Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

2023-2024

Trust, innovation, and protecting the fundamental right to privacy in the digital age

Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*

This document is available on the Web at www.priv.gc.ca

Cette publication est aussi disponible en français.

The html version of this report takes precedence over this document in case of a discrepancy.

2023-2024 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*

Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau, Quebec K1A 1H3

Cat. No. IP51-1E-PDF
ISSN 1913-3367

Letter to the Speaker of the Senate

June 6, 2024

The Honourable Raymonde Gagné, Senator
Speaker of the Senate
Senate of Canada
Ottawa, Ontario K1A 0A4

Dear Madam Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada, for the period from April 1, 2023 to March 31, 2024 entitled, *Trust, innovation, and protecting the fundamental right to privacy in the digital age*. This tabling is done pursuant to section 38 of the *Privacy Act* and section 25 of the *Personal Information Protection and Electronic Documents Act*.

Sincerely,

Original signed by

Philippe Dufresne
Commissioner

Letter to the Speaker of the House of Commons

June 6, 2024

The Honourable Greg Fergus, M.P.
Speaker of the House of Commons
House of Commons
Ottawa, Ontario K1A 0A6

Dear Mr. Speaker:

I have the honour to submit to Parliament the Annual Report of the Office of the Privacy Commissioner of Canada, for the period from April 1, 2023 to March 31, 2024 entitled, *Trust, innovation, and protecting the fundamental right to privacy in the digital age*. This tabling is done pursuant to section 38 of the *Privacy Act* and section 25 of the *Personal Information Protection and Electronic Documents Act*.

Sincerely,

Original signed by

Philippe Dufresne
Commissioner

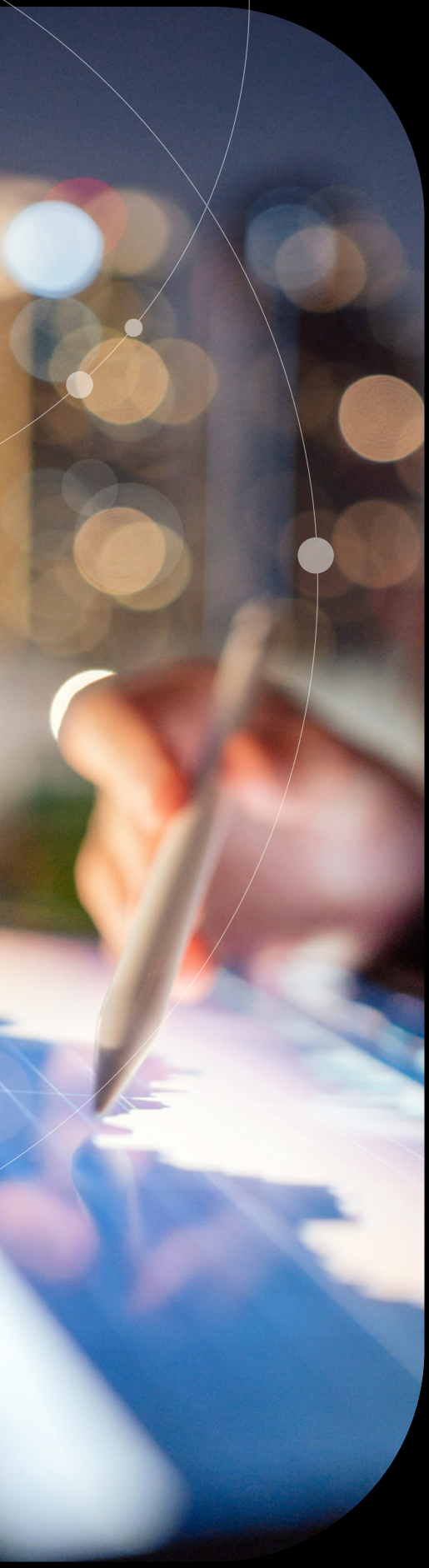


Table of contents

Commissioner's message

I am pleased to submit my 2023-2024 Annual Report to Parliament, highlighting the work of the Office of the Privacy Commissioner of Canada (OPC) over the last fiscal year.

This report details the activities and achievements of my Office to protect and promote the fundamental right to privacy of Canadians. It covers both the *Privacy Act*, which applies to the personal information handling practices of federal government institutions, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal private-sector privacy law.

Central to the work of this past year was the launch of my Strategic Plan in January 2024. Entitled *A roadmap for trust, innovation and protecting the fundamental right to privacy in the digital age*, the plan will guide the efforts of the OPC through to 2027.

The Strategic Plan focuses on three priority areas:

- **Protecting and promoting privacy with maximum impact** by using business intelligence to identify trends that need attention, producing focused guidance and outreach, leveraging strategic partnerships, and preparing for the implementation of potential new privacy legislation;
- **Addressing and advocating for privacy in this time of technological change** with a focus on artificial intelligence (AI) and generative AI, the proliferation of which brings both potential benefits, and increased risks to privacy; and
- **Championing children's privacy rights** to ensure that their unique privacy needs are met, and that they can exercise their rights.

These priorities are reflected in the achievements of my Office over the past year and the outcomes of collaborative engagements with my domestic and international data protection counterparts. This includes issuing a joint statement with G7 data protection and privacy authorities on generative AI, and launching new Principles for responsible, trustworthy, and privacy-protective generative AI technologies with my provincial and territorial counterparts.

In the spring of 2023, I launched a joint investigation with my counterparts in Quebec, British Columbia, and Alberta into OpenAI's ChatGPT.

In December, I also had the pleasure of hosting an international symposium on privacy and AI. The event brought experts from academia, industry, civil society, and government, as well as fellow privacy authorities, to the National Capital Region to discuss how we can protect privacy while harnessing innovation in the context of AI.

Other highlights of our collaborative engagements are the joint resolutions that I issued with my fellow provincial and territorial regulators on the privacy of young people and privacy in the workplace.

To support our public sector work, we launched an online submission form for federal institutions to submit Privacy Impact Assessments.

This report also provides information on advice and recommendations that I have made to Parliamentarians on legislation and privacy issues that were being studied by Committees.

As Bill C-27, the *Digital Charter Implementation Act*, moved through the Parliamentary process, I also had the opportunity to appear before lawmakers to discuss some of the ways that the proposed new private-sector privacy law could be improved to better protect the fundamental right to privacy.

Personal information is increasingly sought after in the digital age and protecting privacy has become one of the paramount challenges of our time. The importance of protecting privacy is exemplified in recent investigations, such as the report of findings following my Office's investigation into Pornhub operator Aylo.

The investigation found significant problems that allowed highly sensitive and intimate content to be posted online without the direct knowledge or consent of those depicted. This led to devastating consequences for the woman at the centre of this investigation and other victims, including social stigmatization, psychological damage, financial loss, and even attempted suicide. I released the findings in February, just as Parliamentarians began debating the *Online Harms Act*, legislation aimed at addressing similar issues to those that we examined in our Aylo investigation.

Just as data is used to fuel innovation, innovation must also be used to protect data. As the world embraces the digital age and opportunities, we must ensure that it does so in a privacy-protective way. It is the message that I intend to repeat as Canada's G7 Presidency in 2025 approaches, when I will host my fellow G7 data protection regulators for a roundtable where many of these issues will be discussed.

As Canada's Privacy Commissioner, I am committed to strong advocacy, education, promotion, enforcement, and importantly, collaboration. This report highlights our outreach activities with individuals, businesses, and federal institutions, as well as engagements with domestic and international partners. In an age where data knows no borders, effective privacy protection demands a global effort. I look forward to continuing to work collaboratively to ensure that the fundamental right to privacy is protected for current and future generations.

Philippe Dufresne
Privacy Commissioner of Canada

Timeline

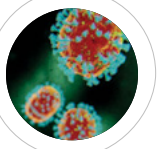
Key activities of the Office of the Privacy Commissioner of Canada (OPC) in 2023-2024.

April **2023**

ChatGPT investigation

Commissioner Dufresne announces investigation into the company behind AI-powered chatbot ChatGPT. In the following weeks, the Commissioner, along with his counterparts from Quebec, British Columbia, and Alberta, announce that they will jointly investigate the matter.

May **2023**



Special report on pandemic-related investigations

Special Report to Parliament outlines findings of several OPC investigations and advisory initiatives that examine federal government's privacy practices in relation to pandemic measures.

June **2023**

G7 data protection and privacy authorities; joint statement on generative AI

Joint statement calling on developers and providers of generative AI technologies to embed privacy in the design, conception, operation, and management of new products and services.

June **2023**

Canadian Digital Regulators Forum launch

Commissioner Dufresne joins his counterparts at the Competition Bureau and Canadian Radio-television and Telecommunications Commission in new forum to strengthen collaboration on matters related to digital markets and platforms.

August **2023**

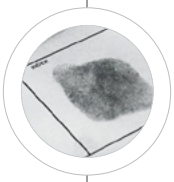
Joint statement on data scraping and the protection of privacy

Commissioner Dufresne and representatives from 11 other members of Global Privacy Assembly sign joint statement to mitigate the risks of unlawful data scraping.

September **2023**

Commissioner Dufresne discusses key recommendations to improve Bill C-27

Appearing before a Commons committee studying the *Digital Charter Implementation Act*, Commissioner Dufresne calls the Bill a "step in the right direction" that "must go further" to protect the fundamental right to privacy and lays out 15 key recommendations.



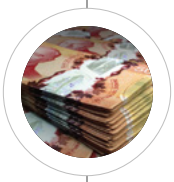
October **2023**

OPC invites input on draft biometrics guidance

OPC releases draft guidance documents on privacy obligations when handling biometric information, which are aimed at businesses and public institutions.

Submission to government consultation on strengthening Canada's anti-money laundering and anti-terrorist financing regime

OPC responds to Finance Canada's Consultation Paper examining ways to strengthen Canada's Anti-Money Laundering/Anti-Terrorist Financing regime.



October **2023**

October **2023**

Privacy regulators pass resolutions on young people and workplace

Federal, provincial, and territorial privacy authorities call on their respective governments to do more to protect the rights of children and workers.

Commissioner Dufresne investigates cyberattack on relocation services

Investigations under both the *Privacy Act* and PIPEDA are launched following a cyberattack that affected the personal information of current and former Government of Canada personnel and members of the Canadian Armed Forces and Royal Canadian Mounted Police (RCMP).

November **2023**

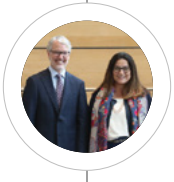
December **2023**

Privacy Commissioner of Canada hosts international symposium on privacy and AI; launches joint principles on generative AI

Commissioner Dufresne welcomes experts to a symposium to discuss opportunities and risks involved in generative AI and how to work together to prepare for them. Together with Canadian privacy authorities, the Commissioner launches Principles for responsible, trustworthy and privacy-protective generative AI technologies.

Joint statement on privacy and democratic rights to mark Human Rights Day

To mark the 75th anniversary of the proclamation of the Universal Declaration of Human Rights, Commissioner Dufresne signs a statement on behalf of the Global Privacy Assembly's Data Protection and other Rights and Freedoms Working Group. He is joined by Dr. Ana Brian Nougrères, United Nations Special Rapporteur on the Right to Privacy.



December **2023**

Commissioner Dufresne launches strategic plan

Commissioner marks Data Privacy Week with the launch of his Strategic Plan, which identifies three strategic priorities, including: protecting and promoting privacy with maximum impact, addressing and advocating for privacy in this time of technological change, and championing children's privacy.

January **2024**

Investigation into data breach at Global Affairs Canada

Privacy Commissioner announces investigation after receiving several complaints related to a data breach at Global Affairs Canada involving a cyberattack on an internal network that compromised the personal information of users, including employees.

February **2024**

Special reports outline findings in GCKey/Canada Revenue Agency cyberbreach and RCMP's Project Wide Awake investigations

Two separate *Privacy Act* investigations underscore need for stronger security safeguards and increased due diligence to better protect the privacy of Canadians.

February **2024**

Investigative findings into Pornhub operator released

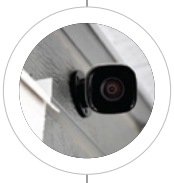
Privacy Commissioner releases findings on investigation into the operator behind Pornhub and other pornographic sites. Investigation concludes that Aylo contravened Canadian privacy law by enabling intimate images to be shared on its websites without the direct knowledge or consent of everyone depicted.

February **2024**

Privacy regulators welcome changes to Airbnb policy on surveillance camera use

Commissioner Dufresne joins Quebec, British Columbia, and Alberta counterparts in issuing a statement welcoming Airbnb's decision to update its global policy on the use of security cameras at rental accommodations and implement the recommendations that the regulators had made to the company the year before.

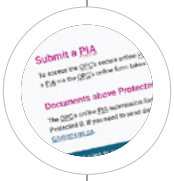
March **2024**



New online submission form for PIAs

OPC makes it easier for federal institutions to submit privacy impact assessments (PIAs) with the launch of a new online PIA submission form.

March **2024**



Top trends in privacy

Technology and digital interconnectivity continue to transform the lives of individuals and have also brought forth an era of new privacy issues. Here are five pivotal trends that are shaping the privacy landscape in Canada and beyond.

Privacy concerns amidst the ongoing rise of digital connectivity

Greater volumes of data are being shared, used, and stored online than ever before. Despite a heavy reliance on digital platforms, there is limited trust, particularly when it comes to social media companies, and growing concern about how personal information is protected in the digital age.

- Digital connectivity has doubled in 10 years, with more than 5.35 billion Internet users worldwide and 5.6 billion mobile device users. Canada boasts a high Internet penetration rate of approximately 95%.[1, 2]
- Canadians spend an average of 6 hours and 18 minutes online per day.[1, 2]
- 91% of Canadians believe that at least some of what they do online or on their smartphones is being tracked by companies or organizations.[3]

- Only 1 in 10 Canadians say that they **trust social media** to protect their privacy.[3]
- Primary motivations for using social media include staying connected with friends and family (58.2%), passing leisure time (43.3%), and accessing news content (31%).[2]

Greater concerns related to children's privacy rights

A global trend toward greater concern for the privacy of young people is driving the development of new laws, regulations, guidelines, and initiatives that are aimed at protecting children's privacy by governments and data protection authorities around the world. This includes, for example, legislative initiatives in the UK and elsewhere to introduce age-appropriate design requirements, as well as large fines against companies like TikTok and Meta following investigations related to children's privacy.

- 59% of young people worldwide report spending more than two hours of their average day on social media.[4]
- 75% of young people find that the technical language of social media terms of service is hard to understand and feel that a take-it-or-leave-it approach forces them to choose between social exclusion or signing up at the cost of their privacy.[4]

- **78%** of Canadian youth use YouTube and social media for the most popular online activity, watching videos.

  Messaging ranks second at **70%**.[5]

- TikTok is the top social media platform for Canadian youth, ahead of Snapchat and Instagram, with 53% using TikTok in the past month.[5]
- 12% of Canadian businesses report collecting personal information from minors; 73% say that they use age-appropriate language to explain their privacy policies and 27% say that they carry out PIAs before offering tools or products that are aimed at young people. [6]

Rising threat and severity of cyberbreaches

Data breaches have surged over the past decade. In particular, ransomware and malware attacks are sharply rising. This risk of cyberattacks and data exfiltration from a variety of threat actors is of great concern to private and public sector organizations, and the majority of individuals are concerned about identity theft.

