GET THE MESSAGE:
CASL COMPLIANCE

STEWART McKELVEY
LAWYERS • AVOCATS

Canada's Anti-Spam Legislation (CASL)

CASL is a federal law aimed at eliminating unsolicited and malicious electronic communications. The majority of CASL's provisions came into force July 1, 2014 with the provisions relating to the installation of computer programs (section 8) coming into force as of January 15, 2015. The provisions related to the private right of action (sections 47-51) are scheduled to come into force as of July 1, 2017. Accordingly, organizations will have to comply with specific consent, disclosure and unsubscribe requirements when sending out electronic communications and installation of computer programs.

CASL is accompanied by two sets of regulations from the Canadian Radio-television and Telecommunications Commission (CRTC Regs) and from Industry Canada (IC Regs). The CRTC has also issued interpretative guidelines (including Compliance and Enforcement Information Bulletins CRTC 2012-548 and 2012-549), but these guidelines do not have the force of law.

This guide provides basic information on CASL to help understand how it will impact electronic communication practices and will focus on CASL's prohibition on "spam". We also include a summary in section IX below on CASL's provisions in respect of installation of computer programs. In many cases where a section applies to your organization, we recommend you look closely as the specific wording of CASL as the notes below are paraphrased. Section references to CASL and the applicable regulations have been added for ease of reference.

What does CASL prohibit?

CASL targets three activities:

Spam	Prohibition on sending, causing or permitting to be sent commercial electronic messages (CEMs) without the express or implied consent of the recipient, and in compliance with prescribed form and content requirements (section 6).
Phishing	Prohibition on altering transmission data in an electronic message so that it is delivered to an alternative address without express consent (section 7).
Spyware/malware	Prohibition on installing a computer program on another's computer or causing electronic messages to be sent from such a computer without express consent (section 8).

CASL and its regulations will trump any conflicting provision of the Personal Information Protection and Electronic Documents Act (PIPEDA) (section 2).

CASL distinguishes in some sections between individuals and "persons", which are defined to include an individual, partnership, corporation, organization, association, trustee, administrator, executor, liquidator of a succession, receiver or legal representative (section 1(1)).

I. Spam - Commercial Electronic Messages (CEM)

As we prepare to address the obligations of CASL, it is important to understand the overall concept. Firstly, section 6 includes a broad prohibition against sending, causing or permitting to be sent CEMs without (i) consent, and (ii) compliance with certain form and content requirements. This prohibition catches many

messages, so after reviewing the basic definition of CEMs, the next step is to look at the exceptions where neither the consent nor form requirements are necessary, or, where express and/or implied consent may not be required. It is only by understanding the various exceptions that we can assess the overall impact on a business. The first step is to assess the scope of the definition of "commercial electronic message".

"**Commercial Electronic Message**" or "**CEM**" – defined broadly to capture electronic messages that have as one of their purposes "encouraging participation in a commercial activity" sent from email accounts, text messaging accounts and any other similar account types (section 1(2)). Does not include voicemail or fax messages (section 6(8)), or messages for law enforcement or public safety (section 1(4)).

"**Commercial Activity**" – includes any particular transaction, act, or conduct that is of a commercial nature, whether or not carried out for profit (section 1(1)).

II. Exceptions where CASL does not apply to CEMs

CASL does not apply to certain types of messages, meaning there are no consent or form requirements for:

"**Family or Personal Communications**": CEMs sent to family members or those who have a personal relationship with the sender (section 6(5)(a) & IC Regs). "Personal Relationship" is defined to include (for individuals only) a history of two way communications, and considers factors such as sharing of interests, frequency of communications and whether the parties have met in person (section 2, IC Regs).

"**Commercial Inquiry Communications**": CEMs consisting solely of an inquiry or application related to the commercial activity of the recipient person (section 6(5)(b)).

"**Internal Business Communications**": CEMs sent within the same organization (among employees, representatives, consultants or franchisees) provided the CEM concerns the activities of the organization (section 3(a)(i), IC Regs).

