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

CANADA'S ANTI-SPAM LEGISLATION (CASL)

PERFORMANCE MEASUREMENT REPORT 2022-2023

This publication is available online at:
https://ised-isde.canada.ca/site/canada-anti-spam-legislation/en/canadas-anti-spam-legislation-resources/performance-measurement-reports/canadas-anti-spam-legislation-casl-performance-measurement-report-2022-23

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@ised-isde.gc.ca

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

Cette publication est aussi disponible en français sous le titre *La Loi canadienne anti-pourriel (LCAP) – Rapport de mesure du rendement 2022-2023.*

Table of Contents

1. Introduction

This annual performance measurement report focuses on Canada's anti-spam legislation (CASL) and provides information about its environment, its effectiveness, and the roles and activities of the organizations implicated in its delivery. In this report, the term CASL encompasses the initiative, the legislation and its amendments to legal frameworks in the fields of telecommunications, competition and privacy in relation to cybersecurity and e-commerce.

CASL's purpose is to build trust in the digital, data-driven economy by regulating commercial conduct that discourages e-commerce. It safeguards business and consumers from the improper use of digital technology, including spam, hacking, and other electronic threats. CASL sets forth rules that align with global best practices and anti-spam legislation to ensure fairness for organizations committed to complying with the legislation.

Generally, CASL prohibits:

- **Spamming**
- **Hacking**
- **Deceptive Online Marketing Practices**
- **Address Harvesting**
- **Malware**
- **Privacy Invasion**

2. Partners

The following diagram illustrates the different but complementary roles and mandates of the CASL partners, which support an effective delivery of the CASL initiative.

CASL Initiative

Non-Enforcement (ISED)

National Coordinating Body (NCB)

The NCB resides within ISED's Privacy and Data Protection Directorate. It:

- conducts policy oversight, including monitoring and reporting on the regime's overall effectiveness
- oversees public communication and outreach activities

Office of Consumer Affairs (OCA)

The OCA is responsible for consumer protection and promotion. It:

- coordinates consumer and business education and awareness efforts
- manages the Fightspam.gc.ca website

Enforcement

Canadian Radio-television and Telecommunications Commission (CRTC)

The CRTC is an administrative tribunal that operates at arm's length from the federal government. It:

- enforces and investigates potential violations of CASL's prohibitions against sending spam, altering transmission data and installing software on computer systems and/or networks without consent
- encourages compliance through outreach, sanctions and remedies for violations, such as administrative monetary penalties (AMPs)
- houses the Spam Reporting Centre, the central point for individuals to report spam, file complaints and alert enforcement agencies about alleged CASL violations

Competition Bureau (the "Bureau")

The Bureau is an independent law enforcement agency. Through amendments to the *Competition Act*, it:

- enforces CASL and investigates cases of false or misleading electronic 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
- encourages compliance with CASL-related *Competition Act* provisions through outreach, advocacy and enforcement. Under the *Competition Act*, matters can be resolved through Consent Agreements, court orders, fines and monetary penalties

Office of the Privacy Commissioner of Canada (OPC)

The OPC is an agent of Parliament. Through amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), it:

- enforces and investigates the unauthorized collection and use of electronic addresses through the use of computer programs and of individuals' personal information through unlawful access to their computer systems, via any means of telecommunication.
- encourages compliance with CASL-related PIPEDA provisions through outreach and remedies (excluding AMPs)

3. Context and trends

Over the last two decades, Spam and related online threats such as malware and phishing have been a nuisance to online commerce and have posed a real danger to consumers worldwide. As of 2022, spam emails and text messages continue to flood inboxes and mobile devices, with an estimated 15 billion spam emails passing through the internet every day as indicated in Security Boulevard's report entitled Cyberattacks 2022: Phishing, Ransomware & Data Breach Statistics. Securelist reveals this represents almost half (48.63%) of all emails sent around the world.

48.63%
of all emails sent are spam

Spam and electronic threats can compromise security and privacy. Email has become the weapon of choice for cybercriminals to launch sophisticated attacks. Email is also often the entry point for several types of cybercrime, including ransomware, malware, and a variety of digital scams. According to CIRA's Cybersecurity Survey 2022, the biggest perceived threats amongst cybersecurity professionals are unauthorized malicious software and access and theft of data. According to IBM's Cost of a Data Breach Report, phishing was the costliest of all attacks, averaging $4.91 million (US) in data breach costs. Meanwhile, the average cost of a ransomware attack, as indicated by the same report, excluding the ransom itself, was $4.54 million (US).

Spam e-mails are often the starting point for phishing schemes, with perpetrators fraudulently attempting to obtain sensitive personal information. This creates ample opportunities for identity theft and scamming victims out of their money. In 2022, a Security Boulevard report found that phishing was responsible for almost 90% of security incidents resulting in a data breach. As per Security Boulevard, phishing is today's most persistent and damaging cyberattack for all businesses, regardless of their size, sector or location.

Ultimately, spam and other related threats hurt everyone, individuals and businesses alike. As business efficacy and consumer confidence in the Internet weakens, the growth of e-commerce is impeded, resulting in negative economic consequences. But, not everything is grim. Canadians benefit greatly from living in one of the most internet-connected nations in the world, where these cyberthreats can be mitigated. In fact, CASL measures in combating spam and other electronic threats are instrumental in reducing the nuisance and economic damage caused by such unsolicited communications. Canada has experienced great improvement in regards to organizational cybersecurity. In 2022, not a single Canadian organization was featured in the 10 worst spammers list, nor did Canada feature amongst the 10 Worst Spam Countries or the 10 Worst Botnet Countries by Spamhaus.

As the Internet is a global resource, regulation and enforcement requires international cooperation. CASL is part of a broader range of domestic and international legal and policy frameworks in spectrum, telecommunications, privacy protection, and cyber resilience, including cyber security. CASL partners continue to work collaboratively to ensure that CASL continues to protect Canadians from spam and other electronic threats that lead to harassment, identity theft, and fraud.

CYBER THREAT TRENDS

The assessments provided by the Canadian Centre for Cyber Security identified the following persistent trends:

Cybercrime is still the number one cyber threat activity affecting Canadians

Threat actors have adapted their techniques - new technologies have spurred new cyber capabilities, and the availability of hacking tools and cybercrime expertise as services has democratized cyberattacks.

Technology continues to accelerate with rapid speed

- Digital assets, such as cryptocurrencies and decentralized finance
- Artificial Intelligence
- Quantum computing
- Encrypted information

Hybrid work and work-from- anywhere

As business networks are becoming integrated into employees' homes and public spaces, they also become vulnerable to cyber threat actors.

State-sponsored cyber programs

The state-sponsored cyber programs of China, Russia, Iran and North Korea continue to pose the greatest strategic cyber threat to Canada, with critical infrastructure remaining a prime target for both cybercriminals and state- sponsored actors alike.

4. Results

4.1 Setting policy and ensuring coordination

4.1.1. National Coordinating Body

The National Coordinating Body (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 industry best practices for handling international anti-spam and malware.

In 2022-23 the NCB:

- collaborated with CASL partners to update the CASL website
- helped develop the 2021-2022 CASL Performance Measurement Report in collaboration with CASL partners
- coordinated CASL governance activities, such as the Directors' General Steering Committee and Working Groups, and engaged CASL partners to discuss policy and strategy
- participated in the Messaging, Malware and Mobile Anti-Abuse Working Group—a spam-related international forum—alongside Canadian partners
- collaborated with CASL partners to increase awareness of the CASL initiative by coordinating communication, education and outreach activities
- informed and advised ISED of all developments relating to CASL management and policy

4.2 Promoting compliance

4.2.1 Office of Consumer Affairs

The Office of Consumer Affairs (OCA) manages the creation and maintenance of CASL-related communication products for Canadians, including the CASL website, fightspam.gc.ca, which presents information for consumer and business audiences.

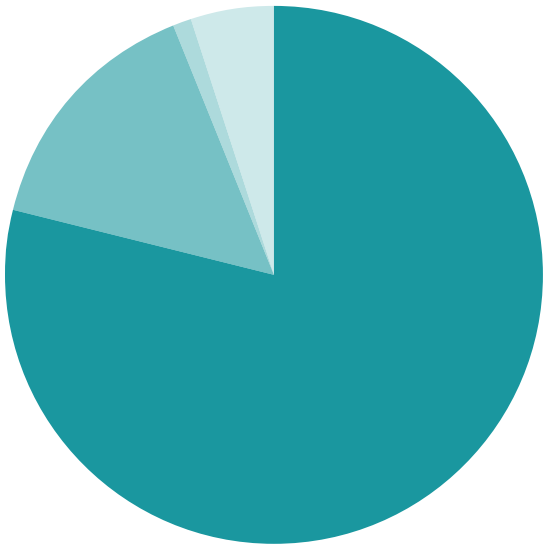
Spam being sent into Canada (whether through commercial electronic messages, malware, software, or altered transmission of data) is subject to CASL, no matter the country of origin. Legislation and the CASL website are sources of information and resources for anyone wishing to send commercial electronic messages to or from Canada.

The OCA regularly updates fightspam.gc.ca content, including the "Spam news" section of the website. This section contains notices, warnings, and enforcement actions for violations of Canada's Anti-Spam Legislation. Additionally, a review of the "About CASL" section of the fightspam.gc.ca website's main page was completed this year. New relevant data on spam and the effects of the legislation were added as updates. The OCA has fixed broken links and maintains the information on this website updating key metrics, language illustrating new trends and outlines benefits derived from CASL legislation and monitoring.

The OCA continued raising awareness of CASL among Canadians. Some highlights include:

- The production of a video educating consumers on reducing unwanted commercial electronic messages and reporting spam.
- A Google advertising and marketing campaign complemented with social media, promoting CASL compliance to business audiences and encouraging consumers to report spam through the Spam Reporting Centre (SRC). During the six-week campaign, which ran in early 2023, traffic to the CASL website increased by 530%. Moreover, when evaluating the aggregate submissions made through both the SRC form and the email submission option in the six weeks preceding these marketing initiatives, notable increases of 9.3% and 60% were observed.
- As part of its education and awareness efforts, the OCA published social media outreach content about CASL. In 2022-23, five OCA social media campaigns promoted CASL- related information to consumer and business audiences and had an overall reach of 9,962 people. Featured posts included helpful tips for sending CASL compliant holiday messaging to customers, as well as promotion of the 2021-2022 CASL Performance Measurement Report.

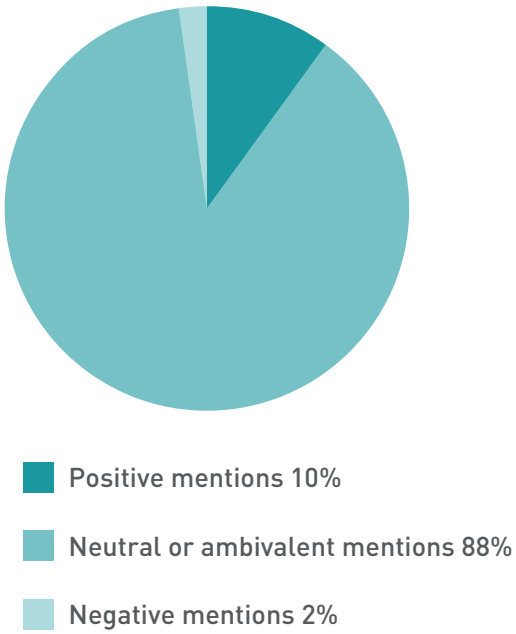
In 2022-23, there were 133,110 visits to fightspam.gc.ca. The distribution of visitors by country to fightspam.gc.ca in 2022-23 was:



4.2.1.1 Key media coverage trends

Media monitoring is a key part of how the OCA gathers data on the awareness of and sentiment towards CASL. The OCA conducted ongoing reviews, reporting and dissemination of information encompassing both traditional and digital media coverage with CASL partners. This initiative aimed to expose trends associated with spam, while also gauging the public perception of CASL and its effectiveness in safeguarding Canadians. There were very few opinion or commentary pieces about CASL legislation in media coverage this year, which explains why the general tone of media coverage was neutral. In 2022-23, a total of 452 CASL-related mentions were captured through online and social media monitoring. These mentions were shared and resulted in 44.3 million impressions online.

Percentage breakdown of the sentiment of media mentions



TRENDS IN TRADITIONAL MEDIA

Two notable spikes in coverage occurred this year, which accounted for 72 of the 110 traditional media appearances and roughly 15.5 million of the 37.7 million total traditional media impressions.

Software Installation Investigation

There was a clear spike in coverage in March, attributed to articles on the topic of a software installation investigation led by the CRTC, which was presented in 67 different publications.

The majority of traditional media articles either educated readers about CASL or covered major violations and enforcement actions.

TRENDS IN DIGITAL MEDIA

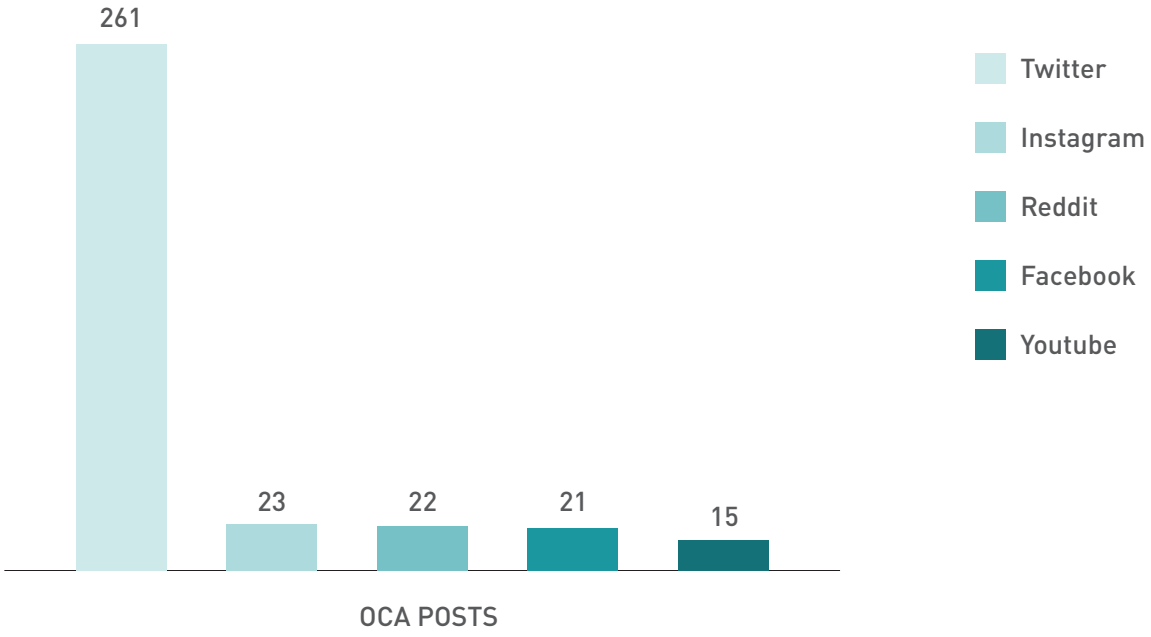
Across all digital platforms, the general theme was educating businesses on how to adhere to legislation or voicing complaints about businesses failing to comply.

Purchase of Twitter and Generative AI

Beyond general scam coverage, including tips to protect individuals against digital scams, there were two main global stories relating to spam: the purchase of Twitter and the arrival of generative AI, posing serious potential implications such as fake news, deep fakes, spam, phishing and malicious chatbots.

Media monitoring continues to inform the OCA's education and awareness efforts. This ensures that Canadian consumers and businesses operating within the country are well-informed about CASL. It aims to equip them with the necessary information and resources to effectively recognize, reject and report spam, as well as to navigate compliance with legislation in their commercial activities.

CASL digital media mentions broken down by social media channel were as follows:



4.2.2 Canadian Radio-television and Telecommunications Commission

In 2022–2023, the CRTC used a variety of approaches to educate and promote industry compliance with CASL. These included over 20 stakeholder interactions, information sharing, video meetings, partner briefings, conference presentations, and webinars. During these sessions, businesses were encouraged to comply with CASL and were reminded of the penalties for non-compliance.

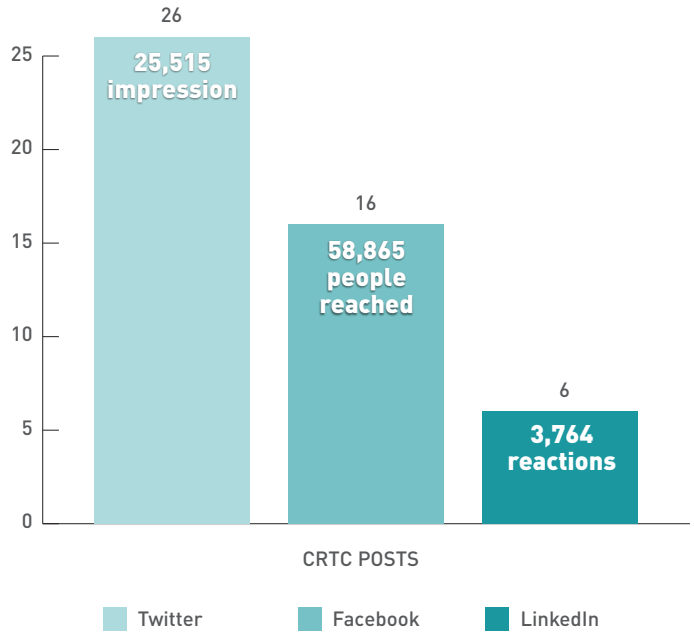
The CRTC's Chief Compliance and Enforcement Officer (CCEO) was a guest speaker at the Canadian Email Summit. The CCEO promoted compliance with the relevant CASL laws and regulations through education and encouragement to comply. At the same time, the CCEO explained that where necessary, the CRTC would enforce adherence through traditional or innovative approaches.

To promote an understanding of CASL with Canadians, the CRTC leveraged its social media channels to conduct outreach that warned the public of emerging phishing and scam campaigns.

The CRTC promoted Fraud Prevention Month to remind Canadians that recognizing fraud is the first step in preventing it. On Twitter and Facebook, the CRTC advised Canadians to watch out for misspelled words, urgent demands, or unknown numbers as tactics used by fraudsters in applying their trade.

In its CASL related communication products to Canadians, the CRTC encouraged Canadians to report suspected CASL violations by using the CASL email address and/or the SRC's online form. The information provided by Canadians is an essential part of the intelligence the SRC gathers on spam and electronic threats for all the CASL partners. It also helps support the CRTC's CASL violation investigations and enforcement efforts.

CRTC social media highlights:



The CRTC outreach efforts included, among other activities...

...publishing biannual snapshots of CASL enforcement activities which listed the:

1. top 5 commercial and affiliated marketing complaints; and
2. the top 5 phishing and scam complaints.

...issuing timely warnings related to a malicious QAKBOT link, a nefarious large- scale Bank Phishing email campaign, a mischievous text message about a CASL judgement, an infected OneNote attachment, and a fraudulent CRA text.

...retweeting warnings from the Canadian Anti-Fraud Center.

...posting two news releases, one about combatting scam communications (11/2022) and the other with information on Cybercrime (04/2023).

4.2.3 Competition Bureau

The Bureau increases awareness of CASL-related issues in numerous ways in order to reach as many Canadian consumers and businesses as possible. In 2022-2023, initiatives undertaken by the Bureau included:

Fraud Prevention Month ("FPM")

Yearly event held in March that seeks to help consumers and businesses recognize, reject and report fraud. This year, the Competition Bureau, the Canadian Anti-Fraud Centre, along with the Royal Canadian Mounted Police, Co-Chaired the monthly campaign. This year's theme was "Tricks of the trade: What's in a fraudster's toolbox". On March 1, 2023, the Bureau published a consumer alert on cryptocurrency investment fraud, entitled "Quick easy money? Sometimes it's a quick easy LIE", followed by a series of social media posts throughout the month on related topics of interest. This aligned with the campaign's two sub-themes of cryptocurrency investment fraud and dark patterns. Specific messaging included information about online deceptive marketing practices on subscription traps, fake online reviews, and deceptive free trials.

Competition and Green Growth Summit

On September 20, 2022, the Bureau hosted international experts for a full day event, featuring two panels and an enforcers roundtable, to explore the relationship between competition and green growth. During the enforcers roundtable, discussions focused on the role of competition enforcement as consumers make more environmentally conscious choices in the marketplace. Protecting consumers from false or misleading environmental claims was among the key issues identified by participants, given its importance in building confidence in the green economy. The report on the 2022 Competition and Green Growth Summit is available here.

Virtual Public Information Sessions on the 2022 changes to the *Competition Act*

In the fall of 2022, responding to the coming into effect of amendments to the *Competition Act* in June 2022, the Competition Bureau hosted public information sessions and published updated guidance.

The amendments expanded evidence-gathering powers and increased fines for deceptive marketing provisions, including those prohibiting false or misleading representations in the sender, subject and content of electronic messages, as well as in locator information such as URLs (sometimes referred to as the "CASL- related provisions").

4.2.4 Office of the Privacy Commissioner of Canada

The OPC publishes CASL compliance help for businesses and information for individuals on how to deal with or prevent spam on their websites and social media channels. Although the OPC carries out CASL-related activities throughout the year, *Canada's anti-spam legislation* topic page on its website is its primary information sharing tool.

In 2022-2023, the OPC...

- received **32,273** unique page views of its CASL-related web pages
- processed **70** CASL-related calls, inquiries and submissions from individuals and businesses
- published **45 tweets** and **14 LinkedIn** posts about CASL that resulted in more than **40,000 impressions**
- directed individuals to priv.gc.ca/spam as part of a national library due date receipt campaign to raise awareness when dealing with spam

4.3 Domestic and International Cooperation

4.3.1 Canadian Radio-television and Telecommunications Commission

In 2022–2023, the CRTC continued to foster partnerships with organizations across the globe, strengthening ongoing efforts to combat spam. As a trusted-source partner, the CRTC:

helped take down Cloud Storage domains (i.e., registered websites) that were facilitating violations of CASL.

established new data source partners to enhance the identification of suspected malicious actors operating malware campaigns.

educated law enforcement and banking security personnel to be aware of suspicious trends and behaviors in the marketplace.

In the fall of 2022, regulatory authorities from Canada, Australia, Ireland, Hong Kong, and the United States met in person to find additional ways to combat scams. Hosted by the CRTC, the Combating Scam Communications summit served as a platform for sharing strategic insights about on going initiatives and cross-border enforcement challenges. Participants explored avenues for greater international collaboration to disrupt scam communications.

Representatives from these five countries affirmed their commitment to sustained collaboration and the sharing of strategic information. They also expressed the intention to engage regulatory agencies in jurisdictions that may be the source of or victims of scam communications. The success of this gathering was possible because of existing bilateral relationships between global regulatory agencies, including members of the Unsolicited Communications Enforcement Network (UCENet), which have established Memorandums of Understanding for the sharing of information.

4.3.2 Competition Bureau

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

Organization for Economic Cooperation and Development ("OECD")

The Bureau participates in the Committee on Consumer Policy which aims to strengthen international cooperation on consumers policy. It gathers senior consumer policy and enforcement officials from OECD governments, and works closely with experts from civil society, and businesses.

The committee released two reports in 2022 and 2023. This includes a report on enhancing the effectiveness of online disclosure (October 25, 2022), and a report on dark patterns (October 26, 2022).

International Consumer Protection Enforcement Network ("ICPEN")

The Bureau shares information about cross-border commercial activities that may affect consumers, and encourages global cooperation and the sharing of best practices among consumer protection enforcement agencies.

In partnership with the Authority at the Consumer Rights Protection Centre of Latvia, the Bureau organized and facilitated the May 2022 Dark Patterns Best Practices Workshop for ICPEN members.

The Bureau continues to be a member of ICPEN's econsumer.gov Advisory Working Group which provides information such as cross border complaints and statistical information to ICPEN members.

Global Anti-Fraud Enforcement Network ("GAEN")

Working across international boundaries, GAEN aims to identify the threats posed by international fraud schemes, and collaborate to pursue the offenders and disrupt their activities.

This year, the Bureau shared with members information about certain digital investigations with a focus with restitution.

Additionally, the Bureau is a member of several domestic partnerships and working groups including:

- Canadian Anti-Fraud Centre, Joint Management Team
- Toronto Strategic Partnership
- Alberta Partnership Against Cross-Border Fraud
- Pacific Partnership Against Cross-Border Fraud
- Québec Strategic Partnership

4.3.3 Office of the Privacy Commissioner of Canada

The OPC is a member of several regulatory networks that are concerned with privacy and data protection online, including:

the **Global Privacy Assembly (GPA)**, which connects more than 130 data protection and privacy authorities worldwide to foster international collaboration, including on enforcement within privacy and across regulatory spheres

the **Global Privacy Enforcement Network**, a network of 70+ privacy enforcement authorities, where the OPC is a member of the management committee, participates in enforcement activities/discussions, and hosts/administers the GPEN website

the **G7 group of Data Protection and Privacy Authorities**

the **Unsolicited Communications Enforcement Network (UCENet)**: regulatory authorities seeking to combat unlawful telecommunications, spam and other electronic threats.

The OPC chairs or participates in GPA working groups, including the International Enforcement Cooperation Working Group (IEWG) and the Digital Citizen and Consumer Working Group (DCCWG).

- The IEWG fosters cooperation on critical global privacy issues. In June 2022, the OPC and 5 other IEWG members issued joint guidance for organizations and individuals to protect themselves against cyber security risks associated with credential stuffing.
- The IEWG also held closed enforcement sessions during the year, which allowed members to discuss best practices, strategies, and tactics in relation to key issues of mutual interest, e.g., a technical analysis of "smart glasses".
- The DCCWG studies the intersections between privacy and other regulatory spheres, including competition and consumer protection, and promotes cross-regulatory cooperation. In February 2023, the OPC hosted a workshop where regulators, civil society and other stakeholders shared their perspectives on the privacy and competition intersection, and on experiences of cross-regulatory cooperation in the digital economy.

In July 2022 and November 2022, OPC participated in the 57th and 58th Asia Pacific Privacy Authorities forums.

- At the virtual 57th forum, the OPC presented on its Tim Hortons investigation (into mobile geolocation tracking in the private sector), the anonymization of personal information, its new technology laboratory, and privacy guidance on facial recognition for police agencies.
- At the in-person 58th forum held in Singapore, the OPC spoke on Canadian private sector law reform, the use of biometrics at the Canadian border, and a recent Voice ID investigation. It also participated in discussions concerning privacy during the pandemic and applying the principle of accountability in regulating Artificial Intelligence.

In May 2022, the OPC entered into an enforcement cooperation and information-sharing memorandum of understanding with the data protection authority of Abu Dhabi.

In September 2022, the Commissioner met with his counterparts from the G7 countries in Bonn, Germany, to discuss current regulation and technical issues centered on the concept of "Data Free Flow with Trust": building consumer trust by ensuring high global data protection standards for information flowing across borders.

In October 2022, the OPC attended the annual GPA meeting in Istanbul, Türkiye, where members issued two resolutions on the appropriate use of personal information in facial recognition technology and on building capacity to improve cyber security regulation. The focus was on collectively understanding the potential harms stemming from cyber incidents.

Finally, in January 2023, the OPC entered into a renewed enforcement collaboration and information sharing memorandum of understanding with 6 other UCENet members, including the CRTC.

Domestic cooperation

Federal, Provincial, and Territorial information and privacy commissioners meet annually and discuss in monthly calls matters of public policy and education opportunities of mutual interest. These meetings may lead to calls for action, advocating for consistent privacy protection for Canadians. At the operational level, the OPC collaborates with domestic counterparts through quarterly meetings in the Private Sector Privacy and Domestic Enforcement Collaboration Forums. These forums include representatives from the OPC, Alberta, British Columbia, and Québec.

Following the September 2022 meeting in St. John's Newfoundland and Labrador, the Federal, Provincial, and Territorial Privacy Commissioners and Ombuds with responsibility for privacy issued a joint Resolution on 'Ensuring the Right to Privacy and Transparency in the Digital Ecosystem in Canada'.

Then in November 2022, the FPT group organized a virtual Investigators' Conference to share mutual investigative challenges, and solutions and tips adopted by members to address them.

4.4 Monitoring Compliance

4.4.1 Canadian Radio-television and Telecommunications Commission

The CRTC host the SRC, which collects information that can serve as evidence of potential CASL violations. Additionally, the SRC supplies intelligence to the CRTC's CASL partners.

> In 2022-2023 Canadians submitted 335,807 complaints to the SRC. That is over 6,457 complaints per week.

> Approximately 9643 of these complaints were submitted using the online form, which represents only about 2.8% of total complaints.
>
> The remainder of complaints were sent by email at spam@fightspam.gc.ca.

It is worth noting that the use of the SRC's online form is designed to collect as much information as possible about potential CASL violations. As such, the CRTC has taken steps where it can to direct more complaint traffic towards submission through the online form.

In the CRTC's efforts to monitor compliance, there are continued updates and enhancements to the SRC database to help it and CASL partners better identify cyber threat actors. In 2022-23, several features were added to the SRC database, including enhanced data retention, improved search functions (i.e., more precision), and superior system navigation. A prime example of one of these new features is the SRC's capacity to process PDF documents submitted by Canadians as part of their complaints. This improvement enables the CRTC to swiftly and precisely identify malicious PDF campaigns for investigation.

4.4.2 Competition Bureau

The Compliance Monitoring Unit of the Bureau's Deceptive Marketing Practices Directorate monitors matters, including CASL-related matters, that have been resolved through consent agreements, criminal sentencing orders, alternative case resolutions, or other court orders.

4.4.3 Office of the Privacy Commissioner

Through its Compliance Monitoring Unit, the OPC engages with organizations to ensure they honour their commitments and address the OPC recommendations that flow from reports of findings and compliance agreements.

In 2022-2023, the Unit was satisfied with the actions taken by financial institution Desjardins to implement the OPC's recommendations, following a joint investigation with Québec's *Commission d'accès à l'information* into a 2017-2019 privacy breach.

During the year, the Unit continued to communicate with Tim Hortons on the implementation of the OPC's recommendations, following the completion of a joint investigation with its provincial counterparts in Alberta, BC and Québec (see 'Enforcing CASL below').

4.5 Enforcing CASL

4.5.1 Canadian Radio-television and Telecommunications Commission

The details of CRTC investigations associated with violations of CASL—and any resulting administrative monetary penalties (AMPs) —are published on the CRTC's Enforcement actions web page.

In 2022–2023, the CRTC enforcement measures included:

- **358 Notices to Produce**
- **6 Undertakings**
- **2 Notices of Violation**
- **10 Preservation Demands**
- **4 Warrants**
- **3 Warning Letters**

An enforcement milestone occurred in January 2023 when the CRTC's Compliance and Enforcement team executed warrants to simultaneously search four dwellings in the Greater Montreal Area. This operation marked the CRTC's most extensive search to date, showcasing substantial coordination and support from local law enforcement agencies. The investigation was launched following reports from financial institutions and submissions by Canadians to the SRC, relating to a series of large-scale bank phishing campaigns targeting Canadians and financial institutions in Canada.

To strengthen protections for Canadians, in June 2022, the CRTC found that regulatory action was necessary to ensure Canadian carriers who block botnets do so in a way that provides a baseline level of protection to Canadians. The CRTC's Decision on this matter established overarching guiding principles for a forthcoming network-level botnet-blocking framework. Subsequently, the CRTC directed the Interconnection Steering Committee (CISC) to examine technical parameters that are consistent with the guiding principles and to submit a report outlining the recommendations for doing so. Following this process, the CRTC aims to formalize standards for botnet blocking.

4.5.2 Competition Bureau

In 2022-2023, the Bureau reached an agreement with NuvoCare Health Sciences Inc. ("NuvoCare") and Ryan Foley to resolve the Bureau's concerns about weight loss claims made by NuvoCare on certain natural health products. The Bureau concluded that representations conveying the general impression that the products were proven to cause weight loss – some of which were made by emails - were false or misleading, and unsubstantiated. Those products include WeightOFF Max!, Forskolin+ and Forskolin Nx.

4.5.3 Office of the Privacy Commissioner

In 2022-2023, the majority of the CASL-related complaints submitted to the OPC concerned the alleged receipt of unsolicited communications (email or SMS text spam), or the alleged failure of private sector organizations to offer an unsubscribe function or act upon such a request.

The OPC resolved 1 spam complaint it received in the previous year through its early resolution investigative process. It closed 2 new additional complaints through the same process. Another 3 complaints have been assigned to early resolution and are expected to be addressed in 2023-2024, and the jurisdiction of a 4th case is under review.

Several additional complaints were resolved by directing individuals to initially address their concerns with the privacy officer of the relevant organization. Alternatively, they were guided to seek resolution through other channels such as the Do Not Call List, the SRC, and/or the Canada Anti-Fraud Centre.

Thanks to CASL's amendments to PIPEDA in 2011, the OPC has been able to collaborate and share information more easily with other domestic and international data protection authorities on compliance and enforcement matters.

Domestically, the OPC collaborates on investigations with privacy enforcement counterparts in Alberta, British Columbia and Québec:

In June 2022, the OPC and its counterparts issued the Report of Findings of their joint investigation into the Tim Hortons' mobile app. The investigation found that:

- The app erroneously informed users it would only collect geolocation data when it was in use, while it in fact tracked users as long as their devices were on;
- This vast collection resulted in privacy harm that was disproportionate to any gains Tim Hortons hoped to obtain from improved promotion of its coffee and other products;
- Tim Hortons continued to collect location data for a year after shelving plans to use it for targeted advertising, having no legitimate need to do so;
- Tim Hortons' contract with an American third-party location services supplier contained vague and permissive language that would have allowed the company to sell "de-identified" (but easily re-identifiable) location data for its own purposes; and
- Tim Hortons lacked a robust privacy management program for the app, which would have allowed the company to identify and address many of these privacy contraventions.
- The company agreed to implement the privacy authorities' recommendations.

In February 2023, the OPC and its counterparts in Alberta, BC and Québec announced a joint investigation into the privacy practices of TikTok.

- The investigation will examine whether valid and meaningful consent is being obtained for the collection, use and disclosure of personal information, and if the company is meeting its transparency obligations.
- The joint investigation will have a particular focus on TikTok's privacy practices as they relate to their many younger users.

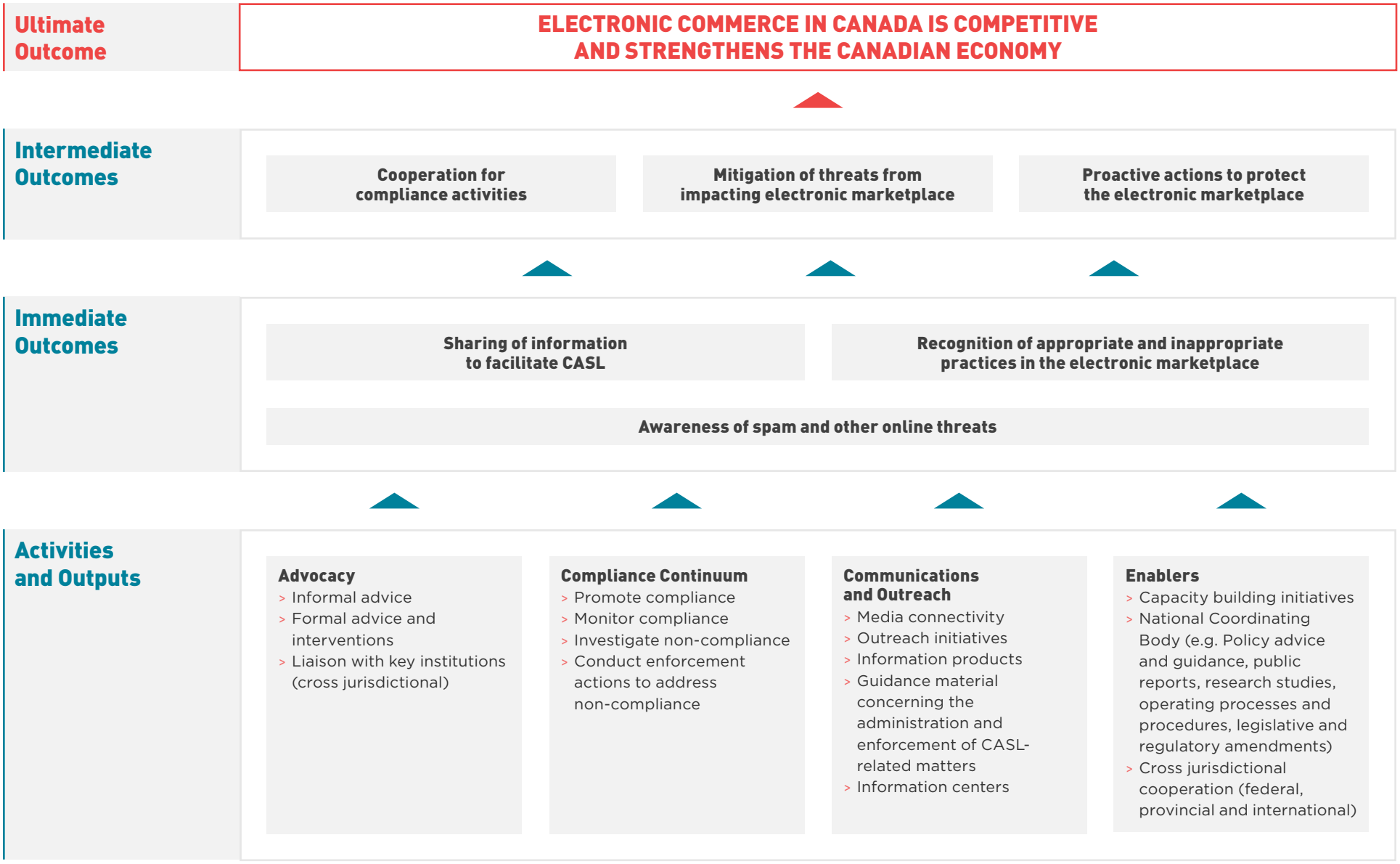
Internationally, the past fiscal year saw the OPC share information and cooperate with various counterparts, including the UK Information Commissioner's Office and the US Federal Trade Commission, on a range of compliance activities. These included active and confidential OPC investigations that were international in scope.

5. Summary

The ubiquity of electronic threats underscores the importance and relevance of CASL in continuing to help protect Canadians from spam and other cyberthreats that can lead to harassment, identity theft, and fraud.

In fiscal year 2022-2023, CASL partners continued to ensure the effectiveness of the CASL initiative by taking numerous unilateral and collaborative steps to promote awareness of and compliance with CASL. They also continued to forge partnerships with organizations across the globe to better fulfill their respective mandates and to advocate for higher standards of cybersafety for all communities.

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 1 ultimate outcome:

1. Electronic commerce in Canada is competitive and strengthens the Canadian economy.