Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada

Canada

CANADA'S ANTI-SPAM LEGISLATION (CASL)

+ PERFORMANCE MEASUREMENT REPORT 2018-2019

This publication is available online at
http://www.fightspam.gc.ca/eic/site/030.nsf/eng/h_00098.html

To obtain a copy of this publication, or to receive it in 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 (international): 613-954-5031
TTY (for hearing impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)
Email: ISED@canada.ca

Cat. No. Iu170-2E-PDF
ISSN 2562-3265

Aussi offert en français sous le titre *Initiative relative à la Loi canadienne anti-pourriel (LCAP), rapport de mesure du rendement.*

Table of Contents

1. Introduction

Enacted in 2010, Canada's Anti-Spam Legislation (CASL) is a technology-neutral law that aims to protect Canadians and the electronic marketplace from spam, spam-related violations, and emerging electronic threats that may impose costs, create inefficiencies, cause harm, or undermine the confidence that businesses and individuals should have in the electronic marketplace. Most of its provisions came into force in 2014 with a three-year transition period to give consumers and businesses time to understand and comply with the legislation.

CASL's rules govern:

- the sending of commercial electronic messages;
- the unauthorized alteration of transmission data;
- the installation of computer programs without consent;
- false or misleading electronic representations;
- the harvesting of electronic addresses; and
- the collection of personal information though illegal access to a computer system.

This performance annual report aims to increase the public's understanding of CASL, including relevant performance data and CASL government partners' roles and activities.

2. Results at a Glance

Promoting

The fightspam.gc.ca website is a key tool for promoting CASL. It contains important information and resources for understanding the Act and increasing compliance. In 2018–2019, the website received 375,342 visits with 331,805 unique visitors (from unique IP addresses). Among these:

- 286,348 visitors were from Canada;
- 33,181 visitors were from the United States; and
- 12,276 visitors were from other countries.

CASL partners also share information, such as FAQs and other guidance for Canadians and businesses, on their respective websites, and through education and outreach activities. The partners are also exploring ways to reach a variety of audiences, including diversifying through formal publications, blog posts and social media. In 2018-2019:

- The Canadian Radio-television and Telecommunications Commission (CRTC) released 57 tweets, 12 Facebook posts and 1 information bulletin, and held 30 outreach sessions.
- The Office of the Privacy Commissioner (OPC) issued 1 blog post, 1 report and 5 announcements, and revised 3 publications.
- The Competition Bureau issued 1 publication and 11 consumer and business alerts.
- The Office of Consumer Affairs (OCA) revamped the fightspam.gc.ca website and issued 5 social media posts.

Monitoring

The CRTC hosts the Spam Reporting Centre, which collects information that can serve as evidence of potential CASL violations. In 2018–2019, Canadians made 280,920 submissions to the centre, including 8,214 web form submissions and 272,706 email forwards.

Enforcing

The 3 agencies responsible for enforcing CASL are the CRTC, the Competition Bureau and the OPC. CASL gives these enforcement agencies a set of tools to respond to non-compliance such as warnings (or notices), undertakings and consent agreements. The CRTC and the Competition Bureau can also impose Administrative Monetary Penalties. These responses are meant to promote and enforce compliance with the Act and its regulations.

The CRTC issued or executed:

- 2 notices of violations;
- more than 50 warning letters;
- 1 search warrant; and
- 1 undertaking.

The Competition Bureau:

- resolved 1 case that resulted in $700,000 in administrative monetary penalties;
- resolved 2 cases using the alternative case resolution process; and
- has 1 ongoing case with the Competition Tribunal.

The OPC undertook:

- 1 investigation into allegations of indiscriminately collected email addresses and unsolicited email communication by a publishing company (completed); and
- an industry-wide investigation of the privacy management practices of data and list brokers (ongoing).

3. Partners

The CASL initiative engages multiple federal partners with different but complementary mandates. Innovation, Science and Economic Development Canada (ISED) oversees the initiative while the CRTC, OPC and Competition Bureau enforce different sections of the Act. The roles and responsibilities of all organizations are defined in relevant laws and regulations.

Innovation, Science and Economic Development Canada

The CASL initiative is administered by ISED. The **National Coordinating Body**, which resides in ISED's Privacy and Data Protection Directorate, is responsible for policy and research, public communications and outreach oversight, monitoring and reporting on the overall effectiveness of the regime. The **Office of Consumer Affairs** coordinates consumer and business education and awareness efforts for the CASL initiative, including the management of the FightSpam website.

Canadian Radio-television and Telecommunications Commission

The CRTC is an administrative tribunal that operates at arm's length from the federal government and has the primary enforcement responsibility under CASL. The CRTC is committed to reducing the harmful effect of spam and related threats to electronic commerce. The CRTC is working toward a safer and more secure online marketplace for Canadians while continuing to allow legitimate uses of telecommunications by businesses.

Competition Bureau

The Competition Bureau is an independent law enforcement agency that ensures Canadian businesses and consumers prosper in a competitive and innovative marketplace, including the electronic marketplace. Through amendments to the *Competition Act*, CASL enables the Competition Bureau to more effectively address false and misleading representations and deceptive marketing practices in the electronic marketplace, including false or misleading sender or subject matter information, electronic messages and locator information such as URLs and metadata.

Office of the Privacy Commissioner of Canada

The OPC is an agent of Parliament whose mission is to protect and promote privacy rights. Through amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the Privacy Commissioner is responsible for investigating and reporting violations of prohibitions against electronic address harvesting and the collection and use of personal information through illegal access to computer systems.

4. The Environment

4.1 International Context

As the pace of innovation increases and new advances in algorithmic technologies and artificial intelligence are integrated into the global marketplace, digital tools are becoming more powerful and creating new opportunities and challenges. Companies, governments and citizens around the world are facing a growing and evolving cybersecurity risk. Canada is a prime target for malicious online activity despite being a smaller market.

To that end, CASL, by addressing spam and related online threats, contributes to address the cybersecurity risks facing Canadians and Canadian businesses hence fostering trust in the online marketplace. Given the inherent international nature of cybersecurity risk, CASL is part of a broad range of domestic and international legal and policy frameworks in the areas of spectrum, telecommunications, privacy protection and cyber resilience, including cyber security. CASL helps maintain a privacy and data protection framework that provides mechanisms to enhance interoperability domestically and internationally with next-generation privacy and e-protection laws, such as the General Data Protection Regulation and the up-coming e-Privacy Regulation in the European Union.

4.2 E-commerce Trends, Indicators and Challenges

CASL helps protect Canadians from spam and other online threats while ensuring that businesses can continue to compete in the global marketplace. It allows Canadian enforcement against spammers operating in Canada and facilitates cooperation in global anti-spam enforcement actions.

Investigations around the world have raised concerns about a modern Internet marketplace that enables the systematic profiling and sharing of detailed web users' profiles among hundreds of organizations along with questionable targeting methods and the widespread sharing of disinformation. New and evolving technologies are being used not only to prevent, but to investigate online electronic threats.

In 2018, in Canada:

- Digital advertising spending surpassed traditional advertising spending for the first time.
- 77% of Canadians were concerned about cyberattacks against organizations that may hold their personal information.
- The email spam rate was 53.4% in Canada, while the global average was 55%.
- E-commerce continued to thrive, with 87% of Canadians making at least one online purchase.

In 2018, worldwide:

- Advertising fraud cost advertisers up to $19 billion.
- There was growing discomfort with the power that social media corporations wield over individuals; according to the 2018 CIGI-Ipsos Global Survey, Internet users expressed a high level of distrust of social media platforms, with 63 percent of respondents feeling that social media has too much power.
- 75% of Internet users said social media platforms contributed to their lack of trust in the Internet.
- 78% of Internet users were concerned about their privacy and security online, with 53% saying they more concerned than they were a year ago.

5. The Results

5.1 Policy and Coordination

National Coordinating Body

CASL policy, research, oversight and coordination are the responsibility of the National Coordinating Body (NCB). The NCB keeps abreast of the most recent developments in spam, online threats, cybersecurity and e-commerce by performing strategic intelligence scans, conducting information research, and analyzing metrics and trends. It also works with national and international partners to align legislative and regulatory frameworks with international anti-spam and malware industry best practices.

In 2018–2019, the NCB:

- led the development of the 2017–2018 CASL Performance Measurement Report, which was completed in collaboration with all CASL partners;
- participated in the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)—a spam-related international forum—alongside its Canadian partners;
- informed and advised ISED (the ministry responsible for CASL) of all developments relating to CASL management and policy;
- advised the minister on the government's response following the release of the House of Commons Standing Committee on Industry, Science and Technology CASL Statutory Review Report.;
- contributed to the National Digital and Data Consultation by providing questions, input and feedback (results are expected to guide legislative changes related to privacy as well as other marketplace framework policy, such as CASL);
- informed the European Commission of CASL developments in the Fifth Update Report on Canada's privacy framework;
- coordinated CASL governance-related activities to discuss policy and strategy;
- supported ISED's Audit and Evaluation Branch Horizontal Evaluation of CASL Report; and
- collaborated with its CASL partners to develop a Management Response and Action Plan and to implement the response to the 4 recommendations made by the Evaluation Report.

5.2 Promoting Compliance

Office of Consumer Affairs

OCA manages CASL-related communication products for Canadian individuals and businesses, including the official CASL website, fightspam.gc.ca.

Fightspam.gc.ca promotes CASL-related information. In 2018–2019, there were 375,342 visits to the website (page views), including:

- 331,805 unique visitors;
- 302,394 who visited once; and
- 29,411 who visited more than once.

The distribution of visitors on fightspam.gc.ca in 2018–2019 was as follows:

- 86.3% from Canada;
- 10% from the United States; and
- 3.7% from all other countries.

During this period, the OCA led the CASL website revitalization project, which included close collaboration

with the NCB and the 3 enforcement partners. The new website, featuring updated content that is simpler in structure and language, was launched on April 1, 2019.

To help promote the website and the publication of the CASL 2017–2018 Performance Measurement Report, the OCA published a web banner on its "For Consumers" homepage in February 2018.

In addition to creating awareness online, the OCA promoted CASL via social media, publishing 5 CASL-related posts on ISED social media channels in 2018–2019. Together, these posts had a total reach of 13,563.

The number of negative mentions identified during media-monitoring activities continued to decline, with:

- 57% positive mentions;
- 34% neutral or ambivalent mentions; and
- 9% negative mentions.

When compared with the tone of mentions in the 3 previous years (26.4% negative in 2015–2016; 22% negative in 2016–2017; and 18% negative in 2017–2018), these findings indicate a steadily decreasing trend in negative perceptions.

Canadian Radio-television and Telecommunications Commission

Complementing fightspam.gc.ca, the CRTC's website also provides CASL-related information to Canadians and stakeholders to make it easier for everyone to get the help they need. The online experience includes easy-to-access alerts, videos, infographics, policies and guidelines intended to inform Canadians about CASL and help businesses comply. The CRTC also educates and informs stakeholders and Canadians using social media platforms, such as Twitter and Facebook.

In 2018–2019, the CRTC:

- had 98,789 unique page views and 128,124 page views of its website related to CASL;
- released 57 tweets, resulting in 163,268 impressions, 240 retweets and 222 reactions/likes;
- made 12 Facebook posts, leading to 61,213 people reached, 528 shares and 123 reactions/likes;
- conducted more than 30 outreach activities for domestic and international stakeholders in the form of information sessions, compliance meetings, webinars and keynote speeches, including:
  - the CRTC Chairperson and Chief Executive Officer's presentation to the "International Regulatory Responses" panel at the International Institute of Communications' (IIC) Telecommunications and Media Forum;
  - the CRTC's Chief Compliance and Enforcement Officer's presentation to the Receivables Management Conference in Toronto, Ontario;
- issued an enforcement advisory and a series of information letters to promote compliance with CASL among members of the Canadian web-hosting service industry, which is uniquely positioned to detect, prevent and stop non-compliant activities; and

- issued an information bulletin discussing the CRTC's general approach to section 9 of CASL and outlining activities that could result in non-compliance as well as measures for managing associated risks.

Competition Bureau

In 2018–2019, the Bureau used a number of means to increase awareness of CASL-related issues among Canadian consumers and businesses:

- In June 2018, the Bureau published its fourth edition of the Deceptive Marketing Practices Digest. The digest offers guidance and advice to marketing professionals, businesses and social influencers about their responsibilities and the risks associated with influencer marketing, "Made in Canada" claims, and savings claims.
- The Bureau issued 11 consumer and business alerts addressing issues like cryptocurrency investment, smart toys, online dating scams and business directory scams.
- The Bureau also played an important role in Fraud Prevention Month.

Office of the Privacy Commissioner of Canada

The OPC delivers ongoing CASL-related compliance guidance for businesses and advice for individuals through different channels. Its web-site is its primary tool for reaching individuals and sharing information with businesses.

In 2018–2019:

- CASL-related OPC webpages were viewed more than 34,400 times.
- The "Helpful tips for businesses doing e-marketing" webpage was consulted more than 17,500 times.
- The OPC updated its online resources related to CASL, including those covering compliance help for businesses and a general page on CASL.
- It also updated the PIPEDA guide for businesses, including a section on CASL, and will post it online in 2019–2020.
- The OPC launched and promoted a new presentation package on PIPEDA for businesses with information about CASL and how the law affects e-marketing.

The OPC shared content through social media channels, promoting CASL-related tips and material with businesses and the public in a series of tweets and LinkedIn posts, for example during Fraud Prevention Month. It also participated in events and conferences and held seminars and conferences, such as:

- the Canadian Association of Virtual Assistants Conference in Ottawa;
- the Canadian Bar Association Competition Law Fall Conference in Ottawa;
- a session hosted by the Canadian Bar Association and Ontario Bar Association in Toronto (delivered along with the Competition Bureau and the CRTC);
- the 2018 Canadian LEAN Conference in Winnipeg;
- Big Data Toronto 2018;
- the Immigrant Women's Small Business Expo in Toronto; and
- Franchise Expos in Winnipeg and Toronto.

In terms of distributing materials in 2018–2019, OPC:

- shared 53 copies of "Helpful tips for businesses doing e-marketing" guidance and 1,001 copies of "Top 10 tips to protect your inbox, computer and mobile device" at events;
- mailed compliance information (including CASL information) to more than 200,000 small businesses through a Canada Revenue Agency insert;
- developed privacy-related cartoons, including some on email address harvesting, for use in presentations and on social media to promote CASL web content;
- sent a promotional email message to 360,000 businesses; and
- conducted outreach through public libraries across Canada to offer CASL-related advice and information on library date-due receipts.

OPC also published articles and ran radio spots, including:

- pieces in community newspapers across the country; and
- a radio campaign that was aired on local stations in Canada during Fraud Prevention month, reaching more than 1.2 million listeners.

In terms of responding to inquiries to its Information Centre:

- OPC received 78 CASL-related requests from individuals and businesses, most by telephone.
- Broadly, the top 3 CASL-related categories were reports of unsolicited messages, questions about unsubscribing from email distribution lists, and questions about the applicability of CASL and how to achieve compliance.

5.3 International and Domestic Cooperation

CASL enforcement partners worked with their domestic and international counterparts to promote compliance. Given the borderless nature of the Internet, CASL violations can originate outside Canadian borders. As such, investigation of online threats often requires international cooperation. To that end, information sharing and cooperation with foreign governments and organizations is essential to ensure effective and coherent international cooperative actions against CASL violators.

Canadian Radio-television and Telecommunications Commission

Unsolicited communications are a global problem. Citizens in every jurisdiction are vulnerable to annoyance or attacks, so it is important for the international community to collaborate to combat this problem. The CRTC has built a trusted network of domestic and foreign allies with whom it has established protocols for sharing information and enforcing collaboration.

In March 2019, the CRTC and the RCMP National Division executed warrants at a residence in the Greater Toronto Area after tips from international private cyber security firms triggered an investigation. The operation was part of an international coordinated effort with the RCMP, the Federal Bureau of Investigation and the Australian Federal Police.

The warrants were obtained as part of ongoing parallel investigations into Remote Access Trojan technology. This type of malicious software (malware) enables remote access to Canadian computers without their users' consent, and can lead to the subsequent installation of other malware and theft of personal information. The execution of this warrant illustrates how cooperation among law enforcement agencies can help protect Canadians from online threats.

Competition Bureau

Along with honouring foreign-related assistance requests, the Bureau continues to be active with a number of international and domestic partnerships and working groups, including:

- Organisation for Economic Co-operation and Development;
- International Consumer Protection; Enforcement Network;
- International Mass Marketing Fraud Working Group;
- Canadian Anti-Fraud Centre, Joint Management Team;
- Toronto Strategic Partnership;
- Alberta Partnership Against Cross-Border Fraud;
- Pacific Partnership Against Cross-Border Fraud.

Office of the Privacy Commissioner of Canada

When CASL came into force, it amended PIPEDA's provisions, giving the OPC the ability to collaborate and share information with provincial and international data protection counterparts. Since then, the OPC has engaged in a number of joint enforcement actions with partners through joint memoranda of understanding by participating in various networks.

- OPC is a member of the Unsolicited Communications Enforcement Network (UCENet), a network of anti-spam, consumer protection and telecommunications regulatory authorities. The OPC attended the joint annual meeting of UCENet and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) in New York in October 2018 and presented a technical study of an adware

investigation and an update on CASL. This event was attended by private sector IT security experts. The OPC also participated in discussions at the meeting to develop the 2019–2021 UCENet Operational Plan.

- The OPC is a member of the executive committee of the Global Privacy Enforcement Network (GPEN). The OPC participates in collaborative enforcement activities, hosts and administers the GPEN website, takes part in privacy-themed monthly teleconference calls, and attends annual meetings.
- The OPC participated in "GPEN Sweep 2018" under the theme of privacy accountability. Participating authorities were asked to survey organizations of their choice to assess their compliance with some of the key elements (indicators) of accountability, including internal privacy frameworks; internal governance structures; training and awareness; transparency; incident management regimes; and their ability to document stored data and track data transfers. While there were examples of good practices, participants found that a number of organizations had no processes in place to deal with complaints or queries, and were not equipped to handle data security incidents appropriately.
- In June 2018, the OPC participated in and presented at the second GPEN Enforcement Practitioner's Conference in Tel Aviv, Israel. Focusing on international enforcement collaboration and investigative techniques, the OPC presented on an RCMP investigation into the use of cell site simulators (also known as international mobile subscriber identity catchers).
- The International Conference of Data Protection & Privacy Commissioners (ICDPPC) is the main global forum for data protection and privacy authorities. The Privacy Commissioner serves on the ICDPPC executive committee, which oversees the conference's activities.
- Related, the OPC co-sponsored the ICDPPC Resolution on Collaboration Between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy. Furthermore, the OPC participated in the Digital Citizen and Consumer Working Group, established by this resolution. In 2018–2019, the OPC co-led the group that explored the intersection of privacy, consumer protection and competition, and ultimately how to promote collaboration across these regulatory spheres.
- At the 40th Conference in Brussels, the Commissioner participated in an open session panel that explored the roles of international data protection authorities in the governance of digital ethics. The OPC co-authored the ICDPPC Resolution on E-Learning Platforms with the Office of the Information and Privacy Commissioner of Alberta and the Information and Privacy Commissioner of Ontario.
- The OPC continues to play a leadership role in the ICDPPC International Collaboration and Enforcement Working Group, which is developing online tools to facilitate increased enforcement cooperation and evaluating alternative mechanisms to broaden the scope of cooperation.
- In June 2018, the OPC spoke at the 49th Asia Pacific Privacy Authorities (APPA) Forum in San Francisco about the issue of online reputation and privacy authorities' technological research capabilities. In December 2018, the OPC spoke at the 50th APPA Forum in Wellington, New Zealand about developments in government data use and the ICDPPC Digital Citizens and Consumers Working Group.
- The OPC has sought to develop links with consumer protection and anti-trust regulators in the International Consumer Protection Enforcement network (ICPEN) in recognition of the growing connection between privacy and consumer protection and anti-trust issues. As an ICPEN observer, the OPC attended the annual ICPEN meeting in Istanbul, Turkey (April 2018) and organized a side meeting to discuss the ongoing mandate of the Digital Citizen and Consumer Working Group.
- The OPC has also become a member of the European Data Protection Supervisor's (EDPS) Digital Clearinghouse, which brings together agencies from competition, data protection and consumer law who are willing to share information and discuss how best to enforce rules in the interests of individual consumers from the European Union and across the world. The OPC participated in the 4th meeting in Brussels, Belgium (December 2018), where members discussed non-price factors in competition (such as privacy) as well as consumer enforcement analysis and online manipulation in election processes.

5.4 Monitoring Compliance

CRTC

The CRTC monitors compliance in several ways. For example, it:

- collects and analyzes data about complaints;
- identifies trends and threats by leveraging data feeds;
- reviews and analyzes other information collected from stakeholders; and
- performs regular environmental scans.

Through these activities, the CRTC can gauge the effectiveness of its compliance program in order to help identify areas of risk for Canadians and ways to help businesses comply with CASL when sending commercial electronic messages. In 2018-19, the CRTC also issued 78 notices to produce and 2 preservation demands in order to verify compliance with CASL.

In 2018–2019, the Spam Reporting Centre received a total of 280,920 submissions. Of these:

- 8,214 were submitted using the detailed web form at fightspam.gc.ca.
- 272,706 were submitted by forwarding email spam to spam@fightspam.gc.ca.

During this same period, Canadians' top reasons for making complaints were:

- receiving email without having consented;
- identification of sender missing or incomplete;
- software and malware; and
- deceptive marketing practices.

Competition Bureau

In fiscal year 2018–2019, the Bureau's Deceptive Marketing Practices Directorate developed a Compliance Monitoring Unit (CMU). The Unit will be launched in April 2019. It ensures that matters that have been resolved through consent agreements, criminal sentencing orders, alternative case resolutions, or other court orders are monitored more consistently to ensure compliance. CASL-related matters resolved by the Bureau are also included in the Unit's compliance monitoring work.

OPC

The OPC established a CMU in fiscal year 2017-2018. The CMU seeks to ensure satisfactory implementation of organizations' PIPEDA and CASL-related commitments to the OPC, including those agreed to via compliance agreements and commitments flowing from the investigations highlighted in this report.

5.5 CASL Enforcement Operations

CRTC

The CRTC is responsible for ensuring compliance with section 6 through 9 of CASL. The CRTC has the power to investigate and take action against violators, and can set administrative monetary penalties.

In general, the CRTC's focus is on those who send commercial electronic messages without the recipient's consent or who install programs on computers or networks without consent. This includes malicious computer programs, spam messages and infected web links.

The CRTC's enforcement tools include:

- warning letters;
- undertakings; and
- Notices of Violations, which may include administrative monetary penalties.

The CRTC publishes its enforcement actions, including those resolved through alternative case resolution mechanisms. In 2018–2019, the CRTC's enforcement actions included:

- 2 Notices of Violation (see below);
- 1 warrant executed(described above);
- more than 50 warning letters; and
- 1 undertaking with 1395804 Ontario Ltd. (doing business as Blacklock's Reporter), which agreed to establish a compliance program to ensure all parties sending commercial electronic messages on its behalf comply with the Act and Regulations.

The CRTC's enforcement actions included a streamlined alternative case resolution blitz that sent letters to more than a dozen Canadian and American companies. Preliminary results show that more than 80% of recipients took action to improve their compliance.

Also in 2018–2019, and for the first time under CASL, the CRTC took enforcement action against Canadian companies for allegedly aiding in the installation of malware through online advertising. More specifically, CRTC staff designated under CASL issued Notices of Violation to Datablocks, Inc. and Sunlight Media Network Inc. for alleged violations of section 9 of CASL.

CRTC staff found evidence that ads distributed through these companies' services—using their proprietary infrastructure—resulted in the installation of malicious programs. Each installation constituted an activity prohibited by section 8 of the Act.

Consequently, the CRTC's Chief Compliance and Enforcement Officer issued Notices of Violation to Datablocks and Sunlight Media, including administrative monetary penalties of $100,000 and $150,000, respectively. These enforcement actions are currently under review by the Commission, pursuant to section 25 of CASL.

Competition Bureau

In 2018–2019, the Bureau resolved:

- 1 case of a registered consent agreement with an administrative monetary penalty of $700,000;
- 2 matters using alternative case resolutions (not public); and
- 1 ongoing matter at the Competition Tribunal.

In October 2018, the Bureau reached a consent agreement with Discount Car & Truck Rentals Ltd. that resulted in a $700,000 administrative monetary penalty.

In January 2018, the Bureau took action against Ticketmaster and its parent company, Live Nation.

OPC

In 2018–2019, the OPC received 11 written CASL-related complaints from the public. Most concerned the alleged receipt of unsolicited commercial electronic messages (spam emails) and the inability to unsubscribe from such messages. All complaints were closed at intake. Among them, 6 were redirected to the senior management of the organizations involved and 5 were considered to be outside of the OPC's jurisdiction to investigate.

The OPC pursued 2 CASL-related investigations:

- The OPC completed an investigation into allegations that a publishing company had indiscriminately collected email addresses and distributed unsolicited email messages. The OPC identified contraventions of PIPEDA's consent and accountability principles by the company, but found no evidence that the company had harvested email addresses.
- The OPC also commenced its first proactive, industry-wide, Commissioner-initiated investigation into the privacy management practices of data and list brokers. Preliminary inquiries into industry practices raised a number of concerns about how such brokers compile databases of Canadians' detailed personal information and disclose information to marketers. The investigation is examining the brokers' compliance with their accountability, openness and transparency obligations in the management of personal information. It is also looking at the means of consent obtained for the collection, use and disclosure of personal information, including email addresses. This investigation is ongoing.

OPC investigations enabled by privacy enforcement engagement and collaboration

PIPEDA provisions amended by CASL enable the OPC to collaborate and share information with provincial and international data protection authorities. The OPC has since engaged in a number of joint enforcement actions with these authorities. Examples of privacy enforcement engagement and collaboration that enabled the OPC to pursue investigations include the following.

- In 2018–2019, the OPC commenced joint investigations, discussed privacy matters of mutual interest, and shared information with the Offices of the Information and Privacy Commissioner of Alberta and British Columbia.
- In August 2018, the OPC announced that it was opening an investigation into Cadillac Fairview and its use of facial recognition technology in mall digital directories following concerns raised about whether the company was collecting and using personal information without consent. The OPC is jointly investigating this matter with its counterparts in Alberta and British Columbia. The investigation is ongoing.
- The end of 2018–2019 also saw the completion of the OPC's joint investigation with the Office of the Privacy Commissioner of British Columbia into the handling of personal information by Facebook in the widely reported Facebook/Cambridge Analytica matter. The OPC issued a joint report of findings in April 2019. The investigation found that Facebook committed serious contraventions of Canadian privacy laws and failed to protect Canadians' personal information. Facebook disputed these findings and refused to implement recommendations to address deficiencies. Specific deficiencies identified included:

- failing to obtain valid and meaningful consent from users installing apps;
- failing to obtain meaningful consent from the installing users' friends to disclose their personal information to apps;
- inadequate safeguards to protect user information: in particular, failing to effectively monitor apps' compliance with contractual terms protecting against unauthorized access to users' information; and
- failing to be accountable for the user information under its control and shifting the responsibility for protecting users' privacy to users and apps.

The OPC has signalled its plans to take the matter to federal court to seek an order to force the company to correct its privacy practices.

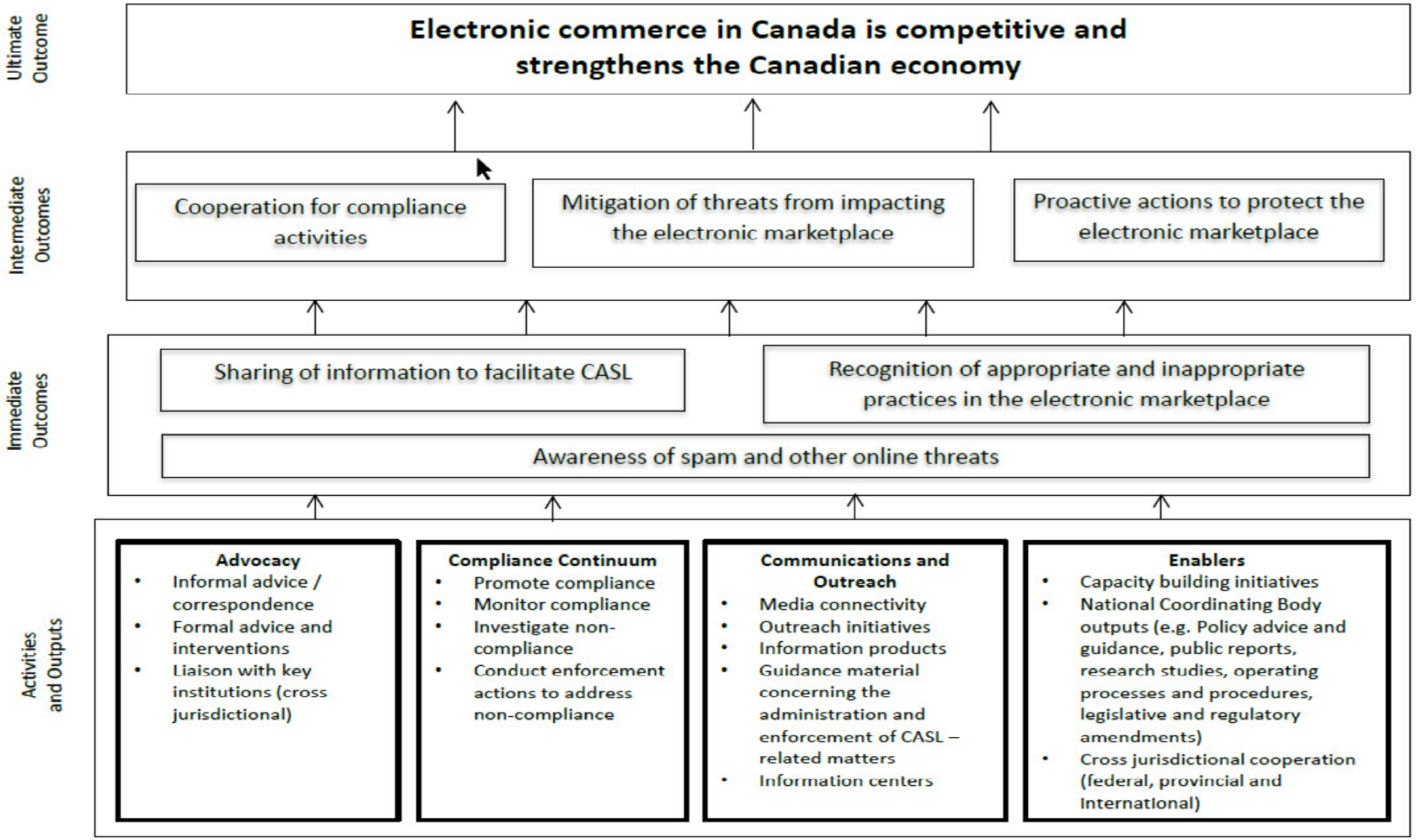
> The OPC also worked with international data protection agencies on various compliance activities involving collaborative enforcement action. In 2018–2019, the OPC collaborated on 2 major international investigations:
  - **Facebook/Aggregate IQ:** The OPC and UK Information Commissioner's Office (ICO) shared information and analysis arising from their investigations. The report of findings is expected to be issued in 2019–2020.
  - **Equifax:** The OPC completed its investigation into this global data breach and found that both Equifax Canada and its US-based parent company, Equifax Inc., fell far short of their privacy obligations to Canadians. Equifax agreed to enter into a compliance agreement to address the OPC's concerns and make privacy a priority. The OPC also benefited from collaborating with the US Federal Trade Commission and the UK ICO during the course of the investigation.

Other notable investigations

> **Profile Technology:** In July 2018, the OPC found that a New Zealand company, Profile Technology, operator of the Profile Engine website, copied old profiles of Facebook users around the globe and violated the privacy rights of potentially some 4.5 million Canadians. The company did this without consent and for inappropriate purposes, resulting in out-of-date and inaccurate information about individuals being easily accessible online. Profile Technology did not fully address the OPC's recommendations. The OPC shared its findings with the Office of the Privacy Commissioner of New Zealand, which agreed to consider what compliance options might be available under New Zealand law to address the company's actions.

> **Microsoft:** In 2018, the OPC concluded an investigation to determine whether Microsoft was obtaining valid consent via the default privacy settings in its Windows 10 operating system. The OPC found that Microsoft's opt-out consent was not sufficient for certain settings, and that it was not giving users the information they needed to meaningfully consent to the company's collection, use and disclosure of their personal information. In response to recommendations by the OPC, Microsoft agreed to make changes, including giving users the choice to "opt in" to their desired privacy settings, enhancing privacy communications, and augmenting privacy procedures. During the investigation, the OPC worked closely with its counterparts in the Netherlands and others. These collaborations helped the OPC to obtain an impactful privacy-protective outcome for Windows 10 users in Canada.

Annex A: CASL Logic Model



Description

The appendix shows a logic model for CASL. A logic model shows how program activities are expected to produce outputs and, in turn, how these outputs are expected to lead to different levels of results or outcomes.

There are 4 sets of activities and outputs:

1. Advocacy, including informal advice or correspondence, formal advice and interventions, and liaising with key institutions (cross-jurisdictional)
2. Compliance Continuum, including promoting compliance, monitoring compliance, investigating non-compliance, and conducting enforcement actions to address non-compliance
3. Communications and Outreach, including media connectivity, outreach initiatives, information products, guidance material concerning the administration and enforcement of CASL-related matters, and information centres
4. Enablers, including capacity-building initiatives, National Coordinating Body outputs (e.g., policy advice and guidance, public reports, research studies, operating processes and procedures, legislative and regulatory amendments) and cross-jurisdictional cooperation (federal, provincial and international)

The 4 sets of activities and outputs lead to 3 immediate outcomes:

1. Awareness of spam and other online threats
2. Sharing of information to facilitate CASL
3. Recognition of appropriate and inappropriate practices in the electronic marketplace

The 3 immediate outcomes lead to 3 intermediate outcomes:

1. Cooperation for compliance activities
2. Mitigation of threats impacting the electronic marketplace
3. Proactive actions to protect the electronic marketplace

The intermediate outcomes lead to one ultimate outcome: electronic commerce in Canada is competitive and strengthens the Canadian economy.