# Understanding and Preparing for Canada's Anti-Spam Legislation (CASL)



**Troy Baril, Associate**

Miller Thomson LLP
millerthomson.com

Miller Thomson
lawyers | avocats

# TABLE OF CONTENTS

# UNDERSTANDING AND PREPARING FOR CANADA'S ANTI-SPAM LEGISLATION

## Spam is Clogging the Internet

- Currently it is estimated that there are approximately 250 to 300 billion e-mails sent each day - 3 million to 3.5 million per second.
- Industry Canada currently estimates that spam represents 75% to 90% of all e-mail traffic.
- In the time it takes to read this sentence, 20 million e-mails were sent.
- It is estimated that the average North American office worker spends 11.2 hours per week reading and answering e-mails.

## Spam Delivers Other Threats

- Spam-born viruses are used to access large numbers of target computers and so spammers can then operate networks of zombie computers (botnets) to send their spam without the computer owner's knowledge.
- Spam has become the primary vehicle for the delivery of on-line threats such as spyware, malware and phishing.

## Spyware, Malware & Phishing

- Spyware - collects information or modifies the operation of a user's computer without the user's knowledge or consent
- Malware - viruses, worms and trojans
- Phishing - involves impersonating a trusted person or organization in order to steal your personal information

## Results of Spam

- All of these on-line threats:
    - Disrupt commerce
    - Perpetrate frauds and thefts
    - Reduce confidence in the on-line marketplace
    - Congest networks
    - Threaten the stability of the Internet and on-line services; and
    - Undermine personal privacy

## Anti-Spam Legislation

- Most of the industrial world has been adopting anti-spam legislation since the turn of the century
    - Japan – since 2002

- U.S. – since 2003
- U.K. – since 2003
- China – since 2005

## Did Canada Go Too Far?

- Canada was late to the game.
- Decided to create the strongest regime in the world.
- Concerns:
  - Description of a Commercial Electronic Message is too broad;
  - Opt-in consent is too onerous;
  - Too short a time period to obtain consents;
  - Social media changes much faster than laws and this will create unintended violations;
  - IT dependent and smaller organizations can't afford an IT solution;
  - Numerous exceptions in CASL will only lure many into the trap of believing they are exempt. The exceptions apply to classes of messages rather than classes of senders and eventually all organizations will send some messages that are caught by CASL;

## Concerns with Enforcement of CASL

- It regulates e-mail not spam.
- Spam is the sending of large batches of unsolicited e-mails.
- CASL applies to every single message or e-mail.
- It regulates commercial electronic messages – essentially:
  - e-mail;
  - but also blogs, texts, tweets & electronic newsletters.
- Potential for enforcement against ethical, law-abiding organizations. Will not deter a criminal in a foreign unregulated country.
- There will be 3 federal agencies responsible for enforcement of this law (CRTC, Competition Bureau, Federal Privacy Commissioner).
- There will also be a private right of action that will permit individuals and organizations to bring a lawsuit against someone who they allege has violated the law.
- Fines are 100 times higher than for privacy legislation.
- Monetary penalties:

  - Up to $10 million for corporations
  - $1 million for individuals

- Contrast with privacy legislation:

  - $100,000 for corporations
  - $10,000 for individuals

## Why Comply

- For these reasons:

  - It regulates e-mail not spam, and we all send e-mail
  - 3 federal agencies enforcing it
  - Significant fines
  - Private prosecutions

- We recommend you take this legislation seriously.

- Do everything you can to be in compliance with the legislation, as it came into force on July 1, 2014.

## What CASL Regulates

- Sending electronic messages without prior consent – this is the anti-spam portion of the legislation which will be enforced by the **CRTC**.

- Altering transmission data without express consent – this is what happens when you click on a link thinking it will take you to a specific web page and it takes you somewhere else. This will be regulated by the **CRTC**.

- Installing a computer program without express consent. This is installation of malware, spyware and viruses hidden in spam messages or downloaded through links to infected websites. This will be regulated by the **CRTC**.

- The legislation also addresses the use of false or misleading representations and deceptive marketing practices for on-line promotions. This will be regulated by the **Competition Bureau**.

- The collection of personal information through access to computer systems (phishing, data harvesting). This is done for identity theft or for electronic address harvesting. This will be regulated by the Office of the **Privacy Commissioner of Canada**.

- Collection of personal information for identity theft etc. is addressed in CASL but is also a violation of the Criminal Code of Canada and will be enforced by the **police**.

## Noble Goals BUT Will It Be Effective?

- Noble goals that we can all support.

- Will CASL stop spam???

- OR will it just catch legitimate businesses that are caught unaware?

- The U.S. has had anti-spam legislation since 2003, yet is currently considered the world's worst spam-producing country, followed closely by China (which has the death penalty in their anti-spam legislation).

- Many criminals and unethical individuals will not be deterred by laws.

## What is Canada's Anti-Spam Law ("CASL")?

- **Full title is**: 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, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23)

- Unofficial short title - "Canada's Anti-Spam Legislation" or "CASL"

## CASL – What's Covered

- Regulates a broad range of activities including:

    - the sending of commercial electronic messages ("CEMs")
    - the installation of a computer program on another person's computer system
    - altering of transmission data in an electronic message

    ➔ All of which require consent

## In Force Dates

- CASL received Royal Assent in December 2010.

- Regulations publicly presented on December 4, 2013.

- Majority of CASL came into force July 1, 2014

    - The window of opportunity to become compliant prior to CASL coming into force has now closed. However, this does not mean you should stop working on compliance.

- January 15, 2015 – in force date for provisions related to computer programs.

- July 1, 2017 – in force date for private right of action.

- July 1, 2017 – implied consent for existing relationships expires.

## Will CASL Apply To My Organization?

- Anti-spam provisions are very broad.

- CASL has the potential to impact any individual or organization in Canada that sends electronic messages to an electronic address (i.e. business, consumer, individual).

- Threshold issue – is it a commercial electronic message?

## Commercial Electronic Messages

- A commercial electronic message (CEM) is an electronic message that, having regard to:

  - the content of the message,
  - the hyperlinks in the message to a website, or
  - the contact information contained in the message,

  it would be reasonable to conclude the CEM has, as one of its purposes, to encourage participation in a commercial activity, including marketing, advertising or promotions.

- CASL focuses on the message, not the sender.

- **Threshold issue is whether it is "commercial"**

- Commercial activity includes any conduct of a commercial character whether or not it is "in the expectation of profit."

## Three Key Requirements of CEMs

- Consent requirements:

  - The onus is on the sender to prove they have consent
  - Opt-out consents are not allowed

- Information requirements:

  - Clearly identify sender
  - Clearly give recipient the right to unsubscribe

- Unsubscribe mechanism:

  - Must be clearly and prominently set out
  - Must occur within 10 days

**KEY MESSAGE**

## Consent Requirements

- CEMs may only be sent with recipient's express or implied consent.

- Previous consents are not sufficient to satisfy CASL.

- Onus of proving consent rests with sender (due diligence).

- Express consent must also be sought for:

