement Information Bulletin, CRTC 2012-548, *supra* note 21.
31. Electronic Commerce Protection Regulations (SOR/2012-36), April 16, 2014, §2, available at http://laws-lois.justice.gc.ca/eng/regulations/SOR-2012-36/FullText.html.
32. *Id.* A person who just facilitates the distribution of a commercial electronic message but has no role in its content or choice of the recipients does not need to be identified. Compliance and Enforcement Information Bulletin, CRTC 2012-548, *supra* note 21.
33. Electronic Commerce Protection Regulations (SOR/2012-36), *supra* note 31, §2.
34. *Id.*
35. *Id.* If you run a home business, you do not have to provide your home address. Any valid mailing address is valid as long as you can be contacted at that address. Compliance and Enforcement Information Bulletin, CRTC 2012-548, *supra* note 21.
36. CASL, *supra* note 1, §6(3).
37. Electronic Commerce Protection Regulations (SOR/2012-36), *supra* note 31, §2(2).
38. CASL, *supra* note 1, §10(1); *see also* CASL FAQs available at http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00050.html.
39. CASL, *supra* note 1, §6(2)(c) and §11(1) and §11(4).
40. CASL, *supra* note 1, §11(3) and §11(4).
41. Electronic Commerce Protection Regulations (SOR/2012-36), *supra* note 31, §3.
42. *Id. See also* Compliance and Enforcement Information Bulletin, CRTC 2012-548, *supra* note 21.
43. Compliance and Enforcement Information Bulletin, CRTC 2012-548, *supra* note 21.
44. CASL, *supra* note 1, §11(4)(a).

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Adam Ruttenberg Washington, DC	aruttenberg@cooley.com +1 202 842 7804

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.