Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

2024-2025

Prioritizing privacy in a data-driven world

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.

2024-2025 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 5, 2025

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, 2024 to March 31, 2025, *Prioritizing privacy in a data-driven world*. This tabling is done pursuant to sections 38 and 40(1) 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 5, 2025

The Honourable Francis Scarpaleggia, 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, 2024 to March 31, 2025, *Prioritizing privacy in a data-driven world*. This tabling is done pursuant to sections 38 and 40(1) 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 2024-2025 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 individuals' fundamental right to privacy. 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.

At a time when the personal information of Canadians is being collected, used, and shared at an unparalleled pace and volume on a global scale, effective privacy protection requires more than the status quo. Prioritizing privacy as a fundamental right reflects our Canadian values and ambitions and reinforces the freedoms and trust that underpin our democracy.

Privacy matters for individuals and for organizations. The continued advancement in the adoption of artificial intelligence (AI) and generative AI, the risk of significant harms caused by data breaches, and the increasingly complex nature of global data flows have put data protection at the forefront of the public interest.

Data is power and protecting it is paramount. To that end, it has been my goal to ensure that my Office is well-positioned to maximize efforts to protect Canadians in a data-driven world and in these unprecedented times.

Throughout this past fiscal year, we have examined our internal processes and structures to ensure that we are using every tool in our toolbox to protect and promote individuals' fundamental right to privacy.

In January 2025, I unveiled a transformation plan marking the beginning of a change journey to a modernized OPC that delivers on its mandate and strategic priorities in the most efficient and impactful way possible.

Once fully implemented, the transformation will aim to allow the OPC to respond more rapidly and effectively to emerging issues; broaden our approach to compliance; and bring stronger alignment to our policy and legal work, as well as our enforcement and advisory activities.

The plan re-frames the OPC's compliance function as a continuum, by combining proactive engagement and formal investigative functions into one sector.

Going forward, my Office will seek to promote compliance more strategically, using measures that are the most relevant and efficient for any given situation. This will include anything along the compliance continuum – from public statements, advisory services, and guidance to help organizations prevent issues from arising, to outreach to organizations, compliance agreements, and full investigations when warranted.

The OPC's transformation plan also recognizes the current fiscal reality, both within the OPC and across the federal government. It is imperative that we exercise even more stringent financial management, while finding creative ways to leverage the strengths of our organization in a manner that will position us for success.

I am looking forward to fully implementing and operationalizing the plan over the coming months, so that Canadians, and Canadian institutions and organizations that are subject to federal privacy legislation, can benefit from this innovative approach to our work.

Working more effectively was at the heart of the three strategic priorities that I launched in January 2024: protecting and promoting privacy with maximum impact; addressing and advocating for privacy in a time of technological change; and protecting the privacy of children.

In the pages that follow, you will read about the work that has taken place over the last year across the OPC to continue to advance these priorities in many areas of our work.

For example, we have strengthened collaboration with domestic and international counterparts and other regulatory institutions to address a wide range of issues. At a time when personal information flows across borders at unprecedented volumes and speed, exchanging information and working together across our respective domains and jurisdictions is essential.

No matter where they or their data may travel, Canadians must have the assurance that institutions and organizations in the public and private sectors are prioritizing the protection of their personal information, to enable them to confidently enjoy the benefits of the digital world.

In the last fiscal year, we continued to offer institutions and organizations advice and tools to support their compliance with privacy laws. This includes the launch, in March 2025, of a new online tool that will help them to determine the real risk of significant harm of privacy breaches.

We have also undertaken initiatives to address and support the privacy needs of young people. This included conducting a survey to better understand the privacy concerns and needs of parents and teachers in Canada and applying a children's privacy lens to our enforcement activities.

Bill C-27, which would have modernized PIPEDA, died on the order paper with the prorogation of Parliament in January 2025. I am confident that law reform, to ensure that Canadians remain protected in a modern world, will again become a legislative priority in the 45th Parliament. This should include both reform to the private-sector privacy law, as well as long-awaited reform of the *Privacy Act*.

I will continue to advocate for modernized laws that recognize privacy as a fundamental right, that advance the public interest, and that foster a strong Canadian economy, including by ensuring that trade with our international partners can continue to flourish.

That being said, I am also confident that the structural changes that I am implementing at the Office will position the OPC well to continue to effectively protect Canadians' fundamental right to privacy. Until changes are made, Canada's existing privacy laws continue to apply, including for new technologies such as generative AI, and I am committed to their application.

As we review the work of the last fiscal year, I am proud of all that we have accomplished. I am also eagerly looking ahead to what is to come in 2025-2026. Highlights will include hosting the G7 Data Protection and Privacy Authorities Roundtable in June 2025, in the context of Canada's G7 presidency, as well as an international privacy symposium that will be focused on issues surrounding youth privacy in the digital age.

As I approach the midpoint in my seven-year mandate as Privacy Commissioner of Canada, I remain grateful for the opportunity to protect and promote Canadians' fundamental right to privacy in an increasingly complex landscape.

Philippe Dufresne
Privacy Commissioner of Canada

Timeline

Highlights of some of the key activities of the Office of the Privacy Commissioner of Canada (OPC) in 2024-2025.

April **2024**

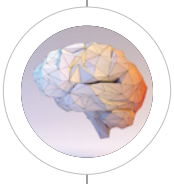
OPC joins international privacy enforcement group

The OPC joins the Global Cooperation Arrangement for Privacy Enforcement, a non-binding arrangement for cross-border data protection and privacy enforcement.

Survey of Canadian businesses on privacy-related issues

Results from the OPC's biennial survey of Canadian businesses suggest that the number of businesses planning to use AI will increase sharply in the next five years.

May **2024**



May **2024**

Commissioner Dufresne becomes Chair of Canadian Digital Regulators Forum

Commissioner Dufresne turns his focus to synthetic media as he assumes the role of Chair of the Canadian Digital Regulators Forum.

New online breach-reporting forms

The OPC launches an online breach-reporting form for federal institutions, and an updated form for businesses subject to PIPEDA, to make it easier to report breaches.

May **2024**

June **2024**

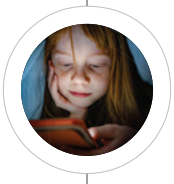
Launch of joint investigation into data breach at 23andMe

The privacy authorities for Canada and the United Kingdom launch a joint investigation into an October 2023 data breach at global direct-to-consumer genetic testing company 23andMe.

Exploratory consultation on age assurance

The OPC seeks input on issues related to age assurance and privacy to inform policy on how and when online services should confirm the age of a user.

June **2024**



July **2024**

[Launch of investigation into Ticketmaster breach]

Commissioner Dufresne launches an investigation following a cybersecurity incident that affected the accounts of millions of people worldwide.

July **2024**

[Global Privacy Enforcement Network releases results of deceptive design privacy sweep]

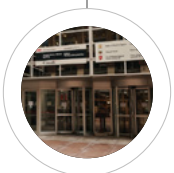
The OPC's Privacy Sweep finds that the vast majority of apps and websites use deceptive design to influence privacy choices, including sites targeting children.

August **2024**

[Agreement with the U.S. Federal Communications Commission]

Commissioner Dufresne signs a Memorandum of Understanding with the United States Federal Communications Commission that establishes parameters for the exchange of information between the two regulators to enforce compliance with laws in both countries.

September **2024**



[Federal Court of Appeal decision on Facebook]

Commissioner Dufresne welcomes the unanimous Federal Court of Appeal ruling, stating that it is an acknowledgement that international data giants must respect Canadian privacy law.

September **2024**

[OPC collaborates with international regulators on age assurance]

The OPC joins other global regulators in moving toward a more common international approach to the data protection and privacy implications of age-assurance methods.

[Annual meeting of access to information and privacy regulators in Canada]

Federal, provincial, and territorial regulators adopt resolutions on deceptive design and sharing information in cases of intimate-partner violence.

October **2024**

[Commissioner Dufresne meets with G7 counterparts]

The G7 Data Protection and Privacy Authorities Roundtable releases statements on the role of data protection and privacy authorities in fostering trustworthy AI, and on child-appropriate AI.

October **2024**

[Launch of investigation into breaches at the Canada Revenue Agency]

Commissioner Dufresne launches an investigation into cyberattacks at the Canada Revenue Agency that led to more than 30,000 privacy breaches dating back to 2020.

October **2024**

[Global Privacy Assembly annual meeting]

Commissioner Dufresne joins international regulators to advance efforts to standardize how personal information is shared between countries.

November **2024**

[Information-sharing agreements with Nigeria and Brazil]

Memorandums of Understanding with data protection authorities from Nigeria and Brazil facilitate information sharing and enforcement collaboration.

November **2024**

[Commissioner Dufresne welcomes LinkedIn pause related to AI training]

LinkedIn paused training of AI models using information from Canadian member accounts pending discussions with the OPC regarding privacy concerns.

December **2024**

January **2025**

Data Privacy Week campaign – Put Privacy First

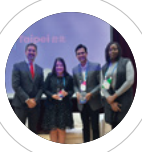
The OPC spreads the message that considering privacy at the beginning of an initiative is a key to future-proofing programs, services, and systems.

January **2025**

OPC Transformation Plan

Commissioner Dufresne launches an internal transformation aimed at maximizing the OPC's impact in protecting and promoting the fundamental right to privacy in an increasingly complex and evolving digital world.

February **2025**



Winners of first global Privacy and Human Rights Award announced

Commissioner Dufresne announces that the 5Rights Foundation and the Internet Freedom Foundation are the co-winners of the first Privacy and Human Rights Award.

February **2025**

OPC seeks court order against Pornhub operator

A Federal Court application requests an order to require Aylo to take steps to obtain meaningful consent from all who appear in images uploaded to the website.