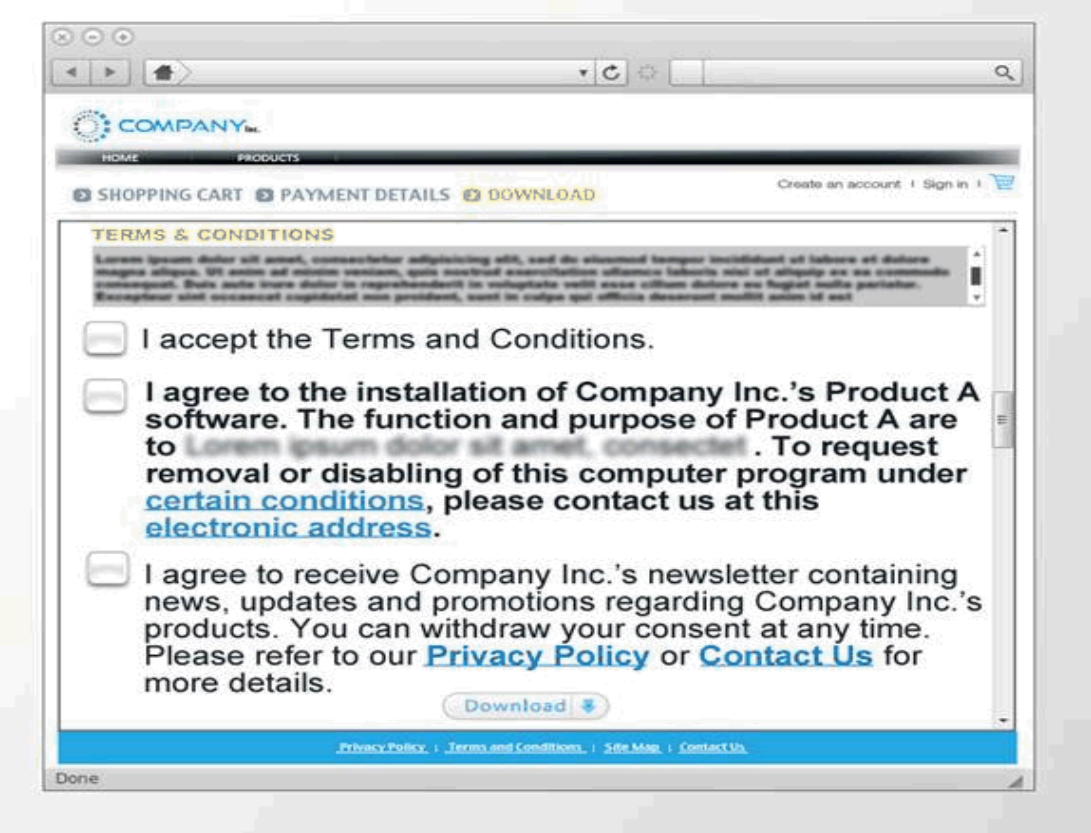
  - alteration of transmission data in electronic messages;

  - installation of a computer program on another person's computer in the course of a commercial activity.

- Express consent must be "sought separately" for each act contemplated under CASL.

- Must be distinct / cannot be bundled with terms and conditions of use or sale or other types of consent (eg. privacy).

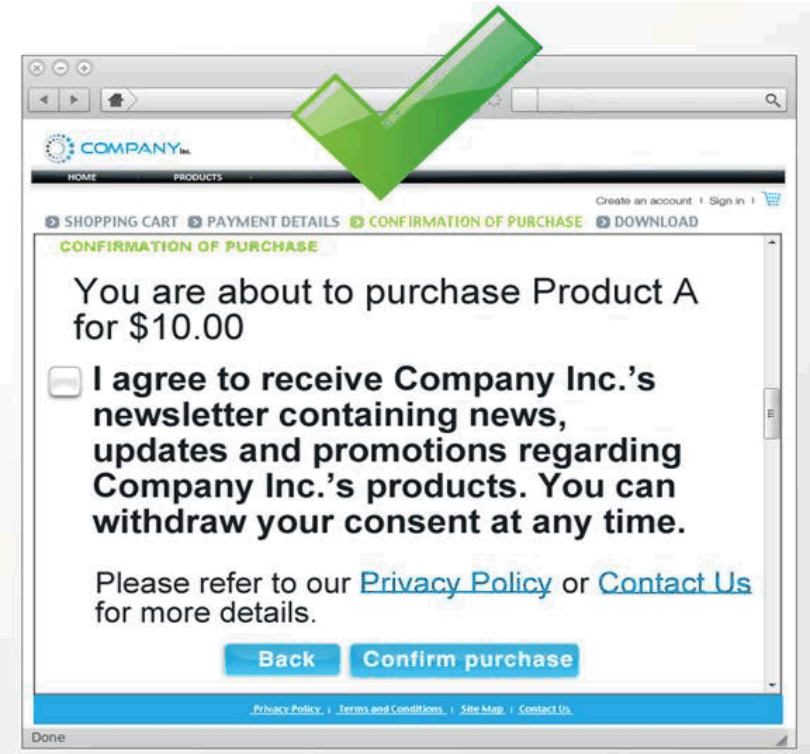
**Consent Requirements – (Example from CRTC 2012-548)**