"**Business to Business Communications**": CEMs sent between different organizations (among employees, representatives, consultants or franchisees), provided (a) organizations have a relationship and (b) the CEM concerns the activities of the organization to which the message is sent (section 3(a)(ii), IC Regs).

"**Prompted Communications**": CEMs which are responses to inquiries, requests or complaints of a person, or that are otherwise solicited by the recipient (section 3(b), IC Regs).

"**Legal Communications**": CEMs sent to satisfy a legal obligation, or to enforce a legal right (section 3(c), IC Regs).

"**Social Network Communications**": CEMs sent and received on "electronic messaging services" provided the required information and unsubscribe mechanism are conspicuously published on the user interface, and recipient has provided implied or express consent (section 3(d), IC Regs). This is anticipated to apply to social networking services or instant messaging services.

"**Secure Account Communications**": CEMs sent to a limited-access secure and confidential account where only the account provider is able to send messages to the account (section 3(e), IC Regs).

"**Foreign Destination Communications**": a CEM sent with the reasonable expectation that the CEM will be accessed in a foreign state having similar anti-spam laws and the message conforms with those foreign laws (section 3(f), IC Regs). A list of recognized countries is scheduled to the regulations.

"**Charity Fundraising Communications**": a CEM sent by or on behalf of a registered charity and the message has the primary purpose of raising funds for the charity (section 3(g), IC Regs).

"**Political Solicitation Communications**": a CEM sent by or on behalf of a political party / organization, with the primary purpose of soliciting contributions (section 3(h), IC Regs).

III. Form requirements for CEMs

Under CASL, all CEMs, unless subject to an exception as noted above in part III, will need to include the following information "clearly and prominently" (section 6(2) and (3), 11(1) – (3) &, CRTC Regs):

- Identity/business name of person sending and on whose behalf the CEM is sent (section 6(2)).
- If the CEM is sent on behalf of another person, a statement must be included indicating which person is sending and which person on whose behalf it is sent.
- Contact information including mailing address and either phone number or email/web address of person sending, or if different, the person on whose behalf CEM sent. The information must enable recipient to readily contact one of such persons (section 6(2)). Contact information must be valid for 60 days after message sent (section 6(3)).
- Unsubscribe mechanism must be included with an electronic address or web link and must be able to be "readily performed". Must be valid for 60 days after message sent. Unsubscribe must be effected within 10 business days after unsubscribe request (sections 11(1) – (3)).

It is also important to ensure that the CEM does not contain any false or misleading statements or claims including in the sender information, subject line, or any URLs or metadata (sections 74 and 75).

IV. Consent

Consent is addressed in one of three ways:

- Express consent from the recipient (section 10(1)).
- Implied consent to send the CEM (section 10(9)) or deemed consent to install the computer program (section 10(8)).
- An exception applies (section 6(6)).

The onus to prove consent rests with the sender of the CEM or the installer of computer program (section 13).

Express Consent

To obtain valid express consent (section 10(1) & CRTC Regs), the request for consent must:

- Set out "clearly and simply" the required information.
- State the purpose(s) for which consent is being sought.
- Include the business name of the person seeking consent, and the business name of any person on whose behalf consent is sought; and specifying which person is seeking consent and which on whose behalf consent is sought.
- Include contact information consisting of mailing address and either phone number or email/web address of person sending or if different the person on whose behalf CEM sent.
- Be Opt-in (i.e. click a box, or enter email address) and not Opt-out (CRTC's view).
- State that consent can be withdrawn.
- Be separate for each act of sending a CEM, installing a computer program and altering transmission data (CRTC Regs).
- Should not be bundled with other terms and conditions, such as terms of use or sale (CRTC Guidelines).

Note: Consent may be obtained orally, in paper form or electronically. **However**, a request for consent sent by an electronic message is a CEM, and so must comply with the form and consent provisions in order to be sent (section 1(3)).

Consent may be obtained on behalf of an unknown person (who will rely on the consent), provided that certain conditions in the IC regulations are met regarding ongoing use of and withdrawal of such consent.

Implied Consent

Implied consent for CEMs exists where:

- Sender and recipient have an "**existing business relationship**" (sections 10(9) and detailed definition in 10(10)):
    - **Within the last two years**: any purchase or lease of products or services, acceptance of business or investment, bartering; or contract for such things in force or expired within last two years.

- **Within the last six months:** an inquiry or application from the CEM recipient to sender, in respect of any such business transactions.

- Sender and recipient have an "**existing NON-business relationship**" (sections 10(9) and detailed definition in 10(13) & IC Regs), i.e. **within the last two years** a donation of time or money to a registered charity, political party, organization or candidate, or, membership in a club, association or volunteer organization.

- Recipient "conspicuously" published their email address, or has disclosed their address to the sender, without indicating that they do not wish to receive unsolicited CEMs, and the CEM being sent is relevant to the recipient's business, role, function or duties in a business or official capacity (section 10(9)(b) &(c)).

See CRTC Guidance on Implied Consent for more information on when you may rely upon implied consent.

Exceptions for Consent

A CEM may be sent without express or implied consent to:

- Provide a quote or estimate requested by the recipient (section 6(6)(a)).

- Facilitate, complete, or confirm a commercial transaction between the sender and recipient that the recipient previously agreed to enter into with sender (section 6(6)(b)).

- Provide warranty/safety/recall/security information about a product or services used or purchased by recipient (section 6(6)(c)).

- Provide notification of factual information about an ongoing subscription, membership, account, loan or similar relationship or goods or services offered thereunder (section 6(6)(d)).

- Provide information directly related to a current employment relationship or benefit plan (section 6(6)(e)).

- Deliver a product, good or service, including updates and upgrades further to an existing relationship (section 6(6)(f)).

- "Third Party Referrals": a **single** CEM may be sent to a recipient without consent based on the referral to the sender by a third party who has a relationship (business, family, personal or non-business) with the sender and the recipient. The CEM must disclose the full name of the referring person and that the message was sent as a result of the referral (section 4, IC Regs).

Always remember that even where consent is addressed by implied consent or an exception, the form requirements of the CEM (contacts, unsubscribe etc.) still apply.

V. Grace period

For the first three years under the law, there will be implied consent for sending CEMs to recipients where, as of July 1, 2014, there was an existing business relationship or non-business relationship, regardless of when that relationship may have last been active (i.e. without reference to the two year or six month time periods); provided that the recipient does not withdraw consent, and, the relationship included the exchange of commercial electronic messages (section 66). The grace period is set to end as of July 1, 2017.

Computer programs that were installed before January 15, 2015 will benefit from implied consent for three years until January 14, 2018, unless the user gives notice that they no longer consent to the original installation (section 67).

VI. Installation of computer programs

The provisions dealing with the unsolicited installation of computer programs came into force on January 15, 2015. Section 8 of CASL is intended to prohibit spyware/malware but will capture any circumstance involving:

- the installation of a computer program
- on any other person's computer system
- located in Canada, (or on a computer located outside Canada, if the person who installed it was located in Canada) (section 8(2))
- during the course of a "Commercial Activity" (as defined above in Section I of this Guide)
- unless that person's express consent is obtained, or the installation is in accordance with a court order.

Exceptions for "self-installed software"

According to CRTC guidelines, CASL does not apply and there are no consent requirements for self-installed software, i.e. any time an individual downloads and installs an app or program, or loads software from a CD, or accepts a prompt to update an existing program. Similarly, if an employer installs software on its own network, CASL will not apply. This exclusion will only apply if the scope of installation is consistent with the program functionalities expected by the consumer, meaning that unexpected functionalities are prohibited from "tagging along" with a consumer's self-installation.

Consent, and Enhanced Disclosure for Certain Program Functions and Purposes

The standard for express consent that is required for the installation of computer programs overlaps with what is necessary for sending CEMs, as described above in Section IV.

Updates or upgrades will not require additional consent where valid express consent has initially been obtained (section 10(7)) and "the person who gave the consent is entitled to receive the update or upgrade under the terms of the express consent and the update or upgrade is installed in accordance with those terms." CRTC's guidelines state simply that consent is needed to install upgrades or updates. Consent may

be assumed for certain core programs such as cookies, HTML code, java scripts, or operating systems (section 10(8)).

When seeking express consent it is required that a party clearly and simply describe the function and purpose of the computer program that is intended to be installed.

In addition, if the person seeking consent knows that the installation will operate to perform any of the functions listed below, and such functions are beyond the reasonable expectations of the owner/user, then such functions must be brought to the attention of the owner/user clearly and prominently apart from license terms and other information, describing function, nature, purpose and reasonably foreseeable impact (section 10(3) -10(5), CRTC Regs s. 5). Those functions include:

- Collecting personal information stored on the computer system.
- Interfering with the owner's or an authorized user's control of the computer system.
- Changing or interfering with settings, preferences or commands already installed or stored on the computer system without the knowledge of the owner or an authorized user of the computer system.
- Changing or interfering with data that is stored on the computer system in a manner that obstructs, interrupts or interferes with lawful access to or use of that data by the owner or an authorized user of the computer system.
- Causing the computer system to communicate with another computer system, or other device, without the authorization of the owner or an authorized user of the computer system.
- Installing a computer program that may be activated by a third party without the knowledge of the owner or an authorized user of the computer system.

The consent requirements for these functions may not apply if the function only collects, uses or communicates transmission data (10(6)).

As noted above, computer programs that were installed before January 15, 2015 will benefit from implied consent for three years until January 14, 2018, unless the owner/user gives notice that they no longer consent to the original installation (section 67).

Request for Program Removal with Above Functions

For a period of one year after consent for installation is given, the person who gave consent must be provided with an electronic address where they can send a request to remove or disable the program which performs one of the functions listed above. The request can be made where the person who gave their consent believes that the function, purpose or impact of the program was not accurately described when their consent was obtained. The removal or disabling of the program must be achieved without cost to the party making the request (section 11(5)).

Deemed Consent

Consent can be deemed for certain types of installations, including cookies, HTML code, Javascript, operating systems, certain telecommunications security and upgrades, programs solely to correct systems failures, and all programs executable through another program that was already consented to (section 10(8)). However, if the owner / authorized user has, for example, disabled cookies or Javascript, or activated "do not track" functionality, this is sufficient to negate deemed consent, according to the CRTC.

Exemptions for Telecommunication Service Providers (TSPs)

Two exemptions are provided for TSPs in regards to the installation of computer programs. First, TSPs will not be required to obtain prior consent to install a computer program for the limited purposes of preventing activities which pose an imminent security risk. Second, TSPs will not be required to obtain prior consent to install network wide software or system upgrades (section 6, IC Regs).

Further, programs that only collect, use or communicate "transmission data" are also exempted. Transmission data is data that does not reveal the substance, meaning or purpose of the communication (sections 1, 10(6)).

VII. Enforcement under CASL

Enforcement may occur under CASL by administrative penalty, or pursuant to private claims. The private claims regime comes into force on July 1, 2017, and there are fears that significant class action proceedings may result.

CRTC enforcement to date has been active and vigorous, with multiple decisions imposing significant fines.

CRTC may impose maximum administrative penalties of one million dollars for individuals and ten million dollars for corporations and other organizations (section 20(4)).

Directors and officers may be liable (section 31); and employers may be liable for acts of their employees (section 32).

The private right of action comes into force as of July 1, 2017 (sections 47-51)

These sections allow a person to make an application to court for a remedial order, in respect of any breaches of CASL, including the sending of spam, phishing (altering transmission data in an electronic message), installing computer programs without consent, or aiding, inducing, procuring or causing the doing of these acts. The private right of action will also apply to certain of sections from the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") which prohibit collecting electronic addresses through a program designed for doing so, or collecting personal information via telecommunications access to a computer system, and also to section 74.011 of the *Competition Act*, in respect of false or misleading electronic communication content, including in respect of sender information, subject matter information, locators (e.g. URLs and metadata), or other representations.

If a court is satisfied that a contravention of these sections has occurred, the court is permitted under section 51 to award actual loss and damage, PLUS potentially steep penalties, including, for example, $200 for each spam communication, but not exceeding $1,000,000 per day. Such a number could add up quickly if

one was engaged in a large email campaign which contravened CASL. The fines for contravening PIPEDA and the *Competition Act*, in respect of those sections noted above, are not to exceed $1,000,000 per day.

The purpose of these sections is stated to be promotion of compliance, rather than punishment (s. 51(2)).

The court is obliged to consider various factors including the purpose of their order, the nature and scope of the contravention, the person's history in respect of these sections, any financial benefit, ability to pay and any other relevant factor (section 51(3)).

It is noteworthy that officers, directors and agents of a corporation that commits a contravention are liable if they directed, authorized, assented to, acquiesced in or participated in the commission of the contravention, even if the corporation does not face proceedings (section 52).

Companies are also vicariously liable for the actions of their employees (section 53).

A three year limitation period for private claims applies (section 47(2)).

VIII. Compliance Programs

A due diligence defence may be available if the sender can show established policies and practices for compliance (section 33 and 54).

The CRTC has issued *Guidelines to help businesses develop corporate compliance programs*. Note, the guidelines are not a "one size fits all" solution and depending on the nature and size of your business, not all the components mentioned in the Compliance Guidelines may be appropriate or practical and should be viewed in the light of your particular business activities.

The following is a brief summary of the components of a compliance program as discussed in the Compliance Guidelines as relate to CASL:

- Senior Management Involvement (and possibly appoint a Compliance Officer)
- Risk Assessment of Current Activities
- Create a Written Corporate Compliance Policy
- Keep Proper Records (including, express consents, unsubscribe requests, recipient and sent logs, campaign records, staff training documents).
- Implement a Training Program
- Regular Auditing and Monitoring
- Complaint Handling System
- Disciplinary Action for Non-compliance with Compliance Policy

Simply having a program is not, in itself, a defence - it must be credible and put in practice. An effective program may enable a business to demonstrate that it took reasonable steps to avoid violating CASL. However, even if a due diligence defence fails, the presence of a credible and effective compliance program may nevertheless be a mitigating factor considered in determining the amount of an administrative monetary penalty.

This Guide is offered for general information purposes and is not intended to provide legal advice.

Last revised June 6, 2017.

For questions please contact the following lawyers in Stewart McKelvey's Halifax office:

Rob Aske at raske@stewartmckelvey.com or 902 420 3310
Burtley Francis at bfrancis@stewartmckelvey.com or 902 444 1714

Charlottetown, PE
65 Grafton Street
Charlottetown, PE C1A 1K8
P 902.892.2485
F 902.566.5283
charlottetown@stewartmckelvey.com

Fredericton, NB
Suite 600, Frederick Square
77 Westmorland Street
Fredericton, NB E3B 6Z3
P 506.458.1970
F 506.444.8974
fredericton@stewartmckelvey.com

Halifax, NS
Suite 900, Purdy's Wharf Tower 1
1959 Upper Water Street
Halifax, NS B3J 3N2
P 902.420.3200
F 902.420.1417
halifax@stewartmckelvey.com

Moncton, NB
Suite 601, Blue Cross Centre
644 Main Street
Moncton, NB E1C 1E2
P 506.853.1970
F 506.858.8454
moncton@stewartmckelvey.com

Saint John, NB
Suite 1000, Brunswick House
44 Chipman Hill
Saint John, NB E2L 2A9
P 506.632.1970
F 506.652.1989
saint-john@stewartmckelvey.com

St. John's, NL
Suite 1100, Cabot Place
100 New Gower Street
St. John's, NL A1C 6K3
P 709.722.4270
F 709.722.4565
st-johns@stewartmckelvey.com