KEY DIFFERENCES BETWEEN US AND CANADIAN ANTI-SPAM LAWS

Posted on April 14, 2014

Categories: Insights, Publications

Canada's Anti-Spam Law (or "CASL") will be in effect in July 2014, about ten years after the U.S. has enacted its anti-spam law. As a matter of fact, the U.S. enacted anti-spam legislation, entitled *Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003* (the "CAN-SPAM" Act) on December 16, 2003.[1]

While the U.S. has enacted an anti-spam law promoting an opt-out model, Canada has adopted an opt-in model. The main difference between these systems is the fact that under an opt-out model, businesses can send promotional email messages unless the recipient informs the sender that it no longer wishes to receive such emails, or "opts out" of receiving them. Business groups, for the most part, tend to prefer the opt-out approach because it is easier to imply consent and thus create mailing lists. Under an opt-in model, the recipient of the promotional email must affirmatively give the organization permission to send information about new products or sales. Generally, a consumer must click on web site boxes or send an email request to the organization in order to authorize consumer email.

How will CASL impact U.S. businesses that want to send promotional emails throughout North America?

The U.S. CAN-SPAM Act does not expressly address messages sent from out of jurisdiction. However in Canada, under section 12 (1) of CASL, a person contravenes section 6 (pertaining to the sending of promotional messages), if a computer system located in Canada is used to send or access the electronic message. Therefore electronic messages sent to persons in Canada have to comply with CASL. The exceptions to this are if the message is accessed here but the sender had reasonable cause to think that it would be opened in another country that has legislation that is substantially similar to CASL,[2] or if the electronic message is routed through Canada on its way to a recipient in another country.[3]

As this provision imposes the stringent CASL opt-in requirements for U.S. businesses when sending promotional emails to Canadians, we have summarized the key differences between *CASL* and *CAN-SPAM* as the following ones:

1. **CEMs versus CEMMs**: *CAN-SPAM* applies to commercial electronic mail messages (or "*CEMMs*") which are defined as any commercial email with a "primary purpose" of commercial advertisement or promotion of a

product or service, which is not an email relating to a business transaction or relationship.[4] Unlike CASL which applies to "commercial electronic messages" (or "CEMs"), which are defined as "any means of telecommunication, including a text, sound, voice or image message," CAN-SPAM applies to "commercial electronic mail messages," i.e., email only. CASL also applies to computer programs in that it prevents a sender from installing or "caus[ing] to be installed" a computer program that causes *CEMs* to be sent from that computer system, without either consent or a court order.[5] *CAN-SPAM* on the other hand, does not expressly apply to the installation of computer programs.

2. **Opt-In versus Opt-Out Consent**: The main difference between these two pieces of legislation mostly has to do with the different type of model for consent. *CAN-SPAM* is based on an opt-out consent model, whereby consent to receive email is considered implicit unless the recipient "opts out," thereby indicating a unwillingness to receive such emails.[6] *CASL* allows *CEMs* only if: i) the sender has the express consent of the recipient, or ii) consent is not required (because it is implied or because the message falls under the listed exemptions). Therefore, U.S. businesses, unless they have express consent, an "existing" business relationship with Canadians or their messages are exempt (for instance if the CEM is sent by an employee to another employee of the organization and that concerns the affairs of the organization),[7] will have to use caution before contacting Canadian email or electronic addresses for promotional purposes.

3. **Existing Business Relationship**: One of the exceptions to compliance with the consent requirements of CASL[8] is if there is an existing business relationship between the parties, which is defined as a business relationship between the recipient and the sender of the message — arising from any of the following activity taking place **within the two-year period** immediately before the day on which the message was sent:

> (a) the purchase or lease of a product, goods, a service, land or an interest or right in land, by the person to whom the message is sent from the sender;[9]
>
> (b) the acceptance by the person to whom the message is sent, of a business, investment or gaming opportunity offered by sender;[10]
>
> (c) the bartering of anything mentioned in paragraph (a) between the person to whom the message is sent and sender;[11]
>
> (d) a written contract entered into between the person to whom the message is sent and sender in respect of a matter not referred to in any of paragraphs (a) to (c), if the contract is currently in existence or expired within the two-year period; or[12]
>
> (e) an inquiry or application, within the six-month period immediately before the day on which the message was sent, made by the person to whom the message is sent to sender, in respect of anything

mentioned in any of paragraphs (a) to (c) above.[13]

Therefore, if any of these relationships can be made out then there is deemed to be implied consent and the sender does not have to comply with the opt-in consent requirements. However the obligation to include all the mandatory content still remains.

4. **Unsubscribe Mechanism**: The *CAN-SPAM* Act requires that every *CEMM* contain an unsubscribe mechanism for the recipient to use to opt-out of receiving further emails. The unsubscribe mechanism can be in the form of a "functioning return electronic mail address or other Internet based mechanism" contained within the *CEMM* or a "list or menu" from which the recipient may chose not to receive further messages from the sender, and must remain active for the recipient to use for at least 30 days after the original *CEMM* was sent.[14] Under CASL, the unsubscribe mechanism "must be able to be readily performed" such that it "should be accessed without difficulty or delay, and should be simple, quick, and easy for the consumer to use,"[15] and the unsubscribe mechanism must remain active for at least 60 days.[16] Under the CAN-SPAM Act, the sender of the communication or "any person acting on behalf of the sender" must act on the request to unsubscribe within 10 business days of receiving it,[17] which requirement is identical under CASL, s. 11(3).

5. **Content Requirements**: Apart from the unsubscribe mechanism described above, which both CASL and the U.S. CAN-SPAM Act require, they also both require that the sender provide certain contact information. *CAN-SPAM* requires that a *CEMM* include "clear and conspicuous" identification that the message is an advertisement or solicitation[18] while CASL prohibits unsolicited CEMs, unless the recipient has consented to receiving it (by express or implied consent).[19] *CAN-SPAM* requires that a *CEMM* include a valid physical postal address of the sender[20] while CASL requires that the CEM "clearly and prominently" disclose the mailing address, and either a telephone number with active response voicemail or an email address or a web address.[21]

6. **Liability**: *CASL* includes potential vicarious liability for directors and officers of corporations and employers of employees acting within the scope of their employment, and *CAN-SPAM* is silent on the issue of a director's, officer's or employer's liability. *CASL* also provides a private right of action to individuals affected by a violation, while *CAN-SPAM* provides no such right to ordinary individuals. Apart from a state attorney general, only *ISPs* who have been "adversely affected by a violation" can bring an action under *CAN-SPAM*.

7. **Penalties**: If there is a breach of *CAN-SPAM*, there are administrative, civil and criminal penalties available, depending on which provisions are violated.

- Administrative actions are initiated by the Federal Trade Commission. This includes the ability to issue administrative orders, including injunctions, or to prosecute certain cases before the courts.[22]
- Civil actions may be brought in the courts either by a state attorney general, or by an Internet Service

Provider (or "*ISP*") under certain conditions.[23] Criminal prosecutions are dealt with by the federal Department of Justice. Statutory damages of up to either $1,000,000 or $2,000,000 may be awarded, depending on whether the action is brought by an ISP or a state attorney,[24] plus aggravated damages where warranted.[25]

- Criminal violations of *CAN-SPAM*, including various fraudulent acts such as falsifying email header information and gaining unauthorized access to computers to use them for spamming, are punishable by fines under the criminal provisions of Title 18 of the *United States Code* and/or a prison term of up to five years, three years or one year, depending on the nature of the offence.[26] It is also possible to seek forfeiture of a spammer's assets in criminal cases.[27]

Higher monetary penalties appear to be in place for violations of CASL, which provides for a maximum penalty of $1,000,000 per violation in the case of an individual, and $10,000,000 per violation "in the case of any other person."[28]

These differences between the U.S. and Canadian legislation in the area of anti-spam highlight the fact that U.S. businesses should be careful when sending out mass emails or other forms of electronic communication for a commercial purpose. The laws in Canada are more stringent, and the penalties for a breach are potentially severe.

by Éloïse Gratton and Sharon Groom

[1] *Controlling the Assault of Non-Solicited Pornography and Marketing Act* of 2003, 15 USC 7701 ["*CAN-SPAM*"].

[2] Electronic Commerce Protection Regulations 81000-2-175 (SOR/DORS) ("Electronic Commerce Protection Regulations"),section 3(f)

[3] See Industry Canada *Regulatory Impact Analysis Statement* published January 5, 2013.

[4] *CAN-SPAM*, section 3(2)(A).

[5] *CASL*, section 8(1).

[6] *CAN-SPAM*, section 5(a)(5)(A)(ii).

[7] Electronic Commerce Protection Regulations, SOR/2013-221, section 3(a).

[8] Compliance with the content requirements of *CASL* is still required.

[9] *CASL*, section 10(10)(a).

[10] *CASL*, section 10(10)(b).

[11] *CASL*, section 10(10)(c).

[12] *CASL*, section 10(10)(d).

[13] *CASL*, section 10(10)(e).

[14] *CAN-SPAM*, section 5(a)(3)(A)(ii).

[15] Electronic Commerce Protection Regulations (CRTC), SOR/2012-36, section 23.

[16] *CASL*, section 11(2).

[17] *CAN-SPAM*, section 5(a)(4)(A)(i).

[18] *CAN-SPAM*, section 5(a)(5)(A)(i).

[19] *CASL*, section 6(1)(a).

[20] *CAN-SPAM*, section 5(a)(5)(A)(iii).

[21] Electronic Commerce Protection Regulations (CRTC), SOR/2012-36, section 3(2).

[22] *CAN-SPAM*, section 7(f)(2).

[23] *CAN-SPAM*, sections 7(f) and (g).

[24] *CAN-SPAM*, sections 7(f) and (g).

[25] *CAN-SPAM*, section 7(3)(c)

[26] *CAN-SPAM*, section 4(b).

[27] *CAN-SPAM*, section 4(c).

[28] *CASL*, section 20(4).

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.