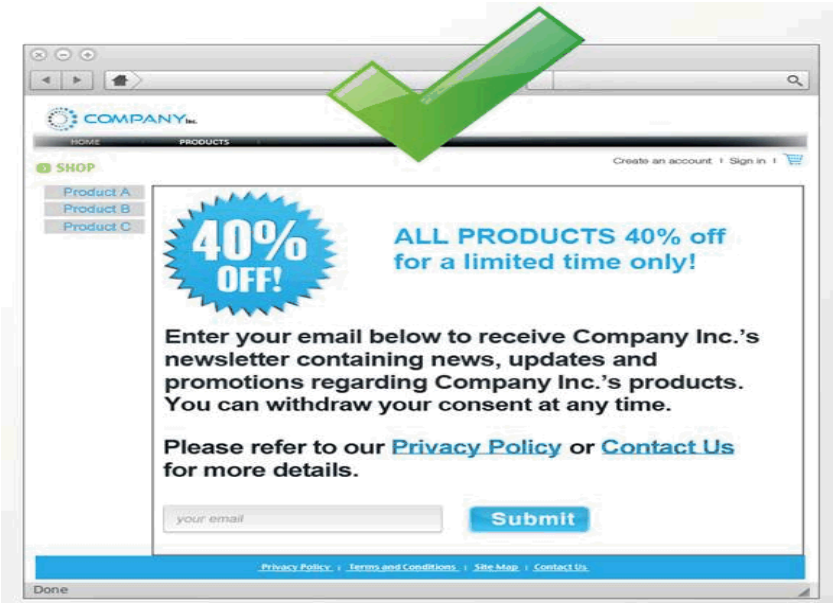

**Consent Requirements to Send CEMs (CRTC Regulation)**

- Request for express consent may be obtained orally or in writing or a combination thereof.
- Oral consent must be verified by an independent third party or a complete, unedited recording must be retained.
- Written consent includes both paper and electronic forms.
- Electronic forms must record date, time, purpose and manner of the consent.
- Opt-out consent is not sufficient under CASL
    - CRTC requires a positive or explicit indication of consent (i.e. providing e-mail address or checking toggle box).
- Onus is on sender to prove consent
    - Written consent – may be a paper based form or recorded in an electronic database (consider recording date, time, purpose and manner of consent in database) (CRTC 2012-548).

## Consent Requirements – Examples (CRTC 2012-549) (checked box)




## Consent Requirements – Examples (CRTC 2012-549) (typing e-mail address)



## Information Requirements

- Purpose of consent.
- Clearly identify the sender and any party it is sent on behalf of.
- Sender's contact information (name, company, mailing address, phone number and e-mail).
- Clearly inform the recipient of the right to unsubscribe from receiving future messages.

## Requirements For Unsubscribe Mechanism

- Must allow recipient to advise sender to stop sending electronic messages.
- Must be clearly and prominently set out in message.
- Must set out an electronic unsubscribe process or address, or link to an "unsubscribe" page.
- Must be effective for 60 days.
- Must be given effect within 10 days following receipt.
- Must be at no cost to recipient.

## Transitional Period for Existing Relationships

- CASL provides for a 3 year transition period after being declared in force, during which time there will be an implied consent for parties who are already in an **existing business or existing non-business relationship**.
- Implied consent is **only valid until July 1, 2017** for these two categories of existing relationships.
- After that you need express consent for them.

## Implied Consent – "Existing Business Relationship"

- Consent is implied if in the two years prior to the sending of the CEM, the recipient had a business relationship with the sender arising from:
    - The recipient has bartered, purchased or leased a product, good, service, land or an interest or right in land from the sender.
    - The recipient has accepted a business, investment or gaming opportunity offered by the sender.
    - A written contract between the sender and recipient of the CEM was in existence anytime in the two years prior to sending the CEM.

## Implied Consent – "Existing Non-Business Relationship"

- Consent to sending of CEM implied where there is an "existing non-business relationship"
    - Sender is a registered charity, political party or candidate for office, and recipient made a donation or performed volunteer work in the preceding two years.
    - Sender is a club, association or voluntary association, and recipient has been a member in the preceding two years.

## Exceptions to Consent, Information and Unsubscribe Requirements

- Messages sent for purposes of law enforcement, public safety, conduct of international affairs or protection of Canada.
- Messages sent from one person to another person if they have an existing "family relationship" or "personal relationship."
- Messages sent to a person engaged in a commercial activity containing an inquiry or application regarding that activity.
- Messages sent internally within an organization where the messages concern the activities of the organization.
- Messages sent from one organization to another organization where there is a relationship and the message concerns the activities of the organization.
- Messages sent in response to a request, inquiry or complaint or otherwise solicited by the recipient.
- Messages sent in regard to legal or judicial orders, rights or obligations.
- Messages sent to a secure, confidential limited-access account such as a message sent by your bank to your electronic bank account address than can only be accessed by you.
- Messages sent to a foreign state so long as you comply with that state's anti-spam law.
- Canadian registered charities will have a limited exemption where they send an electronic message primarily for fundraising purposes, but not for other purposes.
- Messages sent by political parties or politicians to solicit political contributions.

## Exceptions to Consent BUT Information and Unsubscribe Requirements Remain

- A message that responds to a requested quote or estimate.
- A message that facilitates, completes or confirms a commercial transaction previously agreed to.
- A message that provides warranty information, product recall information or safety information about goods or services purchased.

- Factual information about an ongoing purchase of goods or service offered under a subscription, loan, membership or similar relationship.

- Information directly related to an employment relationship or benefit plan.

- A message about product, good or service upgrades or updates.

- A message to a recipient who conspicuously published their electronic address (eg. Business card, website) and the message is relevant to the recipient's business role, functions or duties.

- A message to a recipient who disclosed their electronic address (eg. In a conversation or letter) and the message is relevant to the recipient's business role, functions or duties.

- A message sent to a referral from a common contact but only the first CEM.

## Social Media Exemption

- A CEM that is sent and received on an ***electronic messaging service*** if the information and unsubscribe mechanism are conspicuously published and readily available on the ***user interface***, and the person to whom the message is sent consents to receive it either expressly or by ***implication***.

- **Q.** Is "friending" or "following" someone implied consent?

## What is the Risk of Not Complying with CASL?

- Penalties focus on significant economic disincentives.

- Administrative monetary penalties ("AMPS"):

    - Individuals – **fines up to $1 million/violation**;
    - Other Persons – **fines up to $10 million/violation**.

- Private right of action (class actions) as of July 1, 2017 including right to statutory damages to a maximum of $1,000,000 per day ($200 for each electronic message sent).

- Complaints to Anti-Spam Reporting Centre.

- Private Actions.

- Class Actions.

- Cost, effort and embarrassment defending a prosecution.

- Reputational/PR risk.

- Extended liability – officers, directors and others.

## Extended Liability

- Liability extends to any person who acts, induces or procures a prohibited act.
- Employers are liable for acts of their employees who are acting within the scope of the employee's authority.
- Liability extends to officers and directors if they directed, authorized, acquiesced in or participated in the offending conduct.

## Defences

- Individuals and organizations may be able to rely upon a due diligence defence against claims of non-compliance.
- Your organization needs to be able to demonstrate that it has taken proactive steps to establish policies, procedures and processes to address CASL compliance and properly monitor and enforce those policies.

## Due Diligence is Critical

- S.33(1) "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."
- S. 54 "A person must not be found to have committed a contravention" . . . <of CASL> . . . "if they establish that they exercised due diligence to prevent the contravention or conduct . . ."

## How Do You Prepare For CASL

***First - CASL Audit***:

- Conduct a preliminary audit to understand what electronic messages your organization sends (emails, Christmas cards, marketing materials, Twitter account, Facebook account, etc.) and who to (suppliers, customers, contacts, potential clients or customers, etc).
- Conduct a closing audit after you have completed all of your CASL compliance steps to go back and double check that nothing has slipped through the cracks.

***Second – CASL Compliance Policies***:

- Develop an internal CASL compliance policy.
- Conduct in-house training for staff for CASL compliance.
- Develop a website CASL compliance statement.
- Update your privacy policies.

**NOTE: These steps are critical as there are defence provisions in CASL that state: A person must not be found liable for a violation or contravention if they establish that they exercised due diligence to prevent the commission of the violation or contravention.**

***Third – Obtain Consents***:

- Send an email to all of your current contacts requesting consent to send CEMs.
- Prepare consent forms to use for new contacts and customers and then use them for each new contact/customer.
- Insert consent requests into all relevant documentation (contracts, marketing materials, responses to quotes, RFP's etc).
- Insert consent requests into all on-line forms.
- Address "Consent, Information & Unsubscribe" requirements with any third parties that send out CEMs for you.
- Create a record keeping system to record consents and unsubscribes.

***Fourth – Provide the Required Information***:

- Every email and electronic message should contain the sender's name and contact information and the information of any party the CEM is sent on behalf of.
- Every email and electronic message should contain a statement that the recipient can unsubscribe from receiving further electronic messages.
- Every email and electronic message should have an unsubscribe mechanism. (Even if it is just a statement saying they can unsubscribe by hitting reply and typing in "unsubscribe" on the subject line).

***Fifth – Unsubscribe Mechanism:***

- Create systems or IT solutions to ensure unsubscribe requests actually take effect within 10 days of receipt.
- Keep records of unsubscribes.

## How Can We Help?

Miller Thomson can provide a wide spectrum of CASL compliance services for you to choose from.

We have found that some sole proprietorships, small businesses and Not-for-Profits want a simple, inexpensive solution. In these situations we can provide basic wording for documents, contracts, email consent forms and a CASL policy to adopt. This is generally 5 to 10 hours of legal work per organization.

For larger or more sophisticated organizations that require more comprehensive services we offer a suite of services that you can choose from.

We generally start with a discovery meeting at our client's offices with 5 or 6 of the key people (IT, Marketing, Risk Management & Executive Committee). During this meeting we review CASL requirements in the context of your organization.

With some groups we join their CASL compliance working group and attend weekly meetings with the core planning group until you have a handle on what you need to do.

The first task we give our clients is to have you complete an audit listing all of the electronic messages you send.

From that starting point we can then create a CASL workplan which we fully develop in consultation with you over a couple of weeks and several meetings. Once the workplan is complete we can put the work plan on an excel spread sheet, project management template or Gantt chart so that can be used to manage your CASL compliance project.

You can then effectively manage your CASL compliance.

We usually break the work plan into phases.

**Phase One - essential items that must be completed to fully understand what your organization needs to do to be compliant with CASL:**

1. Review internal audit and develop a workplan

2. Conduct a CASL analysis of completed audit - what is exempt; what needs to be dealt with immediately; and what can wait for the 3 year transition period.

3. Create model language to put in agreements, consent forms, emails etc

4. Provide recommendations and develop consent tracking and unsubscribe processes

5. Develop CASL policies and guidelines

6. Provide boilerplate language for insertion in 3rd party contracts, updating of privacy policies, appoint a CASL compliance officer

**Phase Two - training phase**

1. Core group and general training of staff
2. Train the trainers

**Phase Three - Ongoing**

1. Ongoing advice
2. Ongoing monitoring of compliance
3. Closing audit
4. Ongoing employee training

We can either provide an annual or monthly retainer agreement where key staff have unlimited access to Miller Thomson lawyers to ask questions at a set rate per month or we can provide this service at our usual hourly rates.

## Remember

- Even if relying upon the 3-year transition, start gathering consents as soon as possible.
- Many of the requirements are IT dependant.
- Now is the time to prepare to obtain consent electronically.
- Now that July 1, 2014, has passed it will be an offence to send an e-mail to get consent, unless you have implied consent pursuant to an existing business or non-business relationship with the recipient.

## Additional Information

- Main government website - **www.fightspam.gc.ca**.
- Sign up for Miller Thomson's CASL Updates and visit our website, **www.millerthomson.com** as we continue to develop resource materials and compliance tools.

Please do not hesitate to contact Troy Baril, Miller Thomson's Saskatchewan Region CASL Compliance Leader, if you have any questions or wish to discuss your firm's CASL compliance needs further.

Troy Baril
306.667.5630
tbaril@millerthomson.com

VANCOUVER

CALGARY

EDMONTON

SASKATOON

REGINA

LONDON

KITCHENER-WATERLOO

GUELPH

TORONTO

MARKHAM

MONTRÉAL

Miller Thomson LLP
**millerthomson.com**

Miller Thomson
lawyers | avocats