- Data breaches have more than tripled between 2013 and 2022. More than 2.6 billion personal records were exposed worldwide in the past two years alone.[7]
- 94% of organizations around the world experienced a cyberattack of some form in the last year; 28% were targeted by a ransomware attack, and 41% by malware.[8, 9]
- Since 2020 the frequency of ransomware attacks worldwide has increased, surging by 50% year-on-year during the first half of 2023 alone.[10]
- Business leaders and privacy professionals around the world believe that a cyberattack or data breach is the #1 risk facing their organizations.[11, 12]

- In 2023-2024, private-sector organizations reported 693 breaches to the OPC, affecting approximately 25 million Canadian accounts, compared with 681 breaches the previous year, affecting approximately 12 million accounts.
- 90% of Canadians are at least somewhat concerned about identity theft, and around half are extremely concerned.[3]

Increased development in, use of, and concern about AI

The proliferation of artificial intelligence and generative AI technologies, in Canada and around the world, is generating privacy concerns.

- AI is expected to see an annual global growth rate of 37.3% from 2023 to 2030.[13]
- 42% of enterprise-scale businesses around the world say they have already integrated AI into their operations; 40% are considering doing so.[14]
- 6% of Canadian businesses say that they use AI for business operations; of those not using AI, nearly 25% say that they intend to do so in the next five years.[6]

- The number of Canadians who believe that AI tools are bad for society is increasing, from 25% in 2023 to 32% in 2024 and 81% have privacy concerns about AI.[16]
- Over 90% of Canadians say that AI development should be guided by ethical principles and 78% believe its use should be regulated.[17]

Strengthening fundamental rights with an expansion of privacy laws

Influenced by the EU's experience with the General Data Protection Regulation (GDPR), a new generation of privacy laws are being enacted and applied in many parts of the world. There are likewise efforts to modernize Canada's federal private-sector privacy law with stronger rules, regulatory powers, and incentives to enhance individuals' right to privacy.

- 137 countries have national data privacy laws, a 14.2% increase since 2017, with the result that 6.3 billion people in the world (79.3%) are now covered by privacy laws.[18]

- In 2023, violations of the GDPR cost companies over $2 billion euros (more than 2019, 2020 and 2021 combined), impacting companies beyond EU borders.[19]
- Commissioner Dufresne has made 15 key recommendations to improve and strengthen Bill C-27, which would update Canada's private-sector privacy law, including recognizing privacy as a fundamental right.[20]
- Dozens of countries have already enacted AI laws and policies, such as the *EU AI Act*, which is the first comprehensive legal framework on AI and may have the same effect globally as the GDPR, and others are actively drafting and debating privacy issues in connection to AI laws.[21]

1: DataReportal, Digital 2024: Global Overview Report; 2: DataReportal, Digital 2024: Canada, 2024; 3: OPC, Survey of Canadians on Privacy-Related Issues, 2022-23; 4: Amnesty International, Global Survey, 2023; 5: MTM JR, What's new and what's next? Kids, teens and social media, 2023; 6: OPC, Survey of Canadian Businesses on Privacy-Related Issues, 2023-2024; 7: MIT/Apple, The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase, 2023; 8: Sophos, The State of Cybersecurity, 2023; 9: Thales, Global Data Threat Report, 2024; 10: Canadian Centre for Cyber Security, National Cyber Threat Assessment, 2023-2024; 11: Aon, Global Risk Management Survey, 2023; 12: IAPP/KPMG, Privacy Risk Study, 2023; 13: Grandview Research, Artificial intelligence Market Size and Trends, 2023; 14: IBM, Global AI Adoption Index, 2023; 15: CISCO 2024 Data privacy benchmark study; 16: Leger, Use of AI Tools, 2024; 17: Telus, AI Report, 2024; 18: IAPP, Identifying global privacy laws, relevant DPAs, 2024; 19: Statista, EU Data Protection Fines Hit Record High in 2023, 2024; 20: OPC, 15 Key Recommendations on Bill C-27, 2023; 21: IAPP, Global AI Law and Policy Tracker, 2024.

Spotlight on strategic priorities

In January 2024, Commissioner Dufresne launched his Strategic Plan for the OPC: A roadmap for trust, innovation and protecting the fundamental right to privacy in the digital age. The Strategic Plan will guide the work of the Office of the Privacy Commissioner of Canada (OPC) over the next three years, focusing on three priority areas:

1. **Protecting and promoting privacy with maximum impact** by using business intelligence to identify trends that need attention, producing focused guidance and outreach, leveraging strategic partnerships, and preparing for the implementation of potential new privacy legislation;

2. **Addressing and advocating for privacy in this time of technological change** with a focus on artificial intelligence (AI) and generative AI, the proliferation of which brings both potential benefits, and increased risks to privacy; and

3. **Championing children's privacy rights** to ensure that their unique privacy needs are met, and that they can exercise their rights.

These strategic priorities focus on issues where the OPC can have the greatest impact, and where the greatest risks lie if they are not addressed. They build on the vision for privacy that the Commissioner has articulated since taking on his role in 2022: that privacy is a fundamental right; that privacy supports the public interest and Canada's innovation and competitiveness; and that privacy accelerates Canadians' trust in their institutions and in their participation as digital citizens.

The Strategic Plan offers an overview of the kinds of initiatives that the OPC is undertaking for each priority and the outcomes that the Commissioner intends to achieve. All three strategic priorities include the themes of engagement, partnerships, collaboration, and continued learning.

Strategic priority 1:

Protecting and promoting privacy with maximum impact

This priority serves as the bedrock for fulfilling the OPC's existing mandate, applying existing laws to new and emerging challenges, and preparing for potential changes to federal privacy laws. It commits the OPC to strengthen governance and capacity, foster internal communications and collaboration, and nurture partnerships and networks, at home and abroad, optimizing programs and services that respond to the needs of Canada and Canadians.

In 2023-2024, activities to advance these objectives included:

- Issuing 15 key recommendations to Parliament to strengthen Bill C-27 as part of the Commissioner's submission on the Bill, and preparing for its potential implementation;
- Creating a new Directorate of International, Provincial, and Territorial Relations to bolster engagements with other regulators and privacy organizations;
- Issuing an investigation report into Pornhub operator Aylo, reiterating that the non-consensual sharing of intimate images is a serious privacy violation;
- Creating two new positions; first, the position of Deputy Commissioner and Senior General Counsel, to address increased legal activity, and second, a Chief Services and Digital Officer, to guide the implementation of a digital vision and agenda; and
- Continuing modernization efforts to improve document and data management practices as a foundation for data-informed decisions.

Strategic priority 2:

Addressing and advocating for privacy in this time of technological change

Rapidly evolving and transformative technological advancements, such as AI offer potential opportunities and benefits, but they can also increase risks to privacy.

To advance this priority, the OPC is focusing on enhancing internal capacity, forging strategic partnerships, fostering a culture of privacy, and encouraging the use of privacy-by-design principles for existing and emerging technologies that support innovation while protecting privacy rights.

In 2023-2024, the OPC undertook several activities in connection with this priority, including:

- Hosting an international symposium on privacy and AI;
- Issuing a joint statement on AI with G7 authorities and adopting a resolution on responsible generative AI with other members of the Global Privacy Assembly;
- Launching joint principles for responsible generative AI with provincial and territorial counterparts;
- Conducting stakeholder consultations on draft guidance on biometric technologies;
- Launching an investigation into OpenAI, the company behind ChatGPT, with Quebec, British Columbia, and Alberta counterparts;
- Inviting research proposals through the OPC Contributions Program on the privacy impacts of immersive and embeddable technologies;
- Forming a multi-disciplinary team within the OPC to work collaboratively to tackle the impact of AI on the public and private sectors; and
- Establishing an environment for the OPC's Technology Analysis Directorate for testing, research, and analysis on generative AI.

Strategic priority 3:

Championing children's privacy

This strategic priority recognizes the unique sensitivities around children's privacy and the need to ensure that their rights are protected so that they can benefit from technology without compromising their privacy and well-being. The OPC is deepening its expertise and understanding of children's privacy issues, engaging with young people and those who advocate for them for informed education and outreach, expanding partnerships to increase the uptake of OPC resources, and applying a children's privacy lens to compliance work.

During 2023-2024, OPC activities related to children's privacy included:

- A joint investigation into TikTok's privacy practices as they relate to young users in collaboration with Quebec, British Columbia, and Alberta counterparts;
- Recommending to Parliament that Bill C-27's preamble recognize that the processing of children's personal data should respect the best interests of the child;
- Adopting a resolution with provincial and territorial colleagues calling on governments and organizations to improve privacy protections for children, and producing a child-friendly version of the resolution and a companion guide for organizations;
- Holding a series of roundtable discussions on the best interests of the child in the processing of their personal data;
- Participating in a meeting of the Young Canadians' Parliament to hear from youth about their views on privacy;
- Inviting research proposals for the OPC Contributions Program on the theme of ensuring children's privacy in the digital era; and
- Participating in the Global Privacy Assembly's Age Assurance Working Group on efforts to promote harmonization in the approach to age assurance.

The OPC invited feedback on the Strategic Plan for 2024-2027 when the plan was published, to help inform the implementation of the priorities and generate ideas on how it can most effectively advance each of the three interconnected priority areas. Recognizing the dynamic nature of the priorities selected, the OPC intends to remain agile, so that it may adapt to changing circumstances, effectively report on progress, and best collaborate with its many partners and stakeholders on the important work ahead.

Privacy Act: A year in review

In its 2023-2024 public sector work, the OPC noted an increased interest by federal departments to leverage digital technologies.

An important part of the OPC's work is helping federal institutions to identify and mitigate the privacy-related impacts of new technologies. Privacy Impact Assessments (PIAs) are an important tool to achieve this purpose. The OPC consulted with departments and stakeholders on ways to enhance and improve the PIA process. As a result of feedback received, the OPC launched a new online form that provides a simple, secure means for federal institutions to submit PIAs to the OPC for review.

The OPC also sought input from government organizations on its draft guidance on biometrics through a public consultation that was launched in October 2023. The use of biometrics is surfacing more often in OPC investigative work. At the time of writing, the feedback received was being analyzed as part of the OPC's consultation on draft biometrics guidance documents.

In 2023-2024, the OPC completed 1,278 investigations into complaints against federal institutions, both through early resolution as well as more formal investigations, including summary investigations. This represents a 28% increase over 2022-2023, when the OPC closed 999 investigations.

In February 2024, the OPC tabled special reports in Parliament with findings regarding two separate *Privacy Act* investigations. The first concerned a major privacy breach at Employment and Social Development Canada (ESDC) and the Canada Revenue Agency (CRA) involving vast amounts of sensitive personal information. The second examined the Royal Canadian Mounted Police's (RCMP) use of private-sector surveillance and monitoring services in law enforcement.

Commissioner Dufresne also launched investigations following two major cyberattacks involving federal government institutions. The first investigation that was launched in November 2023 involves a breach affecting the personal information of federal government personnel who used government-contracted relocation services over the past two decades. This breach involves several federal institutions, as well as two third-parties that were contracted by the institutions. The second investigation that was launched in February 2024, involves a breach of a Global Affairs Canada (GAC) virtual private network.

The following section highlights key initiatives under the *Privacy Act* in 2023-2024.

Privacy by the numbers

Privacy Act

Complaints accepted	1,113
Well-founded complaints	412
Complaints closed through early resolution	642
Complaints closed through standard investigation	636
Data breach reports received	561
New advisory consultations opened with government institutions	89
Privacy impact assessments (PIAs) received	123
Letters of recommendation and advice provided to government institutions following PIA review or consultation	137
Public interest disclosures by federal organizations	569

Government advisory work

Members of OPC's Government Advisory Directorate at the Canadian Access and Privacy Association conference in Ottawa, Ontario.

Outreach and capacity-building

The OPC helps federal institutions understand and apply the *Privacy Act* and build privacy risk analysis and protections into programs and activities from the outset. To this end, the OPC's Government Advisory Directorate offers presentations and workshops for departments and agencies to help enhance knowledge and build capacity related to the handling of personal information.

In 2023-2024, the OPC focused on reaching a wider range of federal institutions to increase awareness of PIA fundamentals and the OPC's availability for advisory consultations. These activities included targeted presentations to individual institutions, webinars, panel discussions, and joint events with the Treasury Board of Canada Secretariat (TBS) that were hosted by the Canada School of Public Service. Through 10 outreach events, the OPC reached 127 federal institutions that are covered by the *Privacy Act*.

Consultations with TBS

The OPC and TBS have distinct and complementary roles in overseeing compliance with the *Privacy Act* in that the Privacy Commissioner, as an agent of Parliament, is an independent guardian of Canadians' privacy rights, while TBS creates government-wide policies, directives, and guidelines.

During 2023-2024, the OPC met with TBS to address privacy issues and provided input and advice on several TBS policy instruments.

Government advisory activities

RCMP use of on-device investigative tools

In September 2023, the RCMP submitted a PIA on its use of on-device investigative tools (ODITs) to collect information from digital devices – a requirement under TBS directive that the OPC identified had not been met in the previous year.

Following a review of the PIA, the OPC recommended that the RCMP's use of such tools be assessed regularly for necessity and effectiveness; that the RCMP clearly describe the exigent circumstances that might lead to use of such tools without judicial authorization; and that the provision of related services to other government agencies be covered under information-sharing agreements.

The OPC also recommended that the RCMP have procedures in place to delete any personal information that it collects that is not covered by a warrant or necessary to the investigation. Our engagement on this file is ongoing.

RCMP use of facial recognition

The RCMP's use of facial recognition technology to investigate human trafficking and child sexual exploitation is an example of a public-private partnership that implicates both the *Privacy Act* and PIPEDA.

In consultations with the RCMP, the OPC emphasized the importance of identifying and mitigating privacy risks before implementing new technologies, particularly those with facial recognition capabilities, and recommended that the RCMP consider not using a particular facial recognition technology until it has completed a thorough assessment of the privacy risks and compliance with Canadian public- and private-sector privacy laws. At the time of writing, the OPC was awaiting a PIA addressing the concerns that were raised during the consultation.

Federal employment equity self-identification modernization

TBS has collected personal information for the voluntary Employment Equity Self-Identification process for the federal public service for more than 30 years. It recently launched an exercise to expand information collection by adding a new open-text field for respondents to write in other identities that are not represented in the existing questionnaire options.

The OPC advised TBS that self-identification information may be considered sensitive, and that the expansion of categories is likely to increase the volume of personal information that is collected. The OPC has been consulting with TBS on this process for several years and received a PIA in July 2023.

The OPC recommended that TBS carefully monitor and assess whether collecting the new self-identification variables is effective in meeting the stated purpose of identifying systemic discrimination and promoting equity in staffing practices.

The OPC provided comments to the government's *Employment Equity Act Review Task Force*, noting that privacy is a fundamental right that underpins the values of personal autonomy, identity, dignity and integrity which are inherent in the core objectives of the Employment Equity framework.

In its submission, the OPC expressed its support for the important purposes of the *Employment Equity Act* and the critical work of the Task Force. The OPC noted that institutions need clear legal authority under Section 4 of the *Privacy Act* for such activity, personal information should be collected directly from employees, and clear notice of the purpose for the collection must be provided. The OPC also cautioned against collecting more personal information than is necessary.

Canadian Dental Care Plan

The OPC is consulting extensively with the various government departments that are tasked with rolling out the new Canadian Dental Care Plan, a federal government program that is intended to provide coverage for eligible Canadians who do not have dental benefits.

The OPC provided advice to the departments on ensuring that the privacy practices of third-party contractors are sufficient and noted the need for adequate safeguards for collecting and processing the personal information that is required for applicants to receive program benefits. The OPC recommended that there be strong information-sharing agreements between all parties to ensure that privacy is protected consistently across departments. Discussions will continue, with the goal of building privacy into the program design as the plan rolls out in stages over the next few years.

Online passport applications project

In 2023, the OPC reviewed and provided recommendations related to an Immigration, Refugees and Citizenship Canada (IRCC) pilot project for online passport applications. The pilot is limited to simplified renewal applications that are submitted within Canada and was tested with volunteer federal employees.

As part of the process, applicants submit live digital photographs to an external cloud storage service that is managed by IRCC. The data is downloaded and manually entered into IRCC's Global Case Management System for processing the passport applications.

The OPC anticipates receiving a PIA for the full rollout of the online passport application program and recommends that IRCC carefully identify technical privacy risks, including risks associated with using cloud services.

International humanitarian assistance

The OPC was consulted by Public Safety Canada and GAC on the development of a program that would allow humanitarian groups to apply for authorization to provide aid in geographic locations that are controlled by terrorist groups.

While it is an offence under the *Criminal Code* to provide support for terrorist activity, or to benefit any person carrying out terrorist activity, new legislation provides exceptions for the delivery of humanitarian assistance by impartial organizations that are operating under international law in areas that are controlled by terrorist groups. Canadian organizations may now apply for specific authorization to deliver human rights programming, support for government operations, food aid, and support for the general population in such regions.

Because several federal institutions will be involved in screening applications and issuing the authorizations, and given the sensitivity of the personal information that is collected, the OPC highlighted the need for information-sharing agreements with strong privacy protection clauses. Clear rules should be in place for the collection of personal information from social media as part of the vetting process. The OPC also advised that the consent and notification statements that are given to applicants should contain clear and detailed descriptions of how the collected information will be used.

The OPC anticipates receiving a multi-institutional PIA for this program, led by Public Safety, and will continue to consult with departments as the initiative moves forward.

Privacy Act compliance actions

In 2023-2024, the OPC accepted a total of 1,113 *Privacy Act* complaints. This represented a 10% decrease from 2022-2023, from 1,241 complaints.

As was the case in 2022-2023, the RCMP (266 complaints) and Correctional Service Canada (CSC) (201 complaints) were the institutions for which the OPC accepted the largest number of complaints. These were followed by IRCC (110 complaints), the Canada Border Services Agency (CBSA) (103 complaints), and the Department of National Defence (DND) (78 complaints).

More than half (54%; 603 complaints) of these complaints were related to the length of time that institutions took to respond to personal information access requests – which are referred to as time-limits complaints. The OPC also received several complaints that were related to the application of exemptions to withhold requested information or allegations of missing records (30%), as well as allegations of unauthorized collection, use, and disclosure of personal information (16%).

The OPC also noted an increase in the number of complaints that were received from non-Canadians under the *Privacy Act*. Extension Order No. 3, which came into effect in July 2022, provides foreign nationals who are outside Canada with the right to access, or to correct, their personal information that is held by organizations that are subject to the Act. Of the 268 complaints that were received from foreign nationals, 68% (183) were closed at intake, as most were questions about visa applications and therefore outside of the OPC's jurisdiction.

The OPC also received 561 privacy breach reports from federal institutions, with the majority relating to the loss or misplacement of records that contain personal information (68%). Unauthorized access (for example, incidents resulting from employees misusing their access privileges or social engineering attacks) was the second most common type of reported breach (16%). In addition, 15% of all breaches that were reported were related to unauthorized disclosures, with the majority caused by employee errors, for example, through misdirected correspondence or the mishandling of information.

Top institutions by complaints accepted	
Respondent	**Number**
Royal Canadian Mounted Police	266
Correctional Service Canada	201
Immigration, Refugees and Citizenship Canada	110
Canada Border Services Agency	103
National Defence	78
Canada Revenue Agency	76
Employment and Social Development Canada	32
Canadian Security Intelligence Service	23
Global Affairs Canada	21
Transport Canada	20
Canada Post Corporation	20

Time limit investigations treatment times	
Fiscal year	**Average treatment time in months**
2023-2024	**1.80**
2022-2023	2.10
2021-2022	2.91
2020-2021	5.04
2019-2020	7.50

On the workload front, temporary funding that was received in the 2023 federal budget allowed the OPC to hire additional resources and reduce its backlog of complaints. At the end of March 2024, the investigative backlog represented 20% of all ongoing investigations, which comprises investigations under the *Privacy Act* and PIPEDA. This was a decrease from 2022-2023, when 24% of ongoing investigations were backlogged.

The OPC also began implementing efficiency strategies that were identified as a result of a diagnostic review that was carried out in 2022-2023. While the OPC continues to work to identify effective ways to resolve and investigate complaints, without additional permanent funding, the backlog is at risk of remaining high.

Early resolution

Early resolution is an integral investigative tool used by the OPC to resolve low-complexity, non-systemic complaints quickly and efficiently. The OPC uses approaches such as engagement and negotiation to provide the best outcome for the parties involved. In these cases, the OPC does not issue a formal finding.

In certain instances, the OPC will conduct a summary investigation to address low-complexity, non-systemic complaints. Summary investigations are considered through a variety of factors when resolution of the matter has been determined to no longer be a possibility, but where the investigation is mostly or fully completed.

Percentage of all complaints closed in early resolution	
Fiscal year	**Percentage**
2023-2024	**50%**
2022-2023	47%
2021-2022	40%
2020-2021	52%
2019-2020	25%

In 2023-2024, 87% of all complaints under the *Privacy Act*, including investigations into delays by institutions to respond to requests (time-limits investigations), were either closed through early resolution or summary investigations.

The following are examples of complaints that were resolved through the early resolution approach under the *Privacy Act*:

Redirection of request solves problem of missing records

The complainant submitted an access request for the sponsor's file that they submitted to IRCC. The person complained to the OPC after IRCC responded that it did not have any responsive records.

When the OPC followed up, IRCC realized that the complainant's request had not been sent to the appropriate offices within the department. As a result of the OPC's intervention, the complainant's request was re-tasked to the appropriate offices, and the relevant records were provided to the complainant.

Engagement helps department identify the location of documents

A complainant received some records in response to an access request that they had made under the *Privacy Act*, but believed that there should have been more records.

After the OPC's engagement with Public Services and Procurement Canada, department officials re-tasked the request and ultimately provided 149 additional pages of relevant records to the complainant.

Summaries of key *Privacy Act* investigations

Special report: RCMP's Project Wide Awake

In a special report to Parliament that was tabled in February 2024, the Privacy Commissioner released his findings from an investigation into the RCMP's Project Wide Awake. This project involved using third-party service providers to collect personal information from sources that included social media, the dark web, location-based services, and fee-for-access private databases.

The investigation concluded that the RCMP's processes related to assessing private-sector surveillance and monitoring services before acquiring them should be improved.

In the report on Project Wide Awake, the OPC recommended that the RCMP conduct comprehensive assessments to get a sufficient level of assurance that its third-party service providers are compliant with relevant privacy laws. The OPC also recommended that the RCMP be more transparent about its collection of personal information from open-source intelligence gathering, and about the purposes for which the different types of information collected may be used.

FURTHER READING

Investigation of the RCMP's collection of open-source information under Project Wide Awake – Special report to Parliament

IRCC did not conduct a sufficient search for records

The individual complained to the OPC after IRCC provided access to some records but withheld others. This individual, who sought to come to Canada, had asked IRCC for all of its records pertaining to this individual and their children relating to why their visas were cancelled and then reissued. The complainant's representative alleged that IRCC had contravened the *Privacy Act* by failing to disclose all of the relevant information.

The OPC investigation focused on whether IRCC's search for records had been sufficient. The investigation determined that IRCC had conducted an incomplete search because it had reduced the scope of the complainant's request without the complainant's approval and, consequently, had not sought information from all of the offices that might have held relevant records.

After discussing the case with the OPC, IRCC agreed to expand its search; however, it was still unable to find the specific records that were being sought because they had been destroyed in accordance with its two-year retention policy.

As a result, while the OPC found that IRCC initially failed to conduct a sufficient search for records, the OPC was ultimately satisfied that the department had met its obligations under the Act as the records no longer existed.

FURTHER READING

Investigation into IRCC's search for records using modified wording

IRCC authorized to share permanent resident card application with CBSA

An individual contacted the OPC alleging that IRCC had inappropriately shared their application for a renewed permanent residency card with the CBSA, which was then used to revoke their refugee protection.

CBSA was investigating the complainant because the complainant had travelled frequently to the country from which they had sought protection and had obtained a new passport there. In this context, the CBSA requested the permanent residency card renewal application from IRCC, as it included travel details that were relevant to the investigation to cease the refugee protection.

The complainant alleged that IRCC did not have the authority to disclose their personal information to the CBSA, because the purpose of the disclosure was different from the purpose for which the information had been collected.

During the course of the investigation, the OPC established that IRCC and CBSA have a shared mandate under the *Immigration and Refugee Protection Act*. As a result, information sharing between them for the administration and enforcement of the Act is considered a "consistent use" and therefore permissible under the *Privacy Act*.

After reviewing submissions from the complainant and both IRCC and the CBSA, the OPC found that IRCC's disclosure of the complainant's personal information to the CBSA was consistent with the purpose for which the information was collected. The complaints against both departments were deemed not well-founded.

FURTHER READING

Investigation of IRCC's disclosure of personal information to the CBSA

DND correctly denied executor access to deceased's personal information

The OPC investigated a complaint regarding the fact that DND had declined to release a deceased member's personal information to the executor of their estate.

Through a representative, the executor asked DND for records pertaining to an investigation into allegations against the deceased, as well as records of any actions that were taken by the deceased's chain of command in response to the allegations.

The military eventually released some of the information requested but withheld other information.

The OPC investigation focused on whether the representative was entitled to make a request under the *Privacy Act* on behalf of the executor for the purposes of administering the estate and therefore to access the requested information. The Act allows individuals to request information about them held by a federal institution. A person who is authorized to administer the estate of a deceased individual may only "step into the shoes" of that individual and gain access to their personal information for the purposes of administering the estate.

In their submissions to DND, the representative explained that the complainant, the estate's executor, was seeking the information for two purposes. First, they were planning to bring a complaint on behalf of the estate regarding the allegations against the deceased. Second, the complainant wanted to inform themselves ahead of a Board of Inquiry into the soldier's death.

The OPC determined that there was insufficient evidence to establish that the information that was requested was necessary to administer the estate, and that therefore, DND was correct in finding that neither the representative on behalf of the executor nor the executor themselves had the right to access it.

FURTHER READING

Investigation of the Department of National Defence's refusal to disclose personal information of a deceased individual

Privacy Act breaches

Top institutions by breaches reported	
Institution	**Breaches reported**
Employment and Social Development Canada	377
Canada Revenue Agency	71
Correctional Service Canada	20
Royal Canadian Mounted Police	14
Immigration, Refugees and Citizenship Canada	8
Public Service Commission of Canada	8

In 2023-2024, breach reports to the OPC that were related to federal government institutions rose by 88%, to 561, compared to 298 in the previous year.

Some are the subject of ongoing investigations, including one involving a breach at GAC, and another involving a third-party that provides relocation services to government employees, which affected multiple federal government departments. The latter breach also involves ongoing investigations under PIPEDA into two companies that were contracted by the government as part of the relocation program.

In February 2024, the Privacy Commissioner tabled a special report to Parliament into a cyber incident at the CRA and ESDC that resulted from insufficient cybersecurity safeguards. These attacks compromised the sensitive financial, banking, and employment data of tens of thousands of Canadians, leading to numerous cases of fraud and identity theft – including many fraudulent applications for the Canada Emergency Response Benefit (CERB).

Over the years, the OPC has raised concerns with respect to underreporting of breaches in the federal public sector. In that respect, the increase in breach reports received is a positive sign.

In particular, the OPC received a higher number of reports (377) from ESDC. The volume of breaches that were identified by ESDC may be reflective of the privacy breach detection efforts of the department as well as other factors, such as their mandate, which involves the collection and use of significant amounts of personal information.

Despite the increased total number of reports, and the high-profile nature of some of these incidents, the OPC remains concerned that, too often, breaches are going undetected or are being mis-assessed, leading to under-reporting of privacy breaches in the public sector.

While numerous federal institutions handle sensitive personal information as part of their mandates, the OPC does not receive a large number of breach reports from these organizations. In the public sector, federal institutions that are subject to the *Privacy Act* are required to report breaches under a TBS policy rather than by law, as opposed to what is the case for the private sector under PIPEDA.

For the total 561 incidents reported, the primary cause was the loss of personal information (382 incidents; or 68% of the total), followed by the unauthorized access of personal information (89 incidents; 16%). Unauthorized disclosure was a factor in 85 reported breaches (15%), with the majority of those cases caused by employee errors.

The OPC also continues to see an important gap between the public and private sectors when it comes to the reporting of cyber incidents. In 2023-2024, the OPC received 321 reports of cyber incidents from the private sector, and only 37 from federal institutions.

Due to the technically complex nature of the breaches reported, the OPC has been increasingly dedicating efforts to technical analysis to determine what factors led to a particular breach, as well as to confirm the appropriateness of technical mitigation measures that may have been taken by the institutions involved.

While not within its jurisdiction, the OPC also noted an increase in breaches that are affecting critical public service infrastructure, such as in municipal governments and school boards. This is another indicator that government institutions are increasingly targeted by threat actors.

Privacy Act breach-related investigations

Special report to Parliament: ESDC and CRA breach

In February 2024, the Privacy Commissioner released his findings in a special report to Parliament into a major privacy breach at ESDC and CRA involving vast amounts of sensitive personal information. In this investigation, the OPC found that attackers used stolen credentials to access the CRA's sign-in portal and ESDC's "GCKey" authentication service. This technique, known as credential stuffing, allowed the bad actors to access, modify, and create new online accounts for these stolen identities. As a result, they were able to fraudulently access government services and apply for benefits and/or redirect payments to themselves.

The attack compromised the sensitive financial, banking, and employment data of tens of thousands of Canadians, leading to numerous cases of fraud and identity theft – including a high volume of fraudulent applications for the CERB. Negative impacts on individuals ranged from financial hardship to damaged credit scores, invasion of privacy, and emotional distress.

The OPC found that both the CRA and ESDC had under-assessed the level of identity authentication that was warranted for the online services that were affected by the breach, especially given the sensitivity of personal information that was involved. In addition, the organizations had not taken the necessary steps to promptly detect and contain the breach, due in part to inadequate security assessments and testing of their authentication and credential management systems, and limited accountability and information-sharing between departments.

The OPC made a number of recommendations and the departments accepted all of them.

FURTHER READING

Investigation of unauthorized disclosures and modifications of personal information held by CRA and ESDC resulting from cyberattacks – Special report to Parliament

Breach at IRCC reinforces importance of procedures to protect personal information

A human error in the use of an Excel spreadsheet resulted in an email, that was meant for someone else, to be mistakenly sent to nearly 500 people who were seeking permanent residence.

IRCC was preparing a mass mailing to notify eligible individuals of a special measure that allowed them to remain in Canada on a work permit, while the department finalized the processing of their permanent resident applications. The misdirected emails contained names, addresses, and email addresses, and also revealed that all email recipients held open work permits and had applied for permanent residency.

The OPC determined that this was not a material breach as there was a low risk of harm to those affected.

To avoid another incident of this nature, which in a different context could carry a real risk of significant harm, the OPC recommended that IRCC create a step-by-step job aid for its employees and train them on its use, put in place oversight measures and check regularly to ensure that these measures are followed. The OPC has since confirmed that IRCC implemented these recommendations.

FURTHER READING

Investigation into a privacy breach at IRCC

CRA breach demonstrates the importance of proper authentication processes

In 2023, the OPC received a complaint from an individual whose information had been used by an imposter to apply for, and receive, the CERB.

The complainant's MyAccount at the CRA was compromised in a breach that occurred in 2020. As a result, a bad actor was able to access the complainant's account both online and by phone communication with the CRA, change direct deposit information and contact details associated with the account, and apply for the CERB.

Having had access to this information, the fraudster was also able to subsequently apply for and receive Employment Insurance benefits from ESDC. Because of this, the complainant's 2021 income taxes were reassessed, and they were told that they owed a substantial amount.

In this case, the investigation found that weak security measures, a lack of risk-mitigation measures in regard to high-impact data like direct deposit information, and concerns related to identity and credential authentication, were contributing factors that led to the breach. In the investigation report, the OPC also noted that safeguards used to protect against unauthorized access and modification should be commensurate with the sensitivity of the information that an organization holds.

Following the incident, the CRA implemented changes, including strengthening its procedures for confirming requests received, including those received via telephone, and adding security measures for high impact modifications to personal information.

FURTHER READING

Investigation into the steps that the CRA took to ensure the accuracy of a taxpayer's personal information that it used to make an administrative decision about them

Investigation of unauthorized disclosures and modifications of personal information held by the CRA and ESDC resulting from cyberattacks – Special report to Parliament

Confusion between employees with the same name results in systemic privacy breaches

In this investigation, the OPC determined that a federal government department had contravened the *Privacy Act* by failing to take sufficient measures to avoid privacy breaches related to employees with the same name.

An employee complained that their personal information had been accidentally shared several times with the other employee of the same name, despite numerous complaints to the relevant sectors inside their department that had sent the information.

The employee also noted that changes in human resources and information technology systems were often made to the wrong employee account, despite the fact that the two do not share the same birthdate and have different government-issued personal record identifiers.

While the department argued that the sensitivity of the information disclosed was "low-to-medium," the OPC disagreed, noting that the type of information that was shared, such as home and personal email addresses, as well as financial and health information, could have led to identity theft in other contexts.

While most of the incidents that occurred were the result of human error, the fact that these errors were repeated, and continued to be made despite the employee's complaints, was determined to be evidence of a systemic problem that could have been addressed, for example by putting measures into place to confirm each employee's identity before sending an email containing personal information or changing a personnel file.

The department initially stated that it was unaware of the incidents because they had not been reported to its Access to Information and Privacy (ATIP) Office. In the report, the OPC noted that the fact that none of these breaches had been reported to that office by the complainant or any other employee who knew of the problem indicates a general lack of knowledge of the breach-reporting procedure and the role and responsibilities of the departmental ATIP office.

Following the issuance of the OPC report, the department committed to implementing the recommendations, including

taking measures to prevent unauthorized disclosure of these employees' personal information going forward, and to raise all employees' awareness about their responsibility to report breaches of personal information to the ATIP office.

FURTHER READING

Investigation into the treatment by a government institution of the personal information of two employees with the same name

Active investigations

The Privacy Commissioner launched several investigations in 2023-2024 related to major breaches and high-profile activities. The investigations remain ongoing.

ArriveCAN app and contracting practices

Commissioner Dufresne announced in March 2024 that the OPC will investigate allegations of non-compliance with privacy requirements following a complaint against the CBSA related to the development of the ArriveCAN mobile app.

The investigation will examine contracting practices related to ArriveCAN, and more specifically the measures that were in place to protect personal information during the development of the app, to assess compliance with the *Privacy Act*.

Breach involving government-contracted relocation services

Commissioner Dufresne launched two investigations into a cyberattack that resulted in a breach affecting the personal information of federal government personnel who used government-contracted relocation services over two decades.

The breach involves personal information that was held by BGRS and its affiliated company (Sirva), which are contracted by the Government of Canada to provide relocation services for employees.

The investigation is assessing whether the two government departments that contracted with the companies, Public Services and Procurement Canada and TBS, complied with the *Privacy Act*. A second investigation is examining the two companies' compliance with PIPEDA.

Data breach at GAC

The Commissioner opened an investigation into a data breach at GAC where the personal information of users, including employees, was compromised after unauthorized individuals accessed the department's virtual private network.

The OPC received several complaints about the matter. The investigation is examining the adequacy of the safeguards that are in place to protect personal information and assessing compliance with the *Privacy Act*.

Compliance monitoring unit activities

As part of its investigations, the OPC makes recommendations to help bring institutions into compliance with the *Privacy Act*. In some cases, the OPC will use its compliance monitoring function to ensure that institutions are implementing the recommendations that they have committed to, within the timelines set. Unlike PIPEDA, the *Privacy Act* does not include a provision to enter into a compliance agreement.

In 2023-2024, in addition to 15 monitoring files that were closed under PIPEDA, 23 monitoring files were concluded under the *Privacy Act*, including the following two:

Internal disclosure of personal information at CSPS

In July 2023, an OPC investigation into a complaint against the Canada School of Public Service (CSPS) found that the complainant's access request was improperly disclosed by the CSPS ATIP group to the CSPS security team.

Following the investigation, the OPC recommended that, within nine months, the CSPS:

- Develop guidance that includes a clear process by which its officials assess the merit of proposed consistent use disclosures of personal information internally; and
- Create and offer training to all ATIP employees to remind them of their obligations under both the *Access to Information Act* and the *Privacy Act*, and related policies.

The CSPS implemented the measures within the specified time frame. After reviewing the steps that the CSPS had taken, the OPC was satisfied that the specific concerns raised in the complaint had been resolved.

CSC disclosure of personal information

In August 2023, an OPC investigation into the CSC found that it had improperly disclosed a complainant's personal information. The complainant's name was included in a letter pertaining to a personal human resources matter that was issued in error to another employee. The other employee was therefore able to see that information about the employee whose information was wrongly disclosed.

In its investigation, the OPC found that CSC had not adequately implemented previous recommendations that were made in a 2021 investigation related to CSC's collection, use, and disclosure of a complainant's information.

Following the August 2023 investigation, the OPC recommended that CSC develop guidance for its employees regarding privacy breaches, and also provide training.

This most recent investigation found that CSC had implemented the OPC's recommendations within the specified time frame. The OPC was satisfied that the specific concerns raised in the complaint had now been resolved.

Update: Canada Post's Smartmail Marketing program

In May 2023, an OPC investigation into Canada Post's Smartmail Marketing Program concluded that Canada Post used personal information, leveraged from its operational data for marketing purposes, without obtaining the required authorization from individuals. Under the program, Canada Post built marketing lists from various sources, including the information gleaned from envelopes and packages that it delivered to homes across Canada.

The OPC recommended that Canada Post stop using and disclosing personal information that is taken from its mail operation for marketing activities until it has sought and obtained Canadians' authorization.

Following the investigation, Canada Post implemented some transparency-related measures for this program, such as updating its online information about the program and adding brochures at retail outlets. Since then, it has also announced that it will:

- no longer offer aggregated online shopping trend information at the postal code level to retailers;
- stop using data from publicly available telephone directories combined with its operational data to validate incomplete addresses; and
- work to increase transparency and awareness of its Smartmail Marketing Program, including how individuals may opt out of receiving advertising mail.

In addition, Canada Post has shared with the OPC information regarding the Smartmail Marketing Program going forward, including initiatives being undertaken by Canada Post to increase transparency in its data protection and privacy practices.

The OPC reviewed the measures proposed by Canada Post, and specifically its plan to discontinue using data from publicly available telephone directories combined with its operational data to validate incomplete addresses.

The OPC is satisfied that this measure addresses the specific concerns that were raised in the complaint.

Canada Post's commitment to improve its privacy posture should ensure greater accountability for the protection of Canadians' privacy rights.

FURTHER READING

Investigation of the Canada Post Corporation's collection and use of personal information for the Smartmail Marketing Program

PIPEDA:
A year in review

The influence and impact of technology on privacy was a key theme of the OPC's work under PIPEDA in 2023-2024.

Prominent over the past year was the release of a report by the Privacy Commissioner on the findings of an investigation into Aylo, the operator behind Pornhub and other popular pornographic sites. The OPC investigation found that Aylo contravened Canadian privacy law by enabling intimate images to be shared on its websites without the direct knowledge or consent of everyone depicted.

The investigation uncovered significant consent-related failings that allowed this to happen, resulting in severe impacts on victims, such as social stigmatization, psychological damage, financial loss, and even attempted suicide.

Consent is also a central question in ongoing investigations into TikTok and OpenAI. These investigations, which are currently being carried out jointly with the OPC's counterparts in Quebec, British Columbia, and Alberta, seek to determine, among other things, whether these two companies obtain valid consent for their collection, use, and disclosure of personal information. In the case of TikTok, our examination is considering, in particular, the large proportion of younger users on the platform.

Given the rise in threats and the level of severity of cyberbreaches globally in recent years, technology is a key consideration in the OPC's investigations. The OPC has observed that, while there has been only a slight increase in the number of reported incidents, more individual accounts are being affected, and critical infrastructure is increasingly being targeted via mass cyberattacks.

Privacy protection and innovation are complementary. Organizations that take the privacy of their customers seriously and put in place measures to properly protect their personal information are able to engender trust and foster growth. To support them in building strong privacy practices, the OPC has a Business Advisory team of dedicated experts to help businesses better understand their obligations under the law.

The following section highlights key outcomes under PIPEDA in 2023-2024.

Privacy by the numbers

PIPEDA

Complaints accepted	446
Well-founded complaints	16
Complaints closed through early resolution	363
Complaints closed through standard investigation	42
Data breach reports received	693
Advisory engagements with private-sector organizations	16

PIPEDA compliance actions

In 2023-2024, the OPC accepted 446 complaints under PIPEDA, with the largest proportion of complaints being lodged against businesses in the financial sector (112, or 25% of all PIPEDA accepted complaints) and the online/digital services sector (72, or 16% of all accepted complaints). The latter category includes Internet and computing service providers, as well as companies offering other online services such as news, software and mobile apps, directories, search portals and social media platforms.

In all complaints received, regardless of the sector of activity, matters that were raised included the collection and use of credit information without consent, challenges in obtaining access to personal information, the amount of time taken by businesses to resolve privacy complaints, procedures around retention, and deletion of personal information, and extensive use of personal information.

The OPC has also seen an increase in the number of complaints that are submitted by residential tenants regarding the privacy practices of their landlords. These included complaints related to issues such as video surveillance outside their rental units and online services that are used by landlords to select prospective tenants.

As noted earlier, at the end of March 2024, 20% (152) of all ongoing OPC investigations under the *Privacy Act* or PIPEDA were older than 12 months. While the risk of a growing backlog persists, the OPC continues to implement measures and to look for creative and innovative ways to further improve efficiencies.

Early resolution

As noted earlier in this report, the OPC attempts to resolve low-complexity, non-systemic complaints quickly and efficiently, where possible, using negotiation or engagement techniques, which generally provide the best outcome for the parties involved. In these cases, the OPC does not issue a formal finding.

Percentage of all complaints closed in early resolution	
Fiscal Year	**Percentage of complaints**
2023-2024	90%
2022-2023	73%
2021-2022	85%
2020-2021	71%
2019-2020	69%

Here is an example of a case under PIPEDA:

Building surveillance recorded audio without consent

The individual filed a complaint with the OPC after suspecting that their building's surveillance cameras were recording both video and audio. The property management company had notified tenants about the video surveillance but had not informed them that audio recording would also be enabled.

As a result of the OPC's intervention, the company disabled the audio recording function.

PIPEDA investigations

Investigation finds Pornhub operator failed to obtain meaningful consent for user-generated content

An investigation into Aylo, one of the world's largest operators of pornographic sites, found that the company contravened PIPEDA by enabling intimate images to be shared on its websites without the direct knowledge or consent of everyone depicted.

The investigation was in response to a complaint from an individual who discovered that her former partner had uploaded an intimate video and images, along with other identifying information, to various Aylo websites.

Aylo initially took steps to remove the content at the complainant's request, but the company's privacy protections did not prevent the video from being uploaded again and again on its websites, where it could be downloaded and reposted by website users. Ultimately, over 700 instances of the images were found across more than 80 websites on the Internet.

The individual said that the permanent loss of control over her intimate images led her to withdraw socially, lose a job opportunity, and live in a state of constant fear of being recognized from images available online.

The investigation determined that in many instances, Aylo relied on uploaders to confirm that each individual who appeared in video and image content had provided consent for its upload, despite the company's own evidence that this method was inadequate. The investigation also established that when individuals who had not provided consent for content to be uploaded asked Aylo to take it down, they had to contend with an extremely onerous and ineffective process.

The Privacy Commissioner made several recommendations that are aimed at bringing Aylo into compliance with the law, including a recommendation for Aylo to adopt measures for obtaining valid consent directly from everyone depicted in images and videos that are posted on its websites, delete all content for which such consent was not obtained, and simplify its takedown process.

While Aylo did make changes to its consent practices in recent years that are aimed at improving these issues, it did not provide the OPC with evidence that it had resolved the contraventions identified in the investigation.

The investigation report was initially scheduled for release in May 2023, but was delayed when Aylo launched legal proceedings that prevented the Privacy Commissioner from releasing the report until the Federal Court of Appeal dismissed the proceedings on February 29, 2024.

FURTHER READING

Investigation into Aylo's compliance with PIPEDA

Statement by the Privacy Commissioner of Canada following an investigation into Pornhub operator Aylo

Active investigations

The Privacy Commissioner also had several high-profile investigations into the information-handling practices of businesses in 2023-2024, which remained ongoing at the time of writing.

OpenAI

The Privacy Commissioner, along with his counterparts in Quebec, British Columbia, and Alberta, is investigating the privacy practices of OpenAI.

Commissioner Dufresne launched an investigation following a complaint alleging that personal information was being collected, used, and disclosed without consent. Given the broad scope and significant privacy impact of AI and its relevance to all Canadians, the four offices decided to jointly investigate the matter.

The investigation will seek to establish whether OpenAI:

- obtained valid and meaningful consent for the collection, use, and disclosure of the personal information of individuals based in Canada via ChatGPT;
- respected its obligations with respect to openness and transparency, access, accuracy, and accountability; and
- collected, used and/or disclosed personal information for purposes that a reasonable person would consider appropriate, reasonable or legitimate in the circumstances, and whether this collection is limited to information that is necessary for these purposes.

TikTok

The Privacy Commissioner, along with his counterparts in Quebec, British Columbia, and Alberta is also investigating the privacy practices of TikTok.

The four privacy regulators are examining whether the organization's practices comply with Canadian federal and provincial privacy legislation and, in particular, whether valid and meaningful consent is being obtained for the collection, use, and disclosure of personal information. The investigation will also examine whether the company is meeting its transparency obligations, particularly when collecting personal information from its users.

Given the importance of protecting children's privacy, the joint investigation has a particular focus on TikTok's privacy practices as they relate to younger users.

Google de-listing

The OPC is proceeding with an investigation into a complaint from an individual who alleged that Google was contravening privacy law by returning links to online news articles about the complainant when their name was searched. The individual alleged that the articles were outdated, inaccurate, and disclosed sensitive information about them and that this caused them significant harm.

The investigation was put on hold while the OPC sought clarification from the Federal Court on whether Google's search engine is subject to federal privacy law when it indexes web pages and presents search results in response to queries of a person's name. In September 2023, the Federal Court of Appeal confirmed the OPC's position that Google's search engine service is subject to PIPEDA. The investigation has now been reopened and should be completed in the coming months.

PIPEDA breaches

The OPC has noted an increase in both the scale and complexity of breaches, as well as the increasingly sophisticated nature of threat actors, including state-sanctioned ones and those emanating from organized crime.

There have also been more breaches affecting companies that oversee critical infrastructure, such as financial and telecommunications companies, with the latter representing respectively 25% and 17% of the breach reports received.

Another sector that was targeted more frequently in 2023-2024 was third-party service providers, particularly IT and software providers. The impact of such breaches can be widespread. For example, a breach involving a data processor has the potential to impact many more individuals, as it could affect the clients of multiple companies, sometimes even hundreds of companies.

However, under PIPEDA, data processors are not required to report a privacy breach – that responsibility rests with the companies that use the services of the data processor. As such, the full impact of the breach can be difficult to ascertain if the processors do not provide a breach report along with the individual companies that they service.

Also of note in 2023-2024, twice as many individuals were affected by breaches compared to the previous year, but for a similar number of reported incidents. In 2023-2024, private-sector organizations reported 693 breaches to the OPC, affecting approximately 25 million Canadian accounts, compared with 681 breaches the previous year, affecting approximately 12 million accounts.

The number of reported cyberattacks resulting in privacy breaches increased by 13%. In 2023-2024, 321 (46%) of all breaches that were reported to the OPC were identified as cyber incidents, while 278 cyberattacks were reported in 2022-2023.

The OPC believes that many breaches go unreported, even undetected, particularly by small and medium-sized enterprises (SMEs). While SMEs represent nearly 90% of businesses in Canada, they report nearly the same volume of

Top sectors by percentage of total breaches reported

Industry sector	2020-2021	2021-2022	2022-2023	2023-2024
Financial	22%	20%	27%	**25%**
Telecommunications	14%	14%	17%	**17%**
Professional services	8%	12%	14%	**10%**
Services	6%	5%	4%	**8%**
Sales and retail	10%	8%	9%	**7%**
Manufacturing	6%	8%	4%	**7%**

Percentage of breaches reported by type

Breach type	2020-2021	2021-2022	2022-2023	2023-2024
Unauthorized access	64%	65%	66%	**75%**
Unauthorized disclosure	28%	25%	25%	**18%**
Theft	5%	3%	4%	**3%**
Loss	3%	7%	4%	**3%**

breaches as larger organizations such as telecommunications or communication service providers, banks, insurance and entertainment companies.

OPC's real risk of significant harm tool update

Real risk of significant harm, or RROSH, is the legal threshold for reporting a breach under PIPEDA. However, determining whether a breach meets that threshold can sometimes be difficult.

To assist organizations in establishing that threshold and guide these risk assessments, the OPC developed a tool that it plans to launch in 2024-2025. The RROSH tool takes users through a series of questions to help identify the potential harms to affected individuals and determine whether an incident creates a real risk of significant harm.

Factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm include the sensitivity of the personal information that is involved in the breach, and the probability that the personal information has been, is or will be misused.

Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property.

Organizations that are unsure whether a breach meets the threshold for reporting are encouraged to contact the OPC for advice.

Assessment of safeguards and real risk of significant harm in Brinks Home breach

A Brinks Home customer notified the company that in their own online account they had access to the personal information of other security system clients. Noting that they still had access 10 weeks later, the individual informed the company a second time and filed a complaint with the OPC.

Shortly after the second notification, Brinks Home resolved the unauthorized access issue, which it found was the result of an employee error. As a result, the personal information of 3,340 Brinks Home clients had been accessible to 102 other customers for at least several months.

The OPC investigation found that Brinks Home did not adequately protect customers' personal information from unauthorized access. Following the breach, the company implemented various measures to prevent a similar incident from occurring in the future, including updating its customer registration process and improving customer service training.

The investigation also considered whether Brinks Home had complied with its breach notification requirements. While the OPC investigation concluded that the personal information involved could be considered sensitive, the probability of its misuse in the specific circumstances was deemed low since this was not a case of hacking by malicious actors. The investigation confirmed that no more than 20 Brinks Home customers (those who had logged into their portals during the relevant period) could have accessed other customers' data without authorization.

As a result, it was determined that, in the circumstances, the incident did not pose a real risk of significant harm, which is the threshold for reporting a breach. Brinks Home would therefore not have been required to report the incident to the OPC or to notify affected individuals of the breach.

FURTHER READING

Investigation into Monitronics International, Inc. (Brinks Home) compliance with PIPEDA

Compliance monitoring unit activities

When private-sector organizations agree to enter into a compliance agreement with the OPC or to implement recommendations following an investigation, the OPC follows up to ensure that the appropriate steps have been taken to meet these commitments.

In 2023-2024, in addition to 23 files closed under the *Privacy Act*, the compliance monitoring unit closed 15 follow-up files under PIPEDA, including the following two matters:

Tim Hortons implements OPC recommendations

In 2022, a joint investigation by the OPC and its counterparts in Quebec, British Columbia, and Alberta found that Tim Hortons' mobile app had continuously tracked and recorded app users' movements every minute of every day even when the app was not open. The company used that information to infer where users lived, where they worked, and whether they were travelling. The app also generated an "event" every time users entered or left a Tim Hortons competitor, a major sports venue, or their home or workplace.

The four privacy authorities made several recommendations, including that Tim Hortons delete any location data and also direct third-party service providers to do the same. They also recommended that the company establish an app-related privacy management program to ensure compliance with Canadian privacy laws in future.

Tim Hortons implemented the measures within the specified time. Following a review in 2023 that included provincial counterparts, the OPC was satisfied with the steps that Tim Hortons had taken and concluded that the specific concerns that were raised in the complaint had been resolved.

FURTHER READING

Joint investigation into location tracking by the Tim Hortons App

Marriott International implements OPC recommendations

by Marriott International Inc. found that the hotel chain had insufficient safeguards when the breach occurred. Following the incident, Marriott made several enhancements to its security safeguards.

The OPC recommended that Marriott engage an external assessor to evaluate the enhancements that it had made to its safeguards and conduct regular reviews of its privacy practices to prevent a similar breach from reoccurring on its systems.

Marriott implemented the recommendations and, after reviewing the steps taken, the OPC was satisfied that the specific concerns identified by the investigation had been resolved.

FURTHER READING

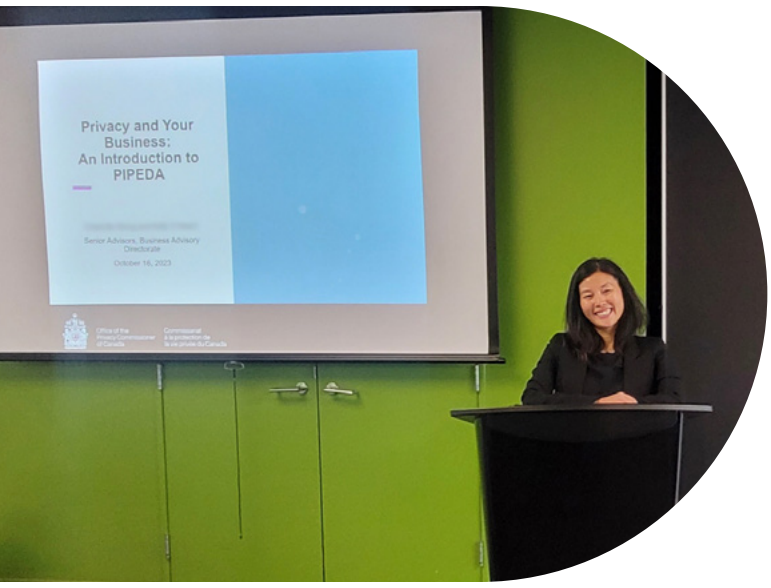
Hotel chain discovers breach of customer database following acquisition of a competitor

PIPEDA advice and outreach to businesses

The OPC provides advice to organizations for making sure that their initiatives and practices for managing personal information comply with PIPEDA.

This work by the OPC's Business Advisory Directorate has supported innovative organizations from a broad spectrum of industries such as health, education, finance, retail, marketing, services, automotive, human resources, technology, analytics, and others.

The adoption of advanced technologies, such as AI and facial recognition technology, continues to accelerate. The OPC has provided advice to businesses that are considering and adopting increasingly complex data-processing models, structures, and practices, as well as on initiatives that involve the application of cutting-edge data technologies to address potential fraud and crime.



A member of OPC's Business Advisory Directorate delivers a presentation on PIPEDA in Halifax, Nova Scotia.

OPC business outreach initiatives

In addition to its other promotional activities, in 2023-2024 the OPC travelled to Nova Scotia, New Brunswick, and Yukon to conduct in-person privacy clinics and PIPEDA compliance information sessions for businesses in these regions.

In the fall of 2023, the team visited Atlantic Canada, where they delivered a presentation on PIPEDA principles and best practices and offered privacy clinics to local businesses in Halifax. In New Brunswick, the team's presentation and discussion panel on PIPEDA and Data Privacy at Moncton's Venn Innovation as part of the Techtoberfest event drew the largest number of attendees at one of their speaking engagements.

In February, the team travelled to Canada's North to interact with and inform businesses about compliance with the federal private-sector privacy law and promote the services that are offered by the OPC's Business Advisory Directorate. These engagement and outreach activities helped the OPC to build and strengthen relationships with key stakeholders and businesses in the region and gain deeper insights into the needs and challenges of the business community.

The team also held privacy clinics and stakeholder meetings, including a presentation on PIPEDA for the Canadian Northern Economic Development Agency. They exhibited at an event hosted by Yukon Government's Department of Economic Development that was attended by more than 250 people. They connected with entrepreneurs and startups from the business community, as well as industry associations, including Tech Yukon, Yukonstruct, Yukon University and other stakeholders in the technology, hospitality, and tourism fields.

Businesspeople asked about their obligations under PIPEDA and discussed various specific compliance areas, such as privacy obligations of business that are using cloud storage, and computing facilities and functions.

The OPC's Technology Analysis Directorate

As technologies continue to evolve and become increasingly complex, it is important to have technological experts to support the work of the OPC in this area.

The OPC's Technology Analysis Directorate is playing an increasingly important role in investigative work, for example, by supporting investigations into online platforms such as TikTok and OpenAI. By providing expert analysis and guidance on privacy concerns in digital environments, the Directorate deepens the OPC's understanding of technological factors in these and other investigations, which helps the OPC to recommend appropriate solutions. The Directorate also provides expert technological analysis in support of the OPC's Government and Business Advisory services.

The OPC's technologists also conduct research in its technology lab, for example, on issues related to smart home devices and advances in AI, including large language models and generative AI.

As well, OPC technologists collaborate with international partners such as the International Working Group on Data Protection in Technology, also known as the Berlin Group, to lay the groundwork for future technology assessments. Analysts also periodically write blog posts for the OPC's website on topics such as post-quantum cryptography and homomorphic encryption, which are aimed at improving public and professional understanding of privacy and technology issues.

FURTHER READING

Privacy Tech-Know blog posts

Public opinion research snapshot

Survey of Canadian businesses on privacy-related issues

The OPC commissions a survey of Canadian businesses every two years to better understand awareness and approaches to privacy protection within Canada's private sector. The survey findings help the OPC provide guidance to both individuals and organizations on privacy issues, and to enhance outreach efforts with businesses.

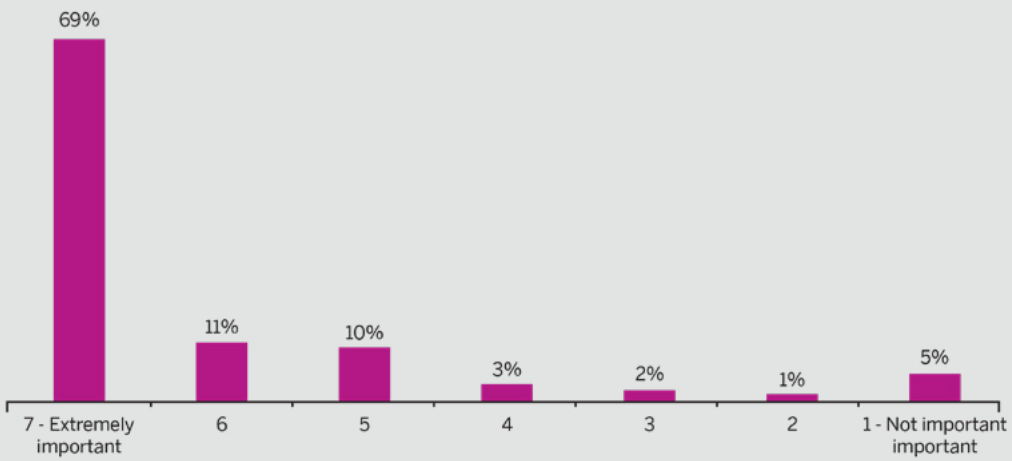
The 2023-2024 survey found that:

- 80% of businesses consider the protection of customers' personal information to be of high or extremely high importance; 14% said privacy is moderately important.
- Most companies are aware of their responsibilities under Canada's privacy laws (88% at least moderately aware) and have taken steps to ensure that they comply with these laws (76%).
- Actions that businesses report taking to manage their privacy obligations include:
  - designating a privacy officer (56%)
  - having procedures to deal with complaints (53%)
  - having internal privacy policies (50%)
  - having procedures to deal with access requests (50%)
  - providing staff with privacy training (33%)

FURTHER READING

2023-2024 Survey of Canadian businesses on privacy-related issues

Importance attributed to protecting customers' personal information



Highlights of other OPC work

Privacy by the numbers

Other work

Bills, parliamentary studies and draft regulations reviewed for privacy implications	38
Parliamentary committee appearances on privacy matters	10
Information requests	2,548
News releases and announcements	58
Speeches and presentations	64
Posts on X (Twitter)	838
X (Twitter) followers	20,170
Posts on LinkedIn	501
Followers on LinkedIn	33,207
Visits to website	3,147,433
Blog visits	68,047
Publications distributed	11,366

Along with its work overseeing compliance with the *Privacy Act* and PIPEDA, the OPC actively pursues its mandate to protect and promote privacy rights. For example, it does so by providing advice to Parliament, collaborating with national and international partners, and by promoting privacy-related research.

The following section provides an overview of the OPC's activities in these areas in 2023-2024.

Advice to Parliament

An important part of the OPC's role is to offer advice to Parliament on privacy-related legislation and other matters. The Office made five submissions to Parliament and the government, and the Commissioner appeared before House and Senate committees 10 times in 2023-2024, including:

Appearance on proposed changes to Elections Act governing personal information collected by political parties

Commissioner Dufresne appeared before the Standing Senate Committee on Legal and Constitutional Affairs to discuss proposed amendments to the *Canada Elections Act* contained in Bill C-47, the *Budget Implementation Act*, that would authorize political parties and their affiliates to collect, use, disclose, retain, and dispose of personal information (in accordance with a party's own written privacy policy).

The Commissioner said that political parties should be subject to privacy requirements that are grounded in legislation and based on internationally recognized privacy principles.

He added that, given the importance of privacy and the sensitive nature of the information being collected, Canadians need and deserve a privacy regime for political parties that goes further than self-regulation and that provides meaningful standards and independent oversight to protect and promote electors' fundamental right to privacy.

Appearances on Bill C-27 – the Digital Charter Implementation Act, 2022

In May 2023, Commissioner Dufresne presented his submission on Bill C-27, a bill to modernize the federal private-sector privacy law. The Commissioner later appeared twice before the Standing Committee on Industry and Technology (INDU) in the fall to discuss his 15 key recommendations for strengthening the bill.

In his September 2023 appearance, Commissioner Dufresne discussed the OPC's recommendations to strengthen the bill, including explicitly recognizing privacy as a fundamental right, stronger protection of children's privacy rights and the best interests of the child, and requiring organizations to conduct PIAs for high-risk activities, including AI.

In his October 2023 appearance, Commissioner Dufresne welcomed statements from the Minister of Innovation, Science and Industry on potential amendments to the Bill which would align with some of the OPC's key recommendations.

Appearance on Bill S-231 – Increasing the Identification of Criminals Through the Use of DNA Act

OPC officials appeared before the Standing Senate Committee on Legal and Constitutional Affairs to discuss Bill S-231, which would expand the circumstances under which DNA samples may be taken from offenders, and retained and used to solve other crimes. It would also allow for familial searching, which involves police using DNA samples to identify near or partial matches in DNA datasets.

The Senate Committee was sensitive to concerns raised by the OPC and others with the familial search provisions that the bill proposed, and these were removed in the course of the Committee's study.

Appearance before Parliamentary committee on its study of data harvesting by social media platforms

Commissioner Dufresne was invited to provide input to the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on its study of the Use of Social Media Platforms for Data Harvesting and Unethical or Illicit Sharing of Personal Information with Foreign Entities.

The Commissioner recommended that a modernized federal privacy law recognize that the processing of personal information should respect children's privacy and take into account the best interests of the child. This would encourage organizations to build privacy for children into their products and services by design and by default.

FURTHER READING

ETHI Appearance on Social Media and Foreign Entities: Additional questions and answers

Appearance before Parliamentary committee on federal government's use of digital forensics tools

Commissioner Dufresne appeared before ETHI to take part in its study on the government's use of tools that can extract data from mobile devices and computers.

Commissioner Dufresne stated that it continues to be important that government institutions carefully consider and assess the privacy implications of their activities. The Commissioner also reiterated his recommendation that the preparation of PIAs be made a formal legal obligation under the *Privacy Act*.

Appearance before Parliamentary committee on its study of Bill C-26

Commissioner Dufresne appeared before the Standing Committee on Public Safety and National Security (SECU) to assist the Committee in its study of Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*.

The Commissioner noted that digital services are central to the ways that we live, work, and interact, and it is therefore critical to protect Canada's cyber infrastructure from potential threats.

He indicated that he strongly supports the objectives of Bill C-26, and shared recommendations for strengthening the Bill in order to achieve those objectives while also protecting the fundamental right to privacy and addressing potential privacy implications.

Appearance before Senate Standing Committee on Indigenous Peoples

Commissioner Dufresne appeared before the Senate Standing Committee on Indigenous Peoples (APPA), to speak to its examination of the federal government's constitutional, treaty, political and legal responsibilities to First Nations, Inuit and Métis peoples and any other subject concerning Indigenous Peoples.

In his remarks, Commissioner Dufresne discussed the circumstances under which federal institutions can share information under the provisions of the *Privacy Act*. He stated that issues affecting Indigenous peoples will need to be carefully considered when the federal government moves forward with much-needed modernization of public sector privacy legislation.

Submission to government

Consultation on strengthening Canada's anti-money laundering and anti-terrorist financing regime

In August, the OPC made a submission in response to Finance Canada's Consultation Paper examining ways to strengthen Canada's Anti-Money Laundering/Anti-Terrorist Financing (AML/ATF) regime. The OPC has had a long-standing interest in, and engagement with, Canada's AML/ATF regime, appearing in Parliament and participating in previous consultations on the issue.

The OPC has long taken the position that the AML/ATF regime must be effective at fighting financial crimes and be underpinned by strong accountability measures, taking into account the principles of necessity and proportionality,

Photos: Commissioner Dufresne at the 59th Asia Pacific Privacy Authorities (APPA) forum; Commissioner welcomes attendees to OPC International Symposium on Privacy and Generative AI; and photos of Symposium panelists and participants.

International and domestic cooperation

The importance of the OPC's domestic and international partnerships with data protection authorities and other regulators became increasingly evident in 2023-2024, as generative AI topped the list of rapidly emerging technologies calling for a coordinated response.

A highlight of the year, showcasing the OPC's work in both the domestic and international arenas, was the International Symposium on Privacy and Generative AI, which Commissioner Dufresne hosted in Ottawa in December 2023. At the symposium, he launched Principles for the responsible development and use of generative AI that were developed in collaboration with provincial and territorial counterparts.

The symposium was held in conjunction with the 72nd meeting of the International Working Group on Data Protection in Technology, which the OPC co-hosted with Germany's Federal Commission for Data Protection and Freedom of Information.

To underscore the importance that Commissioner Dufresne places on collaboration and partnerships, in 2023, the OPC established a new Directorate of International, Provincial and Territorial Relations that will serve as the focal point for international and domestic engagements.

The OPC also helped establish the new Canadian Digital Regulators Forum, along with the Competition Bureau and the Canadian Radio-television and Telecommunications Commission (CRTC), which will enable better collaboration, information sharing, and coordination on matters relating to digital markets and platforms.

Other examples of domestic collaboration included continuing the OPC's joint investigations with its Quebec, British Columbia, and Alberta counterparts into TikTok and OpenAI, the company that developed and launched ChatGPT.

At their annual meeting in October 2023, federal, provincial, and territorial regulators passed joint resolutions on privacy in the modern workplace and on the privacy rights of young people. They also created a version of the resolution for children and their caregivers, and a document that provides additional guidance for organizations about how they can address the principles set out in the resolution.

The OPC continued to work with its international counterparts through organizations such as the G7 Data Protection and Privacy Authorities Roundtable and the Global Privacy Assembly.

The meeting of the G7 Data Protection and Privacy authorities in June resulted in a joint statement on generative AI and an action plan for greater cooperation. The Global Privacy Assembly annual meeting in October likewise focused on emerging technologies. Members adopted several resolutions dealing with AI, including one co-sponsored by the OPC that called on the Global Privacy Assembly to work with organizations that develop or implement AI tools in the employment context, such as surveillance and data collection and retention tools.

In August, Commissioner Dufresne, along with members of the Global Privacy Assembly's International Enforcement Cooperation Working Group, issued a joint statement on data scraping. This statement outlines the key privacy risks with data scraping and sets out how websites should protect individuals' personal information. The statement also outlines steps that individuals can take to minimize privacy risks.

The OPC also sought out new partnerships, for example through memorandums of understanding with the Philippines, by aligning the OPC with groups such as the Global Cooperation Arrangement for Privacy Enforcement (Global CAPE) and by renewing a Memorandum of Understanding with other members of the Unsolicited Communications Enforcement Network.

To commemorate Human Rights Day in December, Commissioner Dufresne, on behalf of the 30 members of the Global Privacy Assembly's Data Protection and Other Rights and Freedoms Working Group, issued a joint statement on privacy and democratic rights along with Dr. Ana Brian Nougrères, United Nations Special Rapporteur on the Right to Privacy.

The OPC coordinated the 2024 Global Privacy Enforcement Network (GPEN) Sweep, which focused on deceptive design patterns, also known as dark patterns. The Sweep was coordinated alongside the International Consumer Protection and Enforcement Network. The aims of the exercise include identifying opportunities for targeted education and enforcement, and creating greater consumer trust in the digital economy.

FURTHER READING

- OPC signs agreement to promote cross-border cooperation on combatting unsolicited communications and scams
- OPC participates in meeting of Asia Pacific Privacy Authorities
- OPC guidance: Privacy in the Workplace
- Commissioner Dufresne joins Asia Pacific counterparts to discuss progress on key privacy challenges

Contributions Program

Each year, the OPC's Contributions Program funds independent research and public education projects to increase knowledge about privacy issues and enhance awareness of the importance of privacy protection.

For 2023-2024, the OPC received 44 proposals answering to the theme, "The future is now! Assessing and managing the privacy impacts of immersive and embeddable technologies." The OPC funded 11 projects, which received a total of almost $500,000 in support.

In December 2023, the OPC put out a call for proposals for the 2024-25 funding cycle based on two of the OPC's strategic priorities: addressing the privacy impacts of new technologies and protecting children's privacy. The OPC also increased the maximum available to each project from $50,000 to $100,000.

The program was established in 2004 to support arms-length, non-profit research on privacy, further privacy policy development and promote awareness on the protection of personal information in Canada.

FURTHER READING

OPC's Contributions Program funds research into impact of technology on privacy

Children's privacy and AI at heart of this year's call for proposals for research and awareness projects

Outreach to Canadians

A member of OPC's Outreach team at the BC Library Conference exhibit in Vancouver, British Columbia.

An important part of the OPC's mission is to promote public awareness and understanding of public privacy issues. With its outreach activities, the OPC seeks to inform people about the implications of their privacy choices and how to protect their personal information in order to help build a generation of children, youth, and adults with strong privacy awareness.

Online, the OPC's outreach efforts included blogs to help people understand their privacy rights and how to protect them, social media content and campaigns, as well as tips and resources for youth.

The OPC also participated in exhibiting events, engaging with youth, parents, educators, librarians, newcomers and seniors at in-person events across the country.

Educational resources for teachers were also promoted through email campaigns, and provided information to Canadians on the importance of creating strong and unique passwords through a radio campaign.

The OPC reached tens of thousands of Canadians and businesses through social media campaigns such as Privacy Awareness Week, Cybersecurity Awareness Month, Small Business Week, Media Literacy Week, Data Privacy Week and Fraud Prevention Month.

FURTHER READING

Playing your part in protecting privacy

It's garbage day for unused apps: Tips for individuals for increasing the security of mobile devices

Before the Courts

The OPC devoted significant resources to litigation in 2023-2024. The OPC worked to enforce the fundamental right to privacy before the courts, obtained clarity about the scope of federal privacy laws, and responded to jurisdictional challenges.

Privacy Commissioner of Canada v. Facebook, Inc. (T-190-20 & A-129-23)

In 2019, an OPC investigation into Facebook found that Facebook contravened PIPEDA by failing to obtain meaningful consent from users for the disclosure of their personal information and to safeguard that information.

The OPC filed a notice of application with the Federal Court on February 6, 2020, under s. 15 of PIPEDA (File T-190-20) seeking an order requiring Facebook to correct its privacy practices to comply with the federal private-sector privacy law.

On April 15, 2020, Facebook brought an application seeking judicial review of the OPC's decision to investigate and to continue to investigate, and of the investigation process (File T-473-20).

The Federal Court heard both applications in March 2023. On April 13, 2023, the Court dismissed Facebook's application for judicial review, finding that Facebook had not filed its application in time and that the OPC had not breached its procedural fairness obligations.

On April 13, 2023, the Court also dismissed the OPC's application, finding, in particular, that there was insufficient evidence to conclude that Facebook had not obtained meaningful consent from users.

In May 2023, the OPC announced that it was appealing the Court's decision, noting that the issues at the heart of the case are directly related to Canadians' fundamental right to privacy and that the issues would benefit from being clarified by the Federal Court of Appeal.

On February 21, 2024, the Federal Court of Appeal heard the appeal. At the time of writing, the Court's decision was pending.

FURTHER READING

Notice of Application with the Federal Court against Facebook, Inc.

Privacy Commissioner of Canada v Facebook, Inc. (T-190-20) (Federal Court) (Facebook 1), Facebook, Inc. v Privacy Commissioner of Canada (T-473-20) (Federal Court) (Facebook 2)

Privacy Commissioner appeals Federal Court decision related to Facebook investigation

Google LLC v. Canada (Privacy Commissioner), 2023 FCA 200

In October 2023, the Federal Court of Appeal released a decision that upheld the Federal Court's 2021 decision that Google's search engine service is subject to federal privacy law and is not exempt from PIPEDA under the journalistic purposes exemption.

The OPC had asked the Court to consider the issue in the context of a complaint involving an individual who alleged that Google was contravening PIPEDA by prominently displaying links to online news articles about the complainant when their name was searched. The individual alleged that the articles were outdated, inaccurate and disclosed sensitive personal information, and that this caused them significant harm. The OPC asked the court to clarify whether Google's search engine is subject to federal privacy law when it indexes web pages and presents search results in response to searches of a person's name.

Google had argued that PIPEDA did not apply in this context and that, if it does apply and requires the articles to be de-listed, it would be unconstitutional.

FURTHER READING

Canada's Privacy Commissioner welcomes Federal Court of Appeal decision that Google's search engine service is subject to Canada's federal privacy law

9219-1568 Quebec Inc. v. Canada (Privacy Commissioner), 2024 FCA 38

This legal proceeding related to the OPC's investigation into Aylo (formerly known as MindGeek), the operator of Pornhub and other pornographic sites. The OPC found that Aylo contravened PIPEDA by failing to undertake reasonable efforts to ensure that it was obtaining meaningful consent from each person who appears in intimate content uploaded to its websites.

In April 2023, before the OPC's final report of findings could be issued and published, Aylo filed a judicial review application with the Federal Court (File T-853-23) seeking, amongst other relief, a declaration that the OPC's investigation and decision to publish its investigation report exceeded its jurisdiction, as well as an order prohibiting the OPC from publishing its report of findings in the investigation.

In May 2023, Aylo filed a motion seeking an interim injunction preventing the publication of the OPC's report of findings until the disposition of its judicial review application.

In October 2023, the Federal Court dismissed Aylo's motion, finding that it had not met the test to obtain an interim injunction. In dismissing Aylo's injunction motion, the Federal Court found that Aylo had not demonstrated that it would be irreparably harmed by the issuance and publication of the report, and that the public interest weighed heavily in favour of the Commissioner, as a statutory actor seeking to carry out his statutory duties. Aylo appealed the Federal Court's decision.

On February 29, 2024, the Federal Court of Appeal heard Aylo's appeal. That same day, the Federal Court of Appeal issued a decision from the bench dismissing Aylo's appeal and upholding the Federal Court's decision. The OPC published its report of findings that day.

FURTHER READING

Statement by the Privacy Commissioner of Canada following an investigation into Pornhub operator Aylo

Pornhub operator failed to obtain meaningful consent before allowing adult content to be posted on its websites

Appendices

Appendix 1: Definitions

Complaint types

Access
The institution/organization is alleged to have denied one or more individuals access to their personal information as requested through a formal access request.

Accountability
Under PIPEDA, an organization has failed to exercise responsibility for personal information in its possession or custody, or has failed to identify an individual responsible for overseeing its compliance with the Act.

Accuracy
The institution/organization is alleged to have failed to take all reasonable steps to ensure that personal information that is used is accurate, up-to-date and complete.

Challenging compliance
Under PIPEDA, an organization has failed to put procedures or policies in place that allow an individual to challenge its compliance with the Act, or has failed to follow its own procedures and policies.

Collection
The institution/organization is alleged to have collected personal information that is not necessary, or has collected it by unfair or unlawful means.

Consent
Under PIPEDA, an organization has collected, used or disclosed personal information without valid consent, or has made the provisions of a good or service conditional on individuals consenting to an unreasonable collection, use, or disclosure.

Correction/notation (access)
The institution/organization is alleged to have failed to correct personal information or has not placed a notation on the file in the instances where it disagrees with the requested correction.

Correction/notation (time limit)
Under the *Privacy Act*, the institution is alleged to have failed to correct personal information or has not placed a notation on the file within 30 days of receipt of a request for correction.

Extension notice
Under the *Privacy Act*, the institution is alleged to have not provided an appropriate rationale for an extension of the time limit, applied for the extension after the initial 30 days had been exceeded, or, applied a due date more than 60 days from date of receipt.

Fee
The institution/organization is alleged to have inappropriately requested fees in an access to personal information request.

Identifying purposes
Under PIPEDA, an organization has failed to identify the purposes for which personal information is collected at or before the time the information is collected.

Index
Info Source (a federal government directory that describes each institution and the information banks – groups of files on the same subject – held by that particular institution) is alleged to not adequately describe the personal information holdings of an institution.

Language
In a request under the *Privacy Act*, personal information is alleged to have not been provided in the official language of choice.

Openness
Under PIPEDA, an organization has failed to make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Retention (and disposal)
The institution/organization is alleged to have failed to keep personal information in accordance with the relevant retention period: either destroyed too soon or kept too long.

Safeguards
Under PIPEDA, an organization has failed to protect personal information with appropriate security safeguards.

Complaint types (continued)

Time limits
Under the *Privacy Act*, the institution is alleged to have not responded within the statutory limits.

Use and disclosure
The institution/organization is alleged to have used or disclosed personal information without the consent of the individual or outside permissible uses and disclosures allowed in legislation.

Dispositions

Well-founded
The institution or organization contravened a provision of the *Privacy Act* or PIPEDA.

Well-founded and resolved
The institution or organization contravened a provision of the *Privacy Act* or PIPEDA but has since taken corrective measures to resolve the issue to the satisfaction of the OPC.

Well-founded and conditionally resolved
The institution or organization contravened a provision of the *Privacy Act* or PIPEDA. The institution or organization committed to implementing satisfactory corrective actions as agreed to by the OPC.

Not well-founded
There was no or insufficient evidence to conclude the institution/organization contravened the privacy legislation.

Resolved
Under the *Privacy Act*, the investigation revealed that the complaint is essentially a result of a miscommunication, misunderstanding, etc., between parties; and/or the institution agreed to take measures to rectify the problem to the satisfaction of the OPC.

Settled
The OPC helped negotiate a solution that satisfied all parties during the course of the investigation, and did not issue a finding.

Discontinued
Under the *Privacy Act*: The investigation was terminated before all the allegations were fully investigated. A case may be discontinued for various reasons, but not at the OPC's behest. For example, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion.

Under PIPEDA: The investigation was discontinued without issuing a finding. An investigation may be discontinued at the Commissioner's discretion for the reasons set out in subsection 12.2(1) of PIPEDA.

No jurisdiction
It was determined that federal privacy legislation did not apply to the institution/organization, or to the complaint's subject matter. As a result, no report is issued.

Early resolution (ER)
Applied to situations in which the issue is resolved to the satisfaction of the complainant early in the investigation process and the OPC did not issue a finding.

Declined to investigate
Under PIPEDA, the Commissioner declined to commence an investigation in respect of a complaint because the Commissioner was of the view that:

- the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;

- the complaint could be more appropriately dealt with by means of another procedure provided for under the laws of Canada or of a province; or,

- the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose, as set out in subsection 12(1) of PIPEDA.

Withdrawn
Under PIPEDA, the complainant voluntarily withdrew the complaint or could no longer be practicably reached. The Commissioner does not issue a report.

Appendix 2: Statistical tables

Statistical tables related to the *Privacy Act*

Table 1 – *Privacy Act* dispositions of access and privacy complaints by institution

Respondent	Discontinued	Early resolved	Not well-founded	Resolved	Settled	Well-founded	Well-founded – Conditionally resolved	Well-founded – Deemed refusal	Well-founded – Resolved	Total
Administrative Tribunals Support Service of Canada		2								**2**
Agriculture and Agri-food Canada			1							**1**
Atlantic Canada Opportunities Agency			1							**1**
Business Development Bank of Canada			1							**1**
Canada Border Services Agency	3	27	8			2	1		1	**42**
Canada Energy Regulator		1	1							**2**
Canada Mortgage and Housing Corporation		1								**1**
Canada Post Corporation		20	4			3			5	**32**
Canada Revenue Agency	2	47	11		1		4		1	**66**
Canada School of Public Service							1			**1**
Canadian Air Transport Security Authority			1							**1**
Canadian Armed Forces			1						1	**2**
Canadian Broadcasting Corporation	2	1								**3**
Canadian Centre for Occupational Health and Safety		1								**1**
Canadian Food Inspection Agency		2	2							**4**
Canadian Heritage		1	1				1			**3**
Canadian Human Rights Commission			1							**1**
Canadian Radio-Television and Telecommunications Commission			1							**1**
Canadian Security Intelligence Service		7	4							**11**
Canadian Space Agency			1							**1**
Canadian Transportation Agency		1								**1**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police		1	1							**2**
Communications Security Establishment Canada			1							**1**

Respondent	Discontinued	Early resolved	Not well-founded	Resolved	Settled	Well-founded	Well-founded – Conditionally resolved	Well-founded – Deemed refusal	Well-founded – Resolved	Total
Correctional Service Canada		52	33	2		4	7	1	13	**112**
Crown-Indigenous Relations and Northern Affairs Canada		4								**4**
Defence Construction Canada		1								**1**
Department of Finance Canada			1							**1**
Department of Justice Canada		7	3			1				**11**
Department of National Defence	1	28	6						2	**37**
Elections Canada / Office of the Chief Electoral Officer		1								**1**
Employment and Social Development Canada	1	28	12		1	3	2			**47**
Environment and Climate Change Canada		3	2							**5**
Federal Government of Canada		1	1							**2**
Fisheries and Oceans Canada		13	4						1	**18**
Global Affairs Canada	2	5	7			1	1		1	**17**
Health Canada		9	3						1	**13**
Immigration and Refugee Board of Canada	2	5							1	**8**
Immigration, Refugees and Citizenship Canada	2	23	4						4	**33**
Impact Assessment Agency of Canada	1	2	2			1			1	**7**
Indigenous Services Canada		5	2							**7**
Innovation, Science and Economic Development Canada		5	2							**7**
Library and Archives Canada		1	1							**2**
Military Grievances External Review Committee		1								**1**
Military Police Complaints Commission		1								**1**
National Research Council Canada		3	1							**4**
National Security and Intelligence Review Agency									2	**2**
Natural Resources Canada		1	1		1					**3**
Natural Sciences and Engineering Research Council of Canada						1				**1**
Office of the Correctional Investigator			1							**1**
Office of the Information Commissioner of Canada	1									**1**

Respondent	Discontinued	Early resolved	Not well-founded	Resolved	Settled	Well-founded	Well-founded – Conditionally resolved	Well-founded – Deemed refusal	Well-founded – Resolved	Total
Parks Canada Agency		1	13						2	**16**
Parole Board of Canada		2			1	1			2	**6**
Passport Canada		2								**2**
Prairies Economic Development Canada			1							**1**
Privy Council Office	1	1								**2**
Public Health Agency of Canada		3	3							**6**
Public Prosecution Service of Canada		2								**2**
Public Safety Canada			2							**2**
Public Service Commission of Canada	1	1	1						1	**4**
Public Services and Procurement Canada	4	10	5	1		1			1	**22**
Royal Canadian Mounted Police	2	53	18			4			2	**79**
Service Canada		1								**1**
Shared Services Canada		2	4							**6**
Social Sciences and Humanities Research Council of Canada		1								**1**
Statistics Canada	1	8	2							**11**
Trans Mountain Corporation		1							1	**2**
Transport Canada		13	3						1	**17**
Treasury Board of Canada Secretariat		1	1						1	**3**
Veterans Affairs Canada	1	7	4			1	1		2	**16**
VIA Rail Canada		1	1							**2**
Total	**27**	**421**	**185**	**3**	**4**	**23**	**18**	**1**	**47**	**729**

Table 2 – *Privacy Act* investigations – Average treatment times by complaint and disposition types

Complaint type	Early resolved		Dispositions not early resolved		All dispositions	
	Number of Cases	**Average treatment time** (months)	**Number of cases**	**Average treatment time** (months)	**Number of cases**	**Average treatment time** (months)
Access	**260**	**8.3**	**166**	**11.6**	**426**	**9.6**
Access	257	8.3	166	11.6	423	9.6
Correction – Notation	3	9.4			3	9.4
Privacy	**161**	**6.8**	**142**	**22.1**	**303**	**13.9**
Accuracy	1	5.4	3	11.6	4	5.0
Collection	25	7.5	52	18.6	77	16.0
Retention and disposal	7	12.2	3	16.3	10	9.5
Use and disclosure	128	5.8	84	24.9	212	8.6
Time limits	**221**	**1.3**	**328**	**2.4**	**549**	**1.8**
Extension notice			4	2.6	4	2.6
Time limits	221		324	2.1	545	1.8
Total	**642**	**5.5**	**636**	**9.0**	**1,278**	**7.3**

Table 3 – *Privacy Act* treatment times – All closed files by disposition

Complaint type	Count	Average treatment time (months)
Early resolved	**642**	**5.5**
All other investigations	**636**	**9.0**
Discontinued	29	15.1
Not well-founded	188	15.5
Resolved	3	15.0
Settled	4	38.0
Well-founded	23	17.6
Well-founded – Conditionally resolved	234	3.3
Well-founded – Deemed refusal	71	2.9
Well-founded – Resolved	84	9.9
Total	**1,278**	**7.3**

Table 4 – *Privacy Act* breaches by institution

Respondent	Number of incidents
Agriculture and Agri-food Canada	1
Bank of Canada	1
Canada Energy Regulator	1
Canada Post Corporation	3
Canada Revenue Agency	71
Canadian Forces Morale and Welfare Services / Non-Public Property and Staff of the Non-Public Funds, Canadian Forces	1
Canadian Grain Commission	1
Canadian Heritage	1
Canadian Human Rights Commission	1
CBC/Radio-Canada	2
Civilian Review and Complaints Commission for the RCMP	1
Communications Security Establishment Canada	3
Correctional Service Canada	20
Department of Finance Canada	1
Department of Justice Canada	1
Department of National Defence	1
Elections Canada / Office of the Chief Electoral Officer	1
Employment and Social Development Canada	377
Environment and Climate Change Canada	1
Federal Economic Development Agency for Northern Ontario	1
Financial Transaction and Reports Analysis Centre of Canada	3
Global Affairs Canada	6
Health Canada	3
Immigration and Refugee Board of Canada	1
Immigration, Refugees and Citizenship Canada	8
Impact Assessment Agency of Canada	3
Infrastructure Canada	1
Innovation, Science and Economic Development Canada	1
Military Grievances External Review Committee	2
National Research Council Canada	1
Natural Resources Canada	1
Office of the Auditor General	1
Office of the Commissioner of Lobbying of Canada	1

Respondent	Number of incidents
Patented Medicine Prices Review Board	1
Public Prosecution Service of Canada	4
Public Safety Canada	1
Public Sector Pension Investment Board	1
Public Service Commission of Canada	8
Royal Canadian Mounted Police	14
Shared Services Canada	1
Statistics Canada	1
Transport Canada	1
Transportation Safety Board of Canada	1
Treasury Board of Canada Secretariat	3
Veterans Review and Appeal Board	2
Windsor-Detroit Bridge Authority	1
Total	**561**

Table 5 – *Privacy Act* complaints and breaches

Category	Total
Accepted	
Access	331
Privacy	179
Time limits	603
Total complaints accepted	**1,113**
Closed through early resolution	
Access	260
Privacy	161
Time limits	221
Total	**642**
Closed through all other investigations*	
Access	166
Privacy	142
Time limits	328
Total	**636**
Total complaints closed	**1,278**
Breaches received	
Unauthorized disclosure	85
Loss	382
Theft	5
Unauthorized access	89
Total breaches received	**561**

*Including summary investigations

Table 6 – *Privacy Act* complaints accepted by complaint type

Complaint type	Early resolution		Summary investigation*		Investigation		Total	
	Number	Percentage	Number	Percentage	Number	Percentage	Number	Percentage
Access								
Access	238	33%	64	19%	26	42%	**328**	**29%**
Correction - Notation	3	0%					**3**	**0%**
Privacy								
Accuracy	2	0%					**2**	**0%**
Collection	23	3%	2	1%	10	16%	**35**	**3%**
Retention and disposal	3	0%	2	1%	2	3%	**7**	**1%**
Use and disclosure	105	15%	6	2%	24	39%	**135**	**12%**
Time limits								
Extension notice	2		3	1%			**5**	**0%**
Time limits	344	48%	254	77%			**598**	**54%**
Total	**720**		**331**		**62**		**1,113**	

*Summary investigations are shorter investigations that conclude with the issuance of a brief report or letter of findings.

Table 7 – *Privacy Act* top institutions by complaints accepted and fiscal year

Respondent	2018-2019	2019-2020	2020-2021	2021-2022	2022-2023	2023-2024
Royal Canadian Mounted Police	273	176	186	179	262	**266**
Correctional Service Canada	426	155	130	182	199	**201**
Immigration, Refugees and Citizenship Canada	59	44	47	49	131	**110**
Canada Border Services Agency	109	42	48	53	78	**103**
Department of National Defence	121	33	51	53	74	**78**
Canada Revenue Agency	79	63	40	48	79	**76**
Employment and Social Development Canada	39	25	41	26	54	**32**
Canadian Security Intelligence Service	24	15	16	14	13	**23**
Global Affairs Canada	20	19	18	11	26	**21**
Transport Canada	12	5	6	10	12	**20**
Canada Post Corporation	29	4	22	45	23	**20**
Total	**1,191**	**581**	**605**	**670**	**951**	**950**

Table 8 – *Privacy Act* complaints accepted by institution

Respondent	Early resolution	Summary investigation	Investigation	Total
Administrative Tribunals Support Service of Canada	1			**1**
Canada Border Services Agency	73	24	6	**103**
Canada Energy Regulator	1			**1**
Canada Mortgage and Housing Corporation	2			**2**
Canada Post Corporation	12	7	1	**20**
Canada Revenue Agency	57	14	5	**76**
Canadian Centre for Occupational Health and Safety	1			**1**
Canadian Food Inspection Agency	1			**1**
Canadian Heritage	1			**1**
Canadian Human Rights Commission	4		1	**5**
Canadian Security Intelligence Service	14	3	6	**23**
Canadian Transportation Agency	1			**1**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police	2	2		**4**
Commissioner of Canada Elections			2	**2**
Communications Security Establishment Canada	4	2		**6**
Correctional Service Canada	84	107	10	**201**
Crown-Indigenous Relations and Northern Affairs Canada	6		1	**7**
Department of Justice Canada	10	3	2	**15**
Department of National Defence	47	26	5	**78**
Employment and Social Development Canada	22	8	2	**32**
Environment and Climate Change Canada	2	3		**5**
Fisheries and Oceans Canada	4			**4**
Global Affairs Canada	13	5	3	**21**
Health Canada	8	2		**10**
Immigration and Refugee Board of Canada	6	1		**7**
Immigration, Refugees and Citizenship Canada	104	2	4	**110**
Impact Assessment Agency of Canada	2		1	**3**
Indigenous Services Canada	4			**4**

Respondent	Early resolution	Summary investigation	Investigation	Total
Innovation, Science and Economic Development Canada	3	1		**4**
Library and Archives Canada	4			**4**
Military Grievances External Review Committee	1			**1**
National Research Council Canada	1			**1**
National Security and Intelligence Review Agency	1	2		**3**
Natural Resources Canada	1			**1**
Office of the Correctional Investigator	1	1		**2**
Office of the Information Commissioner of Canada			1	**1**
Parks Canada Agency	3	12	1	**16**
Privy Council Office	1	2		**3**
Public Health Agency of Canada	4			**4**
Public Prosecution Service of Canada	1			**1**
Public Safety Canada	2	1		**3**
Public Service Commission of Canada			1	**1**
Public Services and Procurement Canada	10		2	**12**
Royal Canadian Mounted Police	162	99	5	**266**
Shared Services Canada	1			**1**
Social Sciences and Humanities Research Council of Canada	1			**1**
Statistics Canada	3	1		**4**
Transport Canada	19	1		**20**
Treasury Board of Canada Secretariat	5	1	1	**7**
Veterans Affairs Canada	10	1	2	**13**
Total	**720**	**331**	**62**	**1,113**

Table 9 – *Privacy Act* dispositions by complaint type

Complaint type	Discontinued	Not well-founded	Resolved	Settled	Well-founded	Well-founded – Conditionally resolved	Well-founded – Deemed refusal	Well-founded – Resolved	Total
Access	**15**	**101**	**262**	**3**	**8**	**5**	**1**	**31**	**426**
Access	15	101	259	3	8	5	1	31	**423**
Correction – Notation			3						**3**
Privacy	**12**	**84**	**162**	**1**	**15**	**13**		**16**	**303**
Accuracy			1		1	2			**4**
Collection	3	45	25		2	2			**77**
Retention and disposal		2	7			1			**10**
Use and disclosure	9	37	129	1	12	8		16	**212**
Time limits	**2**	**3**	**221**			**216**	**70**	**37**	**549**
Extension notice	2	1						1	**4**
Time limits		2	221			216	70	36	**545**
Total	**29**	**188**	**645**	**4**	**23**	**234**	**71**	**84**	**1,278**

Table 10 – *Privacy Act* dispositions of time limits by institution

Respondent	Discontinued	Resolved	Not well-founded	Well-founded – Conditionally resolved	Well-founded – Deemed refusal	Well-founded – Resolved	Total
Administrative Tribunals Support Service of Canada		1					**1**
Canada Border Services Agency		18		16	8	11	**53**
Canada Post Corporation		2		2	3		**7**
Canada Revenue Agency		13		10	1	1	**25**
Canadian Human Rights Commission		1					**1**
Canadian Institutes of Health Research	1						**1**
Canadian Security Intelligence Service		2					**2**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police						1	**1**
Communications Security Establishment Canada		2		4			**6**
Correctional Service Canada		22		78	15	2	**117**
Crown-Indigenous Relations and Northern Affairs Canada		1					**1**
Department of Justice Canada		1		3	2		**6**
Department of National Defence		18		11	15	2	**46**
Employment and Social Development Canada		12		1	3		**16**
Environment and Climate Change Canada		1		3			**4**
Global Affairs Canada		4		1		2	**7**
Health Canada		3		2			**5**
Immigration and Refugee Board of Canada		2		1			**3**
Immigration, Refugees and Citizenship Canada		49		1	1	3	**54**
Indigenous Services Canada		2			1		**3**
Innovation, Science and Economic Development Canada				1			**1**
National Security and Intelligence Review Agency		1	1			1	**3**

Respondent	Discontinued	Resolved	Not well-founded	Well-founded – Conditionally resolved	Well-founded – Deemed refusal	Well-founded – Resolved	Total
Privy Council Office				1		1	**2**
Public Health Agency of Canada		1					**1**
Public Safety Canada		1		1			**2**
Public Service Commission of Canada			1				**1**
Public Services and Procurement Canada		2					**2**
Royal Canadian Mounted Police	1	55		78	21	12	**167**
Transport Canada		3		2			**5**
Treasury Board of Canada Secretariat		2				1	**3**
Veterans Affairs Canada		2	1				**3**
Total	**2**	**221**	**3**	**216**	**70**	**37**	**549**

Statistical tables related to PIPEDA

Table 1 – PIPEDA complaints accepted by industry sector

Industry sector	Number	Proportion of all complaints accepted
Accommodations	24	5%
Construction	3	1%
Entertainment	22	5%
Financial sector	112	25%
Food and beverage	7	2%
Government	3	1%
Health	7	2%
Individual	1	0%
Insurance	12	3%
Internet*	72	16%
Manufacturing	5	1%
Mining and oil and gas extraction	1	0%
Not for profit organizations	2	0%
Professionals	18	4%
Publishers (except Internet)	1	0%
Rental	7	2%
Sales/Retail	40	9%
Services	47	11%
Telecommunications	33	7%
Transportation	28	6%
Utilities	1	0%
Total	**446**	

*This category includes: Internet service providers and other computing and Internet services, excluding information distribution services or online information distribution services (e.g. news, software and mobile apps publishers, directories, search portals and social media sites).

Table 2 – PIPEDA complaints accepted by complaint type

Complaint type	Number	Proportion of all complaints accepted
Access	101	23%
Accountability	1	0%
Accuracy	7	2%
Challenging compliance	8	2%
Collection	32	7%
Consent	63	14%
Correction/Notation	3	1%
Openness	10	2%
Retention	48	11%
Safeguards	30	7%
Time limits	51	11%
Use and disclosure	92	21%
Total	**446**	

Table 3 – PIPEDA investigations closed by industry sector and disposition

Industry sector	Early resolved	Discontinued	Not well-founded	Settled	Well-founded	Well-founded – Conditionally resolved	Well-founded – Resolved	Withdrawn	Total
Accommodations	25						2		**27**
Agriculture, Forestry, Fishing and Hunting							1		**1**
Construction	2								**2**
Entertainment	18				1				**19**
Financial Sector	79	4	4	3			2	4	**96**
Food and Beverage	8								**8**
Government	2								**2**
Health	3						1		**4**
Individual	1								**1**
Insurance	9	1							**10**
Internet*	77		1					1	**79**
Manufacturing	3						2		**5**
Mining and Oil and Gas Extraction	1								**1**
Not for profit organizations	2								**2**
Professionals	15	1					1		**17**
Publishers (except Internet)	2	2							**4**
Rental	5								**5**
Sales/Retail	30	1	1				1		**33**
Services	32		1				1		**34**
Telecommunications	26	1	1			2			**30**
Transportation	23				1	1			**25**
Total	**363**	**10**	**8**	**3**	**2**	**3**	**11**	**5**	**405**

*This category includes: Internet service providers and other computing and Internet services, excluding information distribution services or online information distribution services (e.g. news, software and mobile apps publishers, directories, search portals and social media sites).

Table 4 – PIPEDA investigations closed by complaint type and disposition

Complaint type	Early resolved	Discontinued	Not well-founded	Settled	Well-founded	Well-founded – Conditionally resolved	Well-founded – Resolved	Withdrawn	Total
Access	104	3	2	1			3		**113**
Accountability	5								**5**
Accuracy	7								**7**
Challenging compliance	6								**6**
Collection	41	1							**42**
Consent	51		2				1	1	**55**
Correction/Notation	7								**7**
Openness	12								**12**
Retention	34				1		3		**38**
Safeguards	12	1	1			2	1	1	**18**
Time limits	17				1	1			**19**
Use and disclosure	67	5	3	2			3	3	**83**
Total	**363**	**10**	**8**	**3**	**2**	**3**	**11**	**5**	**405**

Table 5 – PIPEDA investigations – Average treatment times by disposition

Disposition	**Number**	**Average treatment time** (months)
Early resolved	363	6.6
Discontinued (under 12.2)	10	12.1
Not well-founded	8	15.7
Settled	3	4.5
Well-founded	2	8.0
Well-founded – Conditionally resolved	3	39.5
Well-founded – Resolved	11	16.9
Withdrawn	5	3.9
Total	**405**	
Overall weighted average		7.4

Table 6 – PIPEDA investigations – Average treatment times by complaint and disposition types

Complaint type	Early resolved		Dispositions not early resolved		All dispositions	
	Number of cases	Average treatment time (months)	Number of cases	Average treatment time (months)	Number of cases	Average treatment time (months)
Access	104	7.2	9	12.3	113	7.6
Accountability	5	6.2			5	6.2
Accuracy	7	6.5			7	6.5
Challenging compliance	6	5.0			6	5.0
Collection	41	7.2	1	8.9	42	7.2
Consent	51	7.0	4	5.5	55	6.9
Correction/Notation	7	8.4			7	8.4
Openness	12	3.8			12	3.8
Retention	34	5.6	4	21.0	38	7.3
Safeguards	12	5.6	6	29.2	18	13.4
Time limits	17	2.8	2	9.9	19	3.6
Use and disclosure	67	7.0	16	11.2	83	7.8
Total	**363**	**6.6**	**42**	**14.3**	**405**	**7.4**

Table 7 – PIPEDA breach notifications by industry sector and incident type

	Incident type					
Industry sector	**Loss**	**Theft**	**Unauthorized access**	**Unauthorized disclosure**	**Total incidents per sector**	**Percentage of total incidents**
Accommodation			5	2	**7**	**1%**
Agriculture, forestry, fishing and hunting			2	1	**3**	**0%**
Construction			5		**5**	**1%**
Entertainment			8	2	**10**	**1%**
Financial sector	7	5	110	48	**170**	**25%**
Food and beverage			3		**3**	**0%**
Government	1	1	4	4	**10**	**1%**
Health		2	10	10	**22**	**3%**
Insurance	9	4	21	7	**41**	**6%**
Internet*			8	3	**11**	**2%**
Manufacturing			46	1	**47**	**7%**
Mining and oil and gas extraction			5		**5**	**1%**
Not for profit organizations	1	2	30	4	**37**	**5%**
Professionals	2	4	56	8	**70**	**10%**
Publisher (except Internet)			17	2	**19**	**3%**
Rental			1		**1**	**0%**
Sales/Retail	2	2	39	5	**48**	**7%**
Services	1	4	41	9	**55**	**8%**
Telecommunications			99	18	**117**	**17%**
Transportation			8		**8**	**1%**
Utilities			3	1	**4**	**1%**
Total	**23**	**24**	**521**	**125**	**693**	

*This category includes: Internet service providers and other computing and Internet services, excluding information distribution services or online information distribution services (e.g. news, software and mobile apps publishers, directories, search portals and social media sites).

Table 8 – Number of Canadian accounts affected by incident type

Incident type	Number of Canadian accounts affected
Loss	1,053
Theft	1,357
Unauthorized access	23,503,629
Unauthorized disclosure*	1,741,008
Total	**25,247,047**

* In previous years, "Accidental disclosure" was used by our Office to reflect instances where personal information was disclosed outside of the provisions of PIPEDA, either intentionally or accidentally. This term has been changed to "Unauthorized disclosure" to reflect the wording of PIPEDA, but the meaning remains unchanged.

Appendix 3: Substantially similar legislation

Subsection 25(1) of PIPEDA requires the OPC to report annually to Parliament on the "extent to which the provinces have enacted legislation that is substantially similar" to the Act.

Under paragraph 26(2)(b) of PIPEDA, the Governor in Council may issue an Order exempting an organization, a class of organizations, an activity or a class of activities from the application of Part 1 of PIPEDA with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation that is "substantially similar" to Part 1 of PIPEDA.

On August 3, 2002, Industry Canada (now known as Innovation, Science and Economic Development Canada) published the Process for the Determination of "Substantially Similar" Provincial Legislation by the Governor in Council, outlining the policy and criteria used to determine whether provincial legislation will be considered substantially similar. Under the policy, laws that are substantially similar:

- provide privacy protection that is consistent with and equivalent to that in PIPEDA
- incorporate the 10 principles in Schedule 1 of PIPEDA
- provide for an independent and effective oversight and redress mechanism with powers to investigate
- restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate

Organizations that are subject to provincial legislation deemed substantially similar are exempt from Part 1 of PIPEDA with respect to the collection, use, or disclosure of personal information occurring within the respective province.

Accordingly, PIPEDA continues to apply to the collection, use or disclosure of personal information in connection with the operations of a federal work, undertaking or business in the respective province, as well as to the collection, use or disclosure of personal information outside the province.

The following provincial laws have been declared substantially similar to Part 1 of PIPEDA:

- Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*
- British Columbia's P*ersonal Information Protection Act*
- Alberta's *Personal Information Protection Act*
- Ontario's *Personal Health Information Protection Act*, with respect to health information custodians
- New Brunswick's *Personal Health Information Privacy and Access Act*, with respect to health information custodians
- Newfoundland and Labrador's *Personal Health Information Act*, with respect to health information custodians
- Nova Scotia's *Personal Health Information Act*, with respect to health information custodians

Appendix 4: Report of the Privacy Commissioner, Ad Hoc

As Ad Hoc Privacy Commissioner, I review the outcomes of cases where individuals sought access to information held by the Office of the Privacy Commissioner of Canada (OPC), or where it is alleged the OPC mishandled the personal information of an individual. The OPC is subject to the legislation it oversees, the *Privacy Act*, and such outcomes may trigger the right to complain to the Ad Hoc Privacy Commissioner.

In the reporting year of April 1, 2023, to March 31, 2024, two complaints commenced in the prior year were concluded and I received 39 additional matters, representing a great deal more cases filed with me than in the previous year. I noticed a similar increase in the number of complaints in my comparable oversight role under the *Access to Information Act*, observing a notable increase in the level of dissatisfaction by individuals who request information from government institutions, be it from the time it took to obtain a response, to the actual benefit gained from the process itself. For this reason alone, the relative increase in files was not entirely unexpected for my work involving the OPC.

Of the seven new complaints, four cases resulted from unsatisfactory outcomes to requesting personal information, mainly for accessing the contents of complaint investigation files carried out by the OPC, the disclosure of which is governed by section 22.1, a very strict and limiting exemption to disclosure that I reported on in prior annual reports.

Interestingly, one case involved a challenge to the use of the section 26 exemption; some of the requester's personal information also concerned personal information about another identifiable individual. Section 26 required the OPC to address the possibility of disclosure and refuse access after relevant factors are weighed. My task was to review those factors in determining the lawfulness of the OPC's decision to refuse access, meaning the OPC had to demonstrate it considered the applicability of the exemption carefully, and had exercised its discretion in good faith based on existing circumstances.

In another case, I refused to accept a complaint relating to a request for access to information filed out of time, weeks beyond the set time-limit of 60 days from the date a response was issued. I have discretion to examine circumstances related to a 'late filing' and have used it in the past to extend the time limit to accept late complaints; however, I did not in that case based on the individual's established familiarity with the rules surrounding requests as well as those for filing complaints on time. The individual also admitted to not having a valid reason to explain the long delay. Two additional complaint cases regarding access to information were still under review at year end.

In each case investigated and concluded, a report of findings is issued to provide answers to questions, provide clear explanations as to applicability of the rules regarding access to one's personal information while raising greater awareness of the *Privacy Act* as it applies to the OPC.

One new complaint of a privacy breach was filed, and it followed the breach notification I had earlier received from the OPC regarding an incident external to the OPC, but for which the OPC itself was linked. The complaint of a privacy breach was filed with me as the oversight authority on matters of privacy breaches attributable to the OPC. I am currently investigating that complaint while the OPC is investigating the external incident as the oversight authority for privacy in Canada, making this case not only complex but also a first of its kind.

Of the remaining new files received last year, 32 were complaints that I could not accept as they fell outside of my delegated authority: individuals who requested access to their personal information from federal and provincial government institutions and remained dissatisfied with those outcomes. In each case, with explanations, I redirected them to the appropriate provincial or federal oversight office to pursue their concerns and many write they appreciate this service.

Undeniably, all the files I received last year were noteworthy and interesting as was the case in the past year. I once again look forward to continuing my work for those who will seek my assistance in the coming months.

Respectfully submitted,

Anne E. Bertrand, K.C.
Ad Hoc Privacy Commissioner

Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada