



HORIZONTAL EVALUATION OF CANADA'S ANTI- SPAM LEGISLATION (CASL)



MARCH 2018

Table of Contents

<i>page</i>	<i>page</i>	<i>page</i>	<i>page</i>	<i>page</i>
i	ii	1	6	9
<hr/>	<hr/>	<hr/>	<hr/>	<hr/>
Executive Summary	Acronyms	Background	Methodology	Findings
<hr/>	<hr/>	<hr/>	<hr/>	<hr/>

<i>page</i>	<i>page</i>	<i>page</i>	<i>page</i>
19	20	21	27
<hr/>	<hr/>	<hr/>	<hr/>
Conclusions	Recommendations	Appendices	Endnotes
<hr/>	<hr/>	<hr/>	<hr/>

This publication is available online at https://www.ic.gc.ca/eic/site/ae-ve.nsf/eng/h_00351.html

To obtain a copy of this publication or an alternate format (Braille, large print, etc.) please fill out the Publication Request Form at www.ic.gc.ca/Publication-Request or contact:

Web Services Centre
Innovation, Science and Economic Development Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (Ottawa): 613-954-5031
TTY (for hearing-impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. Eastern Standard Time
Email: info@ic.gc.ca

Permission to Reproduce

Except as otherwise specifically noted, the information in this publication may be reproduced, in part or in whole and by any means, without charge or further permission from Innovation, Science and Economic Development Canada, provided that due diligence is exercised in ensuring the accuracy of the information reproduced; that Innovation, Science and Economic Development Canada is identified as the source institution; and that the reproduction is not represented as an official version of the information reproduced, nor as having been made in affiliation with, or with the endorsement of, Innovation, Science and Economic Development Canada.

For permission to reproduce the information in this publication for commercial purposes, please fill out the Application for Crown Copyright Clearance at www.ic.gc.ca/copyright-request or contact the Web Services Centre mentioned above.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of Innovation, Science and Economic Development Canada, 2018.

Cat. No. lu4-230/2018E-PDF
ISBN 978-0-660-26837-8

Aussi offert en français sous le titre *Évaluation Horizontale de la Loi Canadienne Anti-Pourriel (LCAP)*

Executive Summary

ABOUT THE EVALUATION

As CASL is in its early stages, this evaluation assessed the achievement of immediate outcomes by examining components of the compliance continuum; governance; and, the extent to which the impact of CASL can be measured. Using qualitative and quantitative research methods, the evaluation covered the period from 2010-11 to 2016-17.

WHAT THE EVALUATION FOUND

Roles and responsibilities have been defined and mechanisms exist to facilitate the management and delivery of CASL. However, the oversight role of the NCB could be strengthened and the role of OCA clarified. Further, there is an opportunity to improve cohesion among partners, especially between the enforcement agencies and non-enforcement partners. In addition, CASL partners have established international relationships to share information and leverage joint efforts where possible. However, except as it relates to CB, there are no provisions for information sharing with other non-CASL domestic partners, which limits cooperation for compliance activities.

To promote compliance with CASL, each delivery partner conducts education and outreach activities. However, these activities are not coordinated and many aspects of CASL may not be well understood by businesses such as SMEs. Currently, the SRC collects intelligence to monitor compliance and support the enforcement agencies. There may be opportunities for SRC data to support information sharing among the CASL partners and in activities that promote compliance.

CRTC, CB and OPC have distinct powers and processes for investigating and responding to non-compliance. 36 investigations have been completed and a range of compliance actions have been taken since 2014-15. There is a perception by external stakeholders that some types of compliance actions may better promote awareness of CASL.

Although it is too early to conclude on impact, the evaluation found that there are limited data sources available to assess the impact of CASL on the electronic marketplace.

INITIATIVE DESCRIPTION

Canada's Anti-Spam Legislation (CASL) aims to protect Canadians from spam, electronic threats and misuse of digital technology. CASL was passed in 2010 and the majority of provisions came into force in 2014 with a three-year transition period to allow time for consumers and businesses to become aware of and comply with the legislation.

CASL is delivered by:

- *Innovation, Science and Economic Development Canada (ISED): National Coordinating Body (NCB), Office of Consumer Affairs (OCA) and Competition Bureau (CB);*
- *Canadian Radio-television and Telecommunications Commission (CRTC) including the Spam Reporting Centre (SRC); and*
- *Office of the Privacy Commissioner of Canada (OPC).*

The compliance continuum reflects the key activities that partners undertake to promote compliance, monitor compliance, investigate non-compliance and respond to non-compliance.

RECOMMENDATIONS

1. To improve cohesion, the CASL partners should re-examine the existing governance structure including roles and responsibilities and the supporting committees.
2. The National Coordinating Body should work with CASL partners to strengthen information sharing in order to facilitate the management and delivery of CASL. Consideration should be given to the sharing of aggregate Spam Reporting Centre reporting data.
3. As appropriate, the CASL partners should collaborate and develop a coordinated approach to education and outreach activities to improve the understanding of CASL by businesses, as well as the impact and reach of these activities.
4. The National Coordinating Body, in collaboration with the delivery partners, should strengthen its data collection capacity to ensure that performance information is available to assess the impact of CASL.

Acronyms

AMPs	Administrative Monetary Penalties
CASL	Canada's Anti-Spam Legislation
CB	Competition Bureau
CRTC	Canadian Radio-television and Telecommunications Commission
ISED	Innovation, Science and Economic Development Canada
MOU	Memorandum of Understanding
NCB	National Coordinating Body
OCA	Office of Consumer Affairs
OPC	Office of the Privacy Commissioner of Canada
PIPEDA	<i>Personal Information Protection and Electronic Documents Act</i>
SMEs	Small- and medium-sized enterprises
SRC	Spam Reporting Centre

Background

Context

CASL Description

CASL Environment

Compliance Continuum

Context

Unsolicited commercial electronic messages, known as spam, are a global challenge. Spam has become a significant social and economic issue and a disruption to the productivity of businesses and consumers. More than 90% of emails sent globally each day were spam in 2015.¹ As well, it is estimated that spam costs the Canadian economy more than \$3 billion per year.²

In addition to spam, there are other electronic threats such as identity theft, phishing, false and misleading content and malware that have become more sophisticated and widespread. Spam and electronic threats continue to disrupt electronic commerce and reduce business and consumer confidence in the electronic marketplace, impose heavy costs on network operators and users, threaten network reliability and security, and undermine personal privacy.

While spam and electronic threats can be caused by illegitimate actors from around the world, legitimate businesses can also knowingly or unknowingly cause harm to consumers and the electronic marketplace. Consumers and businesses benefit from a decrease in unsolicited commercial electronic communication, as trust in electronic means of communications and those who use them for commercial purposes is essential to the prosperity of the Canadian economy.

Prior to 2010, Canada was the only G8 country without anti-spam legislation. At the time, technological solutions alone had proven largely ineffective in stemming the growth and impact of spam and related threats. Industry continued to make efforts but were hindered by the lack of legal prohibitions to prevent spam and other electronic threats from originating and occurring in Canada.

To deter spam and other electronic threats, Canada's Anti-Spam Legislation (CASL) was passed in 2010. Apart from certain changes to PIPEDA introduced by CASL in 2011, the majority of CASL's provisions came into effect in 2014. CASL aims to protect consumers against spam, electronic threats and misuse of digital technology while ensuring businesses remain competitive in a global digital marketplace.³



CASL Description

CASL is designed to help protect Canadians from spam and other electronic threats received from either legitimate businesses or illegitimate actors. The legislation establishes a regulatory framework consistent with international best practices and contributes to the Government of Canada's efforts to "improve economic opportunity and security for Canadians".⁴

Through CASL, Canada has adopted an opt-in consent model where senders may only send a commercial electronic message if they request consent first, or meet an exception or exemption (see Appendix A). CASL is technology neutral, meaning that it is intended to apply to all forms of electronic communication. It aims for a balanced approach that protects the interest of consumers and organizations that have legitimate reasons for communicating electronically. The expected outcomes of CASL are described in Appendix B.

Activities prohibited by CASL include:⁵

- sending of commercial electronic messages without the recipient's consent (permission), including messages to email addresses and social networking accounts, and text messages sent to a cell phone;
- alteration of transmission data in an electronic message which results in the message being delivered to a different destination without express consent;
- installation of computer programs without the express consent of the owner of the computer system or its agent, such as an authorized employee;
- making false or misleading representations to the public in the form of electronic messages;
- collection of personal information through accessing a computer system in violation of federal law (e.g. the Criminal Code of Canada); and
- collection of electronic addresses by the use of computer programs or the use of such addresses, without permission (address harvesting).

Canada's Anti-Spam Legislation

*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.*⁶

CASL had a three-year transition period to allow time for businesses and consumers to become aware of and comply with consent requirements.

July 1, 2014

Majority of provisions came into force.

January 15, 2015

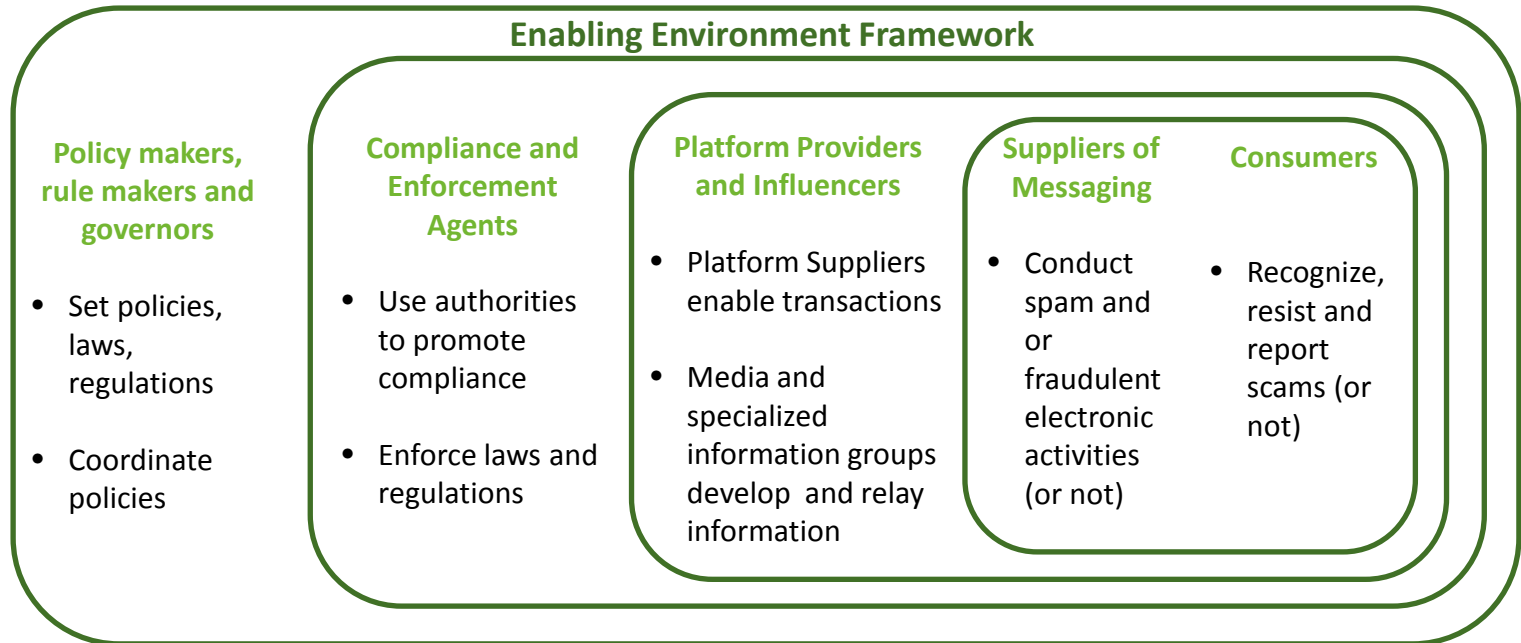
Sections of the Act related to requiring consent to install computer programs came into force.

July 1, 2017

Suspended: Private Right of Action provisions were to come into force.

CASL Environment

The electronic marketplace system in which CASL exists is complex. CASL is part of a broader range of domestic and international legal and policy frameworks in the areas of spectrum, telecommunications, privacy protection and cyber resilience, including cyber security.



The enabling environment of CASL can be viewed as a system with five key actors including legislators and policymakers, compliance and enforcement agents, business platform providers and influencers, suppliers of messaging, and consumers.

To implement CASL, approximately \$69 million over seven years (2010-11 to 2016-17) was allocated to:

- Innovation, Science and Economic Development Canada (ISED) specifically the National Coordinating Body (NCB), Office of Consumer Affairs (OCA) and Competition Bureau (CB);
- Canadian Radio-television and Telecommunications Commission (CRTC), the main enforcement agency of CASL, including the Spam Reporting Centre (SRC); and
- Office of the Privacy Commissioner of Canada (OPC).

The non-enforcement partners of CASL are NCB and OCA, and the enforcement agencies are CRTC, CB and OPC.

Compliance Continuum

The compliance continuum reflects the key activities that the delivery partners undertake to encourage compliance with CASL. The continuum is not linear and its components are interrelated. Results of one component of the continuum can influence results of other components.



Methodology

*Evaluation Context and
Considerations*

Methods of Data Collection

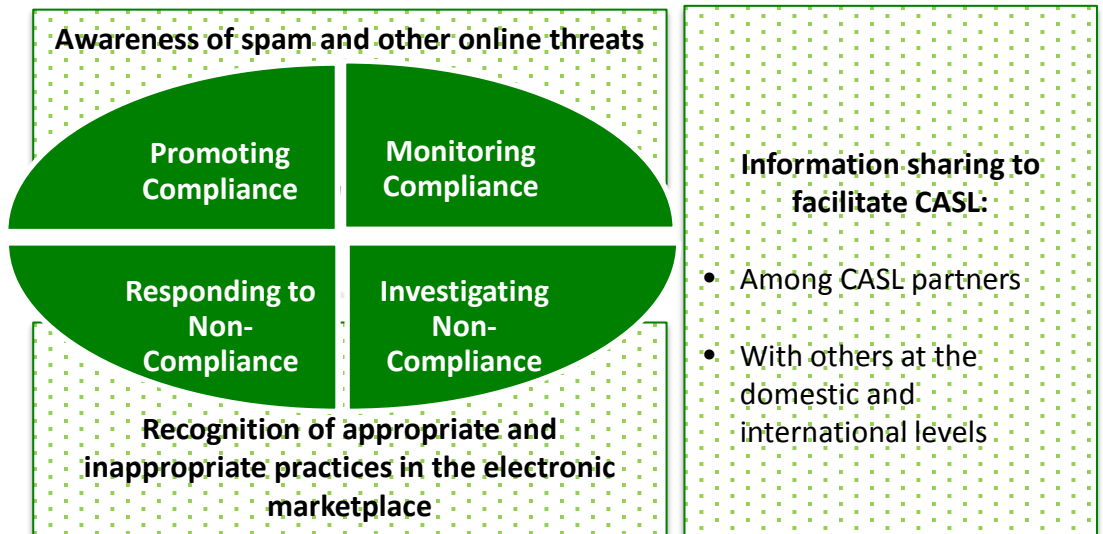
Evaluation Context and Considerations



The objectives of this evaluation were to provide early insights regarding the implementation of CASL and to identify areas where delivery could be improved.

An evaluation of CASL was required in 2017-18 to meet policy commitments. This is the first evaluation of CASL and covers the period from 2010-11 to 2016-17.

As CASL is in its early stages, this evaluation focused on the achievement of immediate outcomes (see Appendix B) in terms of what works, for whom, and in what circumstances by examining components of the compliance continuum as follows:



The evaluation also examined governance and the extent to which the impact of CASL on the electronic marketplace can be measured. Performance data provided for the evaluation is only available commencing in 2014-15, when the majority of CASL provisions came into force. Details on the evaluation limitations can be found in Appendix C.

The evaluation was conducted by the Audit and Evaluation Branch of ISED. It is separate from the 2017 legislative review completed by the House of Commons Standing Committee on Industry, Science and Technology.⁷

Methods of Data Collection

This evaluation is based on qualitative and quantitative research methods from both primary and secondary data sources.

Document Review

Review of documents including:

- Foundational documents
- External documents such as research papers and articles
- Government priority-setting documents

Interviews

Conduct of 40 semi-structured individual and small group interviews with:

- CASL delivery partners (20)
- External experts and stakeholders (20)

Administrative and Financial Data

Provided by the delivery partners including:

- Performance reports
- Initiative-related operational data
- Human resource and financial data

Service Blueprint

Process mapping of spam reporting from the consumer perspective, developed from data analysis, SRC site visits and interviews with CASL enforcement agencies (Appendix D). This was used as a line of evidence to assess how the SRC supports awareness of CASL and operations of the enforcement agencies.

Comparative Analysis

Analysis of anti-spam legislation in Canada, Australia, UK and US (Appendix E). This was used to assess how Canada's anti-spam legislation with its opt-in model and enforcement capabilities compared with other countries.

Secondary Sources of Survey Data

Surveys conducted from 2012 to 2017:

- *Canadian Anti-Spam Act survey: Bill C-28*⁸
- *Canada's Anti-Spam law is effective, but it's harming Canadian businesses*⁹
- *CASL Experience of Organizations*¹⁰
- *CASL Survey Report: Bridging the Gaps in Understanding and Compliance*¹¹
- *Understanding Canadian reactions to CASL*¹²

Findings

Governance

Information Sharing to Facilitate CASL: Among CASL Partners

Information Sharing to Facilitate CASL: With International and Domestic Partners

Promoting Compliance




Monitoring Compliance

Investigating and Responding to Non-Compliance

Impact of CASL on the Electronic Marketplace

Finding: Roles and responsibilities of the CASL partners were defined at the outset and governance mechanisms exist to support delivery. However, the oversight role of the National Coordinating Body could be strengthened and the role of the Office of Consumer Affairs clarified. Further, there is an opportunity to improve cohesion among partners.

Roles and responsibilities of the partners have been set out in foundational documents and legislative mandates, as follows:

<p><i>Non-Enforcement</i></p> 	<p>NCB</p> <ul style="list-style-type: none"> • Policy oversight, including monitoring and reporting • Oversight of public communication and outreach activities • Support to the enforcement agencies 	<p>OCA</p> <ul style="list-style-type: none"> • Lead and coordinate consumer and small business education and awareness of CASL, including the management of the FightSpam website
<p><i>Enforcement</i></p> 	<p>CRTC - Through CASL:</p> <ul style="list-style-type: none"> • Enforce and investigate violations of prohibitions against the sending of spam, the alteration of transmission data, and the installation of computer programs into computer systems and/or networks without consent • Encourage compliance through outreach, sanctions and remedies for violations such as AMPs <p>CB - Through amendments to the <i>Competition Act</i>:</p> <ul style="list-style-type: none"> • Encourage compliance, enforce and investigate cases of false or misleading electronic representations • Encourage compliance with CASL-related <i>Competition Act</i> provisions through outreach, sanctions and remedies for violations such as AMPs <p>OPC - Through amendments to the <i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i>:</p> <ul style="list-style-type: none"> • Enforce and investigate the unauthorized collection and use of electronic addresses by using computer programs, and the unauthorized collection and use of personal information through any means of telecommunication made by accessing a computer system • Encourage compliance with CASL-related PIPEDA provisions through outreach and remedies (excluding AMPs) 	
<p><i>Intelligence Gathering</i></p> 	<p>Spam Reporting Centre (SRC)</p> <ul style="list-style-type: none"> • Housed within the CRTC, primarily to support the enforcement agencies • Receives submissions and reports of spam and other electronic threats • Gathers voluntarily provided or publicly available information to identify potential violations and support enforcement of CASL • Manages CASL information databases, allow access to databases by the enforcement agencies and report on trends and metrics 	

Governance

(continued)



Canada is unique when compared to the US, United Kingdom and Australia in that it engages multiple federal partners with different but complementary mandates to implement its anti-spam legislation.

A number of governance committees and mechanisms have been created to deliver CASL. To support all partners, two committees are chaired by NCB: a senior management committee and a working-level committee. These committees are the primary fora for all partners to discuss priorities, share information, avoid duplication and leverage joint efforts. Additionally, for the enforcement agencies:

- A Memorandum of Understanding (MOU) clarifies cooperation, coordination and information sharing between the agencies as they conduct their enforcement activities.
- An Enforcement Working Group including investigators from CRTC, CB and OPC meet on a regular basis to discuss potential and ongoing investigations.
- An SRC Working Group including representatives from the SRC, CRTC enforcement team as well as CB and OPC ensures that the SRC meets the needs of its users.

The evaluation found that the roles and responsibilities of the enforcement agencies are well understood and governance mechanisms are utilized by the agencies. However, there is less clarity for the non-enforcement partners (NCB and OCA).

With respect to NCB, interviewees indicated that they were unclear of the role of NCB in providing oversight given that each agency has clear and distinct legislative mandates. Evidence shows that most meetings of the committees chaired by NCB occurred up to 2014-15 for the coming into force of the majority of CASL provisions and establishment of the SRC. Since then, these committees have met on an infrequent and ad hoc basis.

As well, both NCB and OCA have roles related to coordinating communication and outreach activities, although, in practice, this is not occurring. Given its central enforcement role for CASL, the CRTC has played a primary role for CASL education and awareness. This approach minimizes the risk of providing conflicting interpretations of CASL to the public and stakeholders. Overall, the evaluation found that there would be benefits to more cohesion among all partners particularly between the enforcement agencies and non-enforcement partners.

Recommendation: To improve cohesion, the CASL partners should re-examine the existing governance structure including roles and responsibilities and the supporting committees.

Information Sharing to Facilitate CASL: Among CASL Partners

Spam Reporting Centre

- The SRC collects data that is used to investigate and respond to non-compliance.
- The enforcement agencies can individually access the SRC database to extract information for their own CASL-related mandates.
- The SRC produces aggregate quarterly reports of spam submission data such as the number of spam submissions by type and by reason. Upon request, these reports have been provided to partners such as NCB.
- Some CASL interviewees suggest that proactively sharing aggregate SRC data would help CASL partners, especially NCB and OCA, understand trends around electronic threats.
- Broader distribution of the existing reports on spam submissions would respond to the interest of having this information by CASL partners.

Finding: Information sharing among the enforcement agencies is effective. Although partners have distinct mandates, there are opportunities to enhance information sharing among all partners.

There are two levels of information sharing among the delivery partners:

Among the Enforcement Agencies

The enforcement agencies are able to share information with one another if it is related to CASL enforcement. The evaluation found evidence of information sharing to support parallel investigations. For example, CRTC and OPC shared information regarding their investigations of Compu-Finder. Compu-Finder was investigated by the CRTC primarily for sending unsolicited commercial electronic messages to recipients without prior consent and for failing to action unsubscribe requests, and was investigated by the OPC with regards to consent matters under PIPEDA and address-harvesting.

The evaluation also found that information sharing can be challenging particularly as the enforcement agencies' legislative mandates extend beyond CASL. For example, while OPC was conducting an investigation, it found information that could pertain to CB's mandate for ensuring truth in advertising. Since the information was not CASL-related, it could not be shared with CB.

Despite some challenges, the evaluation found that CRTC, CB and OPC have formed good working relationships to support the enforcement of CASL in view of their respective legislative mandates.

Among All Partners

While information sharing is essential as it encourages communication and enables coordination among partners that conduct similar activities, the evaluation found that information sharing has been limited largely given the challenges noted under the governance section. Interviews with CASL partners suggested that ongoing communication would help facilitate the implementation of CASL.

Recommendation: The National Coordinating Body should work with CASL partners to strengthen information sharing in order to facilitate the management and delivery of CASL. Consideration should be given to the sharing of aggregate Spam Reporting Centre reporting data.

Information Sharing to Facilitate CASL: With International and Domestic Partners

Finding: CASL includes provisions for information sharing between the enforcement agencies and international partners but, except as it relates to CB, there are no provisions for information sharing with other non-CASL domestic partners, which limits cooperation for compliance activities.

With International Partners

Data analysis and interviews show that CASL delivery partners participate in various international fora and networks and have established a number of international MOUs and bilateral agreements. This allows the partners to share best practices, become aware of investigations and leverage joint efforts where possible. Through MOUs, the partners have established relationships with over ten countries including Australia, the Netherlands, the United Kingdom and the United States.

In 2011, CASL amended PIPEDA to allow the OPC to share information and collaborate with domestic and international data protection agencies. For example in 2015, OPC and the Office of the Australian Information Commissioner conducted a joint investigation into the data breach of the Ashley Madison website that exposed the sensitive personal information of 36 million user accounts.

Also in 2015, CRTC executed its first warrant under CASL as a part of a coordinated international effort led by the US Federal Bureau of Investigation for an international botnet investigation that infected more than one million computers in over 190 countries.

With Domestic Partners

There are no explicit provisions for sharing CASL-related information outside of the CASL enforcement agencies with one exception. CB is able to share information, through pre-existing provisions of the *Competition Act*, with other law enforcement agencies, or where the information to be shared serves the purpose of administering or enforcing the *Competition Act*. While CRTC, CB and OPC have access to the SRC, other organizations do not, nor can SRC data be shared with organizations such as the Canadian Anti-Fraud Centre and the Royal Canadian Mounted Police. Interviewees suggested that restrictions on information sharing with domestic law enforcement and national security agencies significantly impact cooperation for compliance activities. While collaboration could assist in protecting Canadians from electronic threats, efforts to address these challenges are not within the control of CASL partners.



Promoting Compliance

Finding: Each delivery partner conducts education and outreach activities with the objective of promoting compliance with CASL. However, these activities are not coordinated and there are many aspects of CASL that may not be well understood.

To promote compliance, the partners conduct education and outreach to stakeholders which is intended to create awareness about the purpose, requirements and implications of CASL. These activities are essential to educate businesses about the legislation and to promote compliance with CASL.

CASL partners (primarily CRTC and OPC) conduct individual and joint communication and outreach activities with businesses, associations, law firms and other stakeholders. Examples of these activities include:

- **CRTC:** In 2014-15, CRTC conducted over 20 outreach activities, reaching over 3,500 organizations across Canada. CRTC also conducted an outreach tour that reached approximately 1,700 business representatives. Since 2015-16, CRTC has conducted more than 15 information sessions with industry representatives and 17 compliance outreach sessions.
- **OPC:** In 2014-15, OPC undertook multiple activities including presentations to Canadian businesses, organizations and individuals. Since 2015-16, approximately 29 activities have occurred including a speaking tour targeted to small businesses which included CASL information.
- **CB:** CB has a more limited role in CASL-specific communication and outreach activities. CB issues regular alerts to consumers and businesses regarding deceptive marketing practices, and publishes content and guidance on different topics to raise awareness of false and misleading marketing practices in the electronic marketplace. CB has participated in events such as a joint seminar hosted by the American Bar Association and the Canadian Bar Association.
- **OCA:** OCA manages the FightSpam website and, up to 2014-15, developed a number of infographics targeted at small- and medium-sized enterprises (SMEs) and individuals.
- **NCB:** NCB has not directly led outreach activities but has participated in joint sessions with the CRTC, and is the main contact when stakeholders reach out to the Minister of ISED about CASL-related matters.

The FightSpam website is the primary communication vehicle of CASL information to consumers and businesses. It acts as a conduit to the websites of the enforcement agencies. The enforcement agencies also provide mandate-specific guidance and compliance information through their own websites.

FightSpam visits:

- 885,000 in 2014-15
- 344,000 in 2015-16
- 369,000 in 2016-17

Promoting Compliance

(continued)



CASL partners also educate the public by integrating CASL-related content into general communication on topics such as consumer protection, privacy protection and cyber security. The reach of CASL communication and outreach activities to industry stakeholders, and the extent of public awareness of CASL, is unknown.

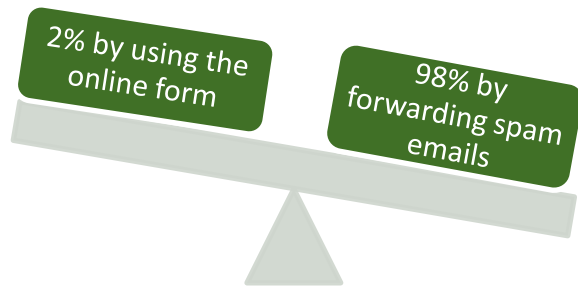
Despite these communication and outreach activities, the evaluation found that the frequency and types of outreach conducted vary by partner and that there is infrequent coordination among the partners even though the target audiences are similar. Further, it was found that there are many aspects of CASL that may not be well understood. A 2017 survey of over 200 SMEs¹³ and external interviewees suggested that guidance was insufficient for businesses. Through an analysis of administrative data, interviews and document review, the evaluation found a number of areas where CASL may not be well understood:

- **Basics of CASL:** Including the definition of commercial electronic messages, the requirements of consent and the various exceptions to CASL.
- **Intent of CASL:** Some external interviewees believe that deterring unsolicited messages from commercial businesses does not address more harmful threats to the marketplace such as those caused by illegitimate actors. CASL is intended to help deter various kinds of electronic threats. However, to date, the majority of compliance actions have been limited mainly to unsolicited commercial electronic messages, with few enforcement actions against other threats, such as those caused by illegitimate actors. This may influence the perception of external stakeholders and their understanding of CASL's broader purpose.
- **Reach of CASL:** Some external interviewees and 48% of respondents from a 2015 survey by Cyberimpact¹³ noted that CASL hinders their ability to compete with their international counterparts who may not comply with Canadian legislation. However, this concern is based on a misperception as CASL applies to both domestic and international companies sending commercial electronic messages to recipients in Canada.
- **Scope of CASL:** There is limited information on how CASL addresses harmful electronic threats beyond spam and on how CASL complements other Canadian and international efforts for consumer protection and cyber security.

Recommendation: As appropriate, the CASL partners should collaborate and develop a coordinated approach to education and outreach activities to improve the understanding of CASL by businesses, as well as the impact and reach of these activities.

Monitoring Compliance

The public can submit information about spam and electronic threats to the SRC by forwarding emails or by using an online submission form. The online form is rarely used but is the only mechanism to report electronic threats that are not received by email (e.g., threats received by text message).



Approximately 1.3 million submissions from the public to the SRC

CRTC is currently examining technical solutions to gather more data about malware and to receive forwarded text messages from the public.

Finding: The Spam Reporting Centre monitors compliance by gathering information that supports the enforcement agencies in investigating and responding to non-compliance. There may be opportunities for the SRC to support other activities to promote compliance and awareness of spam and online threats.

The SRC serves as a central repository of intelligence by gathering information about spam and other electronic threats. It contains records from public submissions, international reports and other data sources.

SRC data is used by the enforcement agencies to monitor compliance with CASL. As shown through the Service Blueprinting of Spam Reporting (see Appendix D), the SRC database is individually accessed by each enforcement agency who each individually determine how SRC data will be used. Evidence shows that the SRC helps the enforcement agencies investigate and respond to non-compliance. For example:

- Over 90% of CRTC intelligence reports use information from the SRC, and 86% of their investigations in 2014-15 were advanced using SRC data.
- OPC analyzed about 1000 submissions related to the Compu-Finder case.
- CB uses SRC information for general sweeps on trends, statistics to inform priorities and to advance investigations.

The evaluation found that there may be opportunities for SRC data to also be used to improve awareness of CASL. Interviewees suggested that greater awareness of CASL and the SRC would likely increase submissions to the SRC which would provide more information to the enforcement agencies. Further, they suggested that aggregate SRC data could be used for external communication products to promote compliance with CASL. It is important to note that CRTC does provide some aggregate SRC information in outreach presentations but there may be additional opportunities to share this type of information with the public.

Investigating and Responding to Non-Compliance

Examples of Investigations

CRTC conducted an investigation of an organization that allegedly sent commercial emails containing an unsubscribe mechanism that did not function properly or which could not be readily performed by the recipient.

CB investigated misleading advertising of companies that resulted in unauthorized charges to consumers. These companies agreed to refund/rebate customers and to donate to advocacy groups working in the public interest.

Finding: The enforcement agencies have conducted a number of investigations and issued a range of compliance actions. There is a perception that some types of actions may better promote awareness of CASL and, in turn, improve compliance.

Each enforcement agency has distinct powers and processes for investigating and responding to non-compliance of legitimate businesses and illegitimate actors. Decisions to pursue a potential investigation and issue a compliance action are based on a number of factors. While these factors vary slightly from partner to partner, in general they include:

- the nature, seriousness and impact of the violation;
- the history of non-compliance; and
- duration and scope of conduct at issue.

There are a number of actions the enforcement agencies can take to encourage compliance, ranging from warning letters to AMPs (excluding OPC) to litigation (in the case of CB).

Compliance Actions (2014-15 to 2016-17)		
CRTC	CB	OPC
<ul style="list-style-type: none"> • Warning letters (22) • Notices of violation (7) • Undertakings (4) • AMPs (\$1.9M) 	<ul style="list-style-type: none"> • Consent agreements (7) • AMPs (\$5.25M) • Rebates / refunds to affected consumers (\$24.58M) • Donations to advocacy groups working in the public interest (\$1.05M) • Payment of investigative costs to CB (\$350,000) 	<ul style="list-style-type: none"> • Compliance agreement (1) • Letters of Concern (6)

Investigations often carry over from year to year, as duration is dependent on the complexity and nature of the potential violations. Between 2014-15 and 2016-17, a total of 36 investigations were completed by the enforcement agencies (23 by CRTC, eight by CB and five by OPC). The majority of these have been related to spam and address harvesting.

Document review and an international comparative analysis indicated that Canada is considered one of the toughest anti-spam regimes in the world. Penalties for violations of CASL can go as high as \$1M for individuals and \$10M for businesses. External interviewees suggest that escalation approach to compliance actions (e.g. issuing warnings before AMPs) could help businesses better understand and comply before more severe penalties are imposed. However, compliance actions are taken based on an analysis of multiple factors. The evaluation found that there may be opportunities for the enforcement agencies to better explain the factors considered and the determination of penalties.

Impact of CASL on the Electronic Marketplace

Reduction of Spam Originating in Canada

In 2009, prior to the Royal Assent of CASL, spam represented over 90% of all email traffic in Canada. As of 2015, there was a 37% reduction in the volume of spam originating in Canada.²⁰ As well, Canada is no longer in the top 10 list of spamming countries reported by Spamhaus.²¹

This reduction can not be attributed solely to CASL as other mechanisms also protect consumers from electronic threats. For example, one in five emails are blocked by Internet Service Providers.²²

Finding: Given that CASL is in its early stages, there is little evidence to conclude on impact. Further, there is limited data available to assess the impact of CASL on the electronic marketplace.

Given that CASL is in its early years, it is too early to reach conclusions on the impact of CASL on the electronic marketplace. However, the evaluation identified some preliminary observations. To ensure that the impact of CASL can be fully assessed at a later stage, it will be important for the partners to identify appropriate data sources.

Impact on Businesses

While it was not the intent of CASL to cause unnecessary compliance costs, document review and interviews indicate that businesses incur set-up and ongoing operation costs to comply with CASL.¹⁴ The extent of these costs is unknown. Further, some SMEs may not have the resources to secure legal counsel and technology that would allow them to operate in compliance with the provisions of CASL.

Evidence also suggests that as a consequence, some businesses may be choosing to reduce electronic marketing.¹⁵ A 2017 survey found that 42% of businesses have decreased their reliance on electronic marketing and 7% have stopped using electronic marketing altogether.¹⁶ The impact of these costs and the changes to business practices on the ability to compete is unknown.

Impact on Consumers

The opt-in model for consent is meant to encourage businesses to enhance data clean up and processes to manage communication with consumers.¹⁷ Data show that since CASL's implementation, average unsubscribe rates and complaint rates have decreased, which indicates that customers are receiving the communications they want.¹⁸ Further, Canadian marketers achieved one of the highest inbox placement rates with an average of 90% - above the global average of 80%.¹⁹

Recommendation: The National Coordinating Body, in collaboration with the delivery partners, should strengthen its data collection capacity to ensure that performance information is available to assess the impact of CASL.

Conclusions

Based on quantitative and qualitative data sources, the evaluation led to seven findings.

GOVERNANCE

- Roles and responsibilities of the CASL partners were defined at the outset and governance mechanisms exist to support delivery. However, the oversight role of the National Coordinating Body could be strengthened and the role of the Office of Consumer Affairs clarified. Further, there is an opportunity to improve cohesion among partners.

INFORMATION SHARING TO FACILITATE CASL: AMONG CASL PARTNERS

- Information sharing among the enforcement agencies is effective. Although partners have distinct mandates, there are opportunities to enhance information sharing among all partners.

INFORMATION SHARING TO FACILITATE CASL: WITH INTERNATIONAL AND DOMESTIC PARTNERS

- CASL includes provisions for information sharing between the enforcement agencies and international partners but, except as it relates to CB, there are no provisions for information sharing with other non-CASL domestic partners, which limits cooperation for compliance activities.

PROMOTING COMPLIANCE

- Each delivery partner conducts education and outreach activities with the objective of promoting compliance with CASL. However, these activities are not coordinated and there are many aspects of CASL that may not be well understood.

MONITORING COMPLIANCE

- The Spam Reporting Centre monitors compliance by gathering information that supports the enforcement agencies in investigating and responding to non-compliance. There may be opportunities for the SRC to support other activities to promote compliance and awareness of spam and online threats.

INVESTIGATING AND RESPONDING TO NON-COMPLIANCE

- The enforcement agencies have conducted a number of investigations and issued a range of compliance actions. There is a perception that some types of actions may better promote awareness of CASL and, in turn, improve compliance.

IMPACT OF CASL ON THE ELECTRONIC MARKETPLACE

- Given that CASL is in its early stages, there is little evidence to conclude on impact. Further, there is limited data available to assess the impact of CASL on the electronic marketplace.

Recommendations

As a result of the findings of this evaluation, four recommendations have been made.



To improve cohesion, the CASL partners should re-examine the existing governance structure including roles and responsibilities and the supporting committees.



The National Coordinating Body should work with CASL partners to strengthen information sharing in order to facilitate the management and delivery of CASL. Consideration should be given to the sharing of aggregate Spam Reporting Centre reporting data.



As appropriate, the CASL partners should collaborate and develop a coordinated approach to education and outreach activities to improve the understanding of CASL by businesses, as well as the impact and reach of these activities.



The National Coordinating Body, in collaboration with the delivery partners, should strengthen its data collection capacity to ensure that performance information is available to assess the impact of CASL.

Appendices

A – CASL Exceptions

B – CASL Logic Model

C – Evaluation Limitations

D – Service Blueprinting of Spam Reporting

E – Comparative Analysis

Appendix A: CASL Exceptions

CASL contains exceptions related to:

Commercial electronic messages²³

- sent on platforms where the required identification and unsubscribe information is conspicuously published and readily available to the recipient on the user interface, where duplication in each message would be needlessly repetitious;
- sent and received within limited access secure and confidential accounts to which only the provider of the account can send messages, such as banking websites;
- solicited or sent in response to complaints, inquiries, and requests;
- sent due to a legal or juridical obligation or to enforce a right, legal or juridical obligation, court order, judgment or tariff; to provide notice of an existing or pending right, legal or juridical obligation, court order, judgment or tariff; or to enforce a right arising under a law of Canada, of a province or municipality of Canada, or of a foreign state.
- sent by or on behalf of registered charities* for fundraising purposes; or
- sent by or on behalf of a political party or organization, or a person who is a candidate—as defined in an Act of Parliament or the legislature of a province—for publicly elected office and the message has as its primary purpose soliciting a contribution as defined in subsection 2(1) of the *Canada Elections Act*.

Altering transmission data

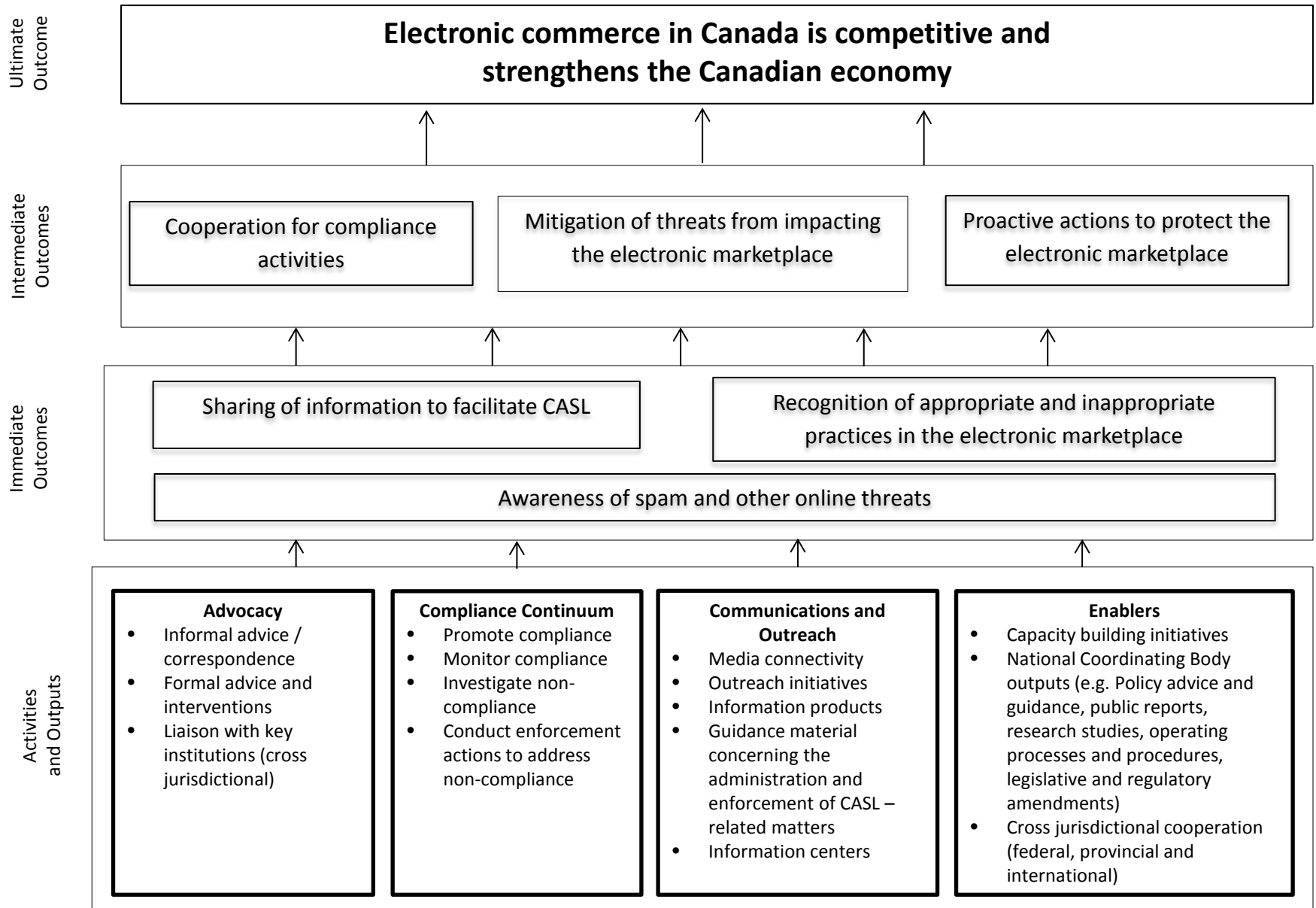
- It is prohibited, in the course of a commercial activity, to alter or cause to be altered the transmission data in an electronic message. This does not apply if the alteration is made by a telecommunications service provider for the purposes of network management.

Express consent

- If a person is seeking express consent on behalf of a person whose identity is not known (in accordance with sections 6 to 8 of the Act) then
- (a) the only information that is required to be provided under that paragraph is prescribed information that identifies the person seeking consent; and
- (b) the person seeking consent must comply with the regulations in respect of the use that may be made of the consent and the conditions on which the consent may be used.

* The *Competition Act* does not include this exception as provisions of the *Competition Act* apply equally to charities.

Appendix B: CASL Logic Model



Appendix C: Evaluation Limitations

Performance Information

- CASL implementation started in 2014-15 limiting the availability of performance information and the ability to identify trends.
- Each enforcement agency is responsible for different aspects of delivering CASL, operating under distinct legislative, organizational, and remedial regimes, which made it difficult to summarize performance information.
- Financial and human resources information was also limited as this is an evaluation of the implementation of legislation rather than of a program.



Mitigation

1. The evaluation considered the context in which the activities, outputs and outcomes were accomplished.
2. The findings were triangulated and validated with other lines of evidence.

Respondent Bias

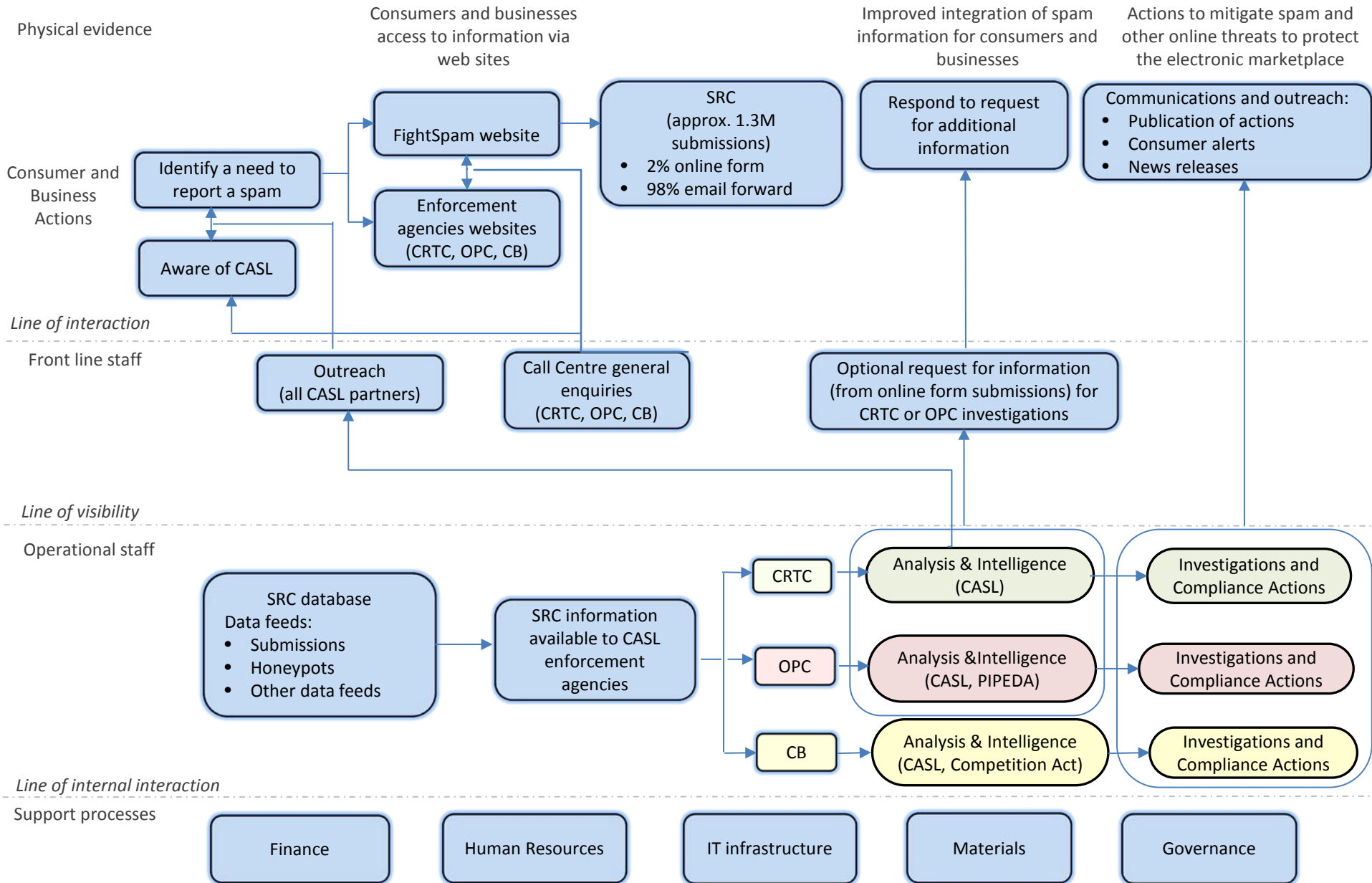
- The evaluation was undertaken at the same time of the CASL legislative review by the House of Commons Standing Committee on Industry, Science and Technology. Some interviewees were interviewed by both processes.
- Interviewee responses may have also been impacted by the suspension of CASL Private Right of Action provisions.



Mitigation





1. The purpose of the interview and strict confidentiality of responses were communicated to participants.
2. Responses were cross-referenced with those of other groups for consistency and validation.
3. Where possible, findings were triangulated and validated with other lines of evidence.

Appendix D: Service Blueprinting of Spam Reporting



Appendix E: Comparative Analysis

Canada has a robust anti-spam legislation with its opt-in model and enforcement capabilities, comparable to Australia and the United Kingdom.

	Canada 	Australia 	United Kingdom 	United States 
Legislation	Canada's Anti-Spam Legislation	Spam Act 2003	Privacy and Electronic Communications (EC Directive) Regulations 2003	Controlling the Assault of Non-Solicited Pornography and Marketing Act
Consent Model	Opt-in	Opt-in	Opt-in	Opt-out
Penalties	Up to \$1,000,000 (Canadian dollars) for individuals and up to \$10,000,000 (Canadian dollars) for businesses, per violation.	Fines up to \$1,370,349 (US dollars) per day.	Fines up to \$607,927 (US dollars) for serious breaches.	Civil penalties up to \$16,000 (US dollars) for each separate e-mail, Damages up to \$250 per violation - maximum award of \$2,000,000 (US dollars).
Application	Commercial electronic messages: messages whose purpose is to encourage participation in a commercial activity.	Commercial electronic messages: a message sent by an electronic address and using an internet carriage service with a commercial intent. Voice calls are not considered an electronic message.	Electronic means including telephone, automated telephone messages, fax and electronic mail.	Commercial electronic mail messages: Any electronic mail message that has primary purpose of commercial advertisement or promotion of a commercial product or service.
Private Right of Action	Sections have been suspended Intended to apply to businesses and individuals. No need to prove damages.	Applies to businesses and individuals that have suffered loss or damage.	Applies if someone suffers damage.	Applies to Internet Service Providers only as they incur costs for protecting their systems and customers. Not applicable to individuals.

End Notes

1. Internet Governance Forum. (2015). Best Practice Forum Regulation and Mitigation of Unsolicited Communications, p.6.
2. Canada's Anti-Spam Legislation. Canada's law on spam and other electronic threats. Retrieved from <http://fightspam.gc.ca/eic/site/030.nsf/eng/home>.
3. Canada's Anti-Spam Legislation. Frequently Asked Questions. Retrieved from <http://fightspam.gc.ca/eic/site/030.nsf/eng/00304.html>
4. Justin Trudeau, Prime Minister of Canada. (2015). Mandate Letters. Retrieved from <https://pm.gc.ca/eng/mandate-letters>.
5. Canada's Anti-Spam Legislation. (2013). Retrieved from: http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00039.html
6. Justice Laws. Canada's Anti-Spam Legislation. Retrieved from <http://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html>
7. Dan Ruimy, D. (2017). Canada's Anti-Spam Legislation: Clarifications Are In Order. Report of the Standing Committee on Industry, Science and Technology. Retrieved from <http://www.ourcommons.ca/Content/Committee/421/INDU/Reports/RP9330839/indurp10/indurp10-e.pdf>.
8. Martineau, F. (2012). Canadian Anti-Spam Act survey: Bill C-28.
9. Cyberimpact. (2015). *Canada's Anti-Spam law is effective, but it's harming Canadian businesses*.
10. The Canadian Chamber of Commerce. (2017). Canadian Anti-Spam Legislation Experience of Organizations.
11. Fasken Martineau DuMoulin LLP & Direct Marketing Association of Canada. (2017). CASL Survey Report: Bridging the Gaps in Understanding and Compliance.
12. Canadian Internet Registration Authority (CIRA) and Ipsos Reid. (2012). Understanding Canadian reactions to CASL.
13. Fasken Martineau DuMoulin LLP & Direct Marketing Association of Canada. (2017). *CASL Survey Report: Bridging the Gaps in Understanding and Compliance*.
14. Grant, M. (2017). *The Economic Impact of Canada's Anti-Spam Law (CASL)*, p. 3.
15. Grant, M. (2017). *The Economic Impact of Canada's Anti-Spam Law (CASL)*, p. 20.
16. The Canadian Chamber of Commerce. (2017). *Canadian Anti-Spam Legislation Experience of Organizations*.
17. Inbox Marketer. (2017). *The Impact of CASL on Email Marketing, Facts and Observations*.
18. Inbox Marketer. (2017). *The Impact of CASL on Email Marketing, Facts and Observations*, p.7.
19. Return Path. (2017). *2017 Deliverability Benchmark Report*.
20. Cloudmark Intelligent Network Security. *Security Threat Report 2015 Q1*, p. 6.
21. Internet Governance Forum. (2015). *Best Practice Forum Regulation and Mitigation of Unsolicited Communications*, p.12.
22. Return Path. (2017). *2017 Deliverability Benchmark Report*, p.3
23. Canada's Anti-Spam Legislation. *Archived — Regulatory Impact Analysis Statement*. Retrieved from <http://fightspam.gc.ca/eic/site/030.nsf/eng/00271.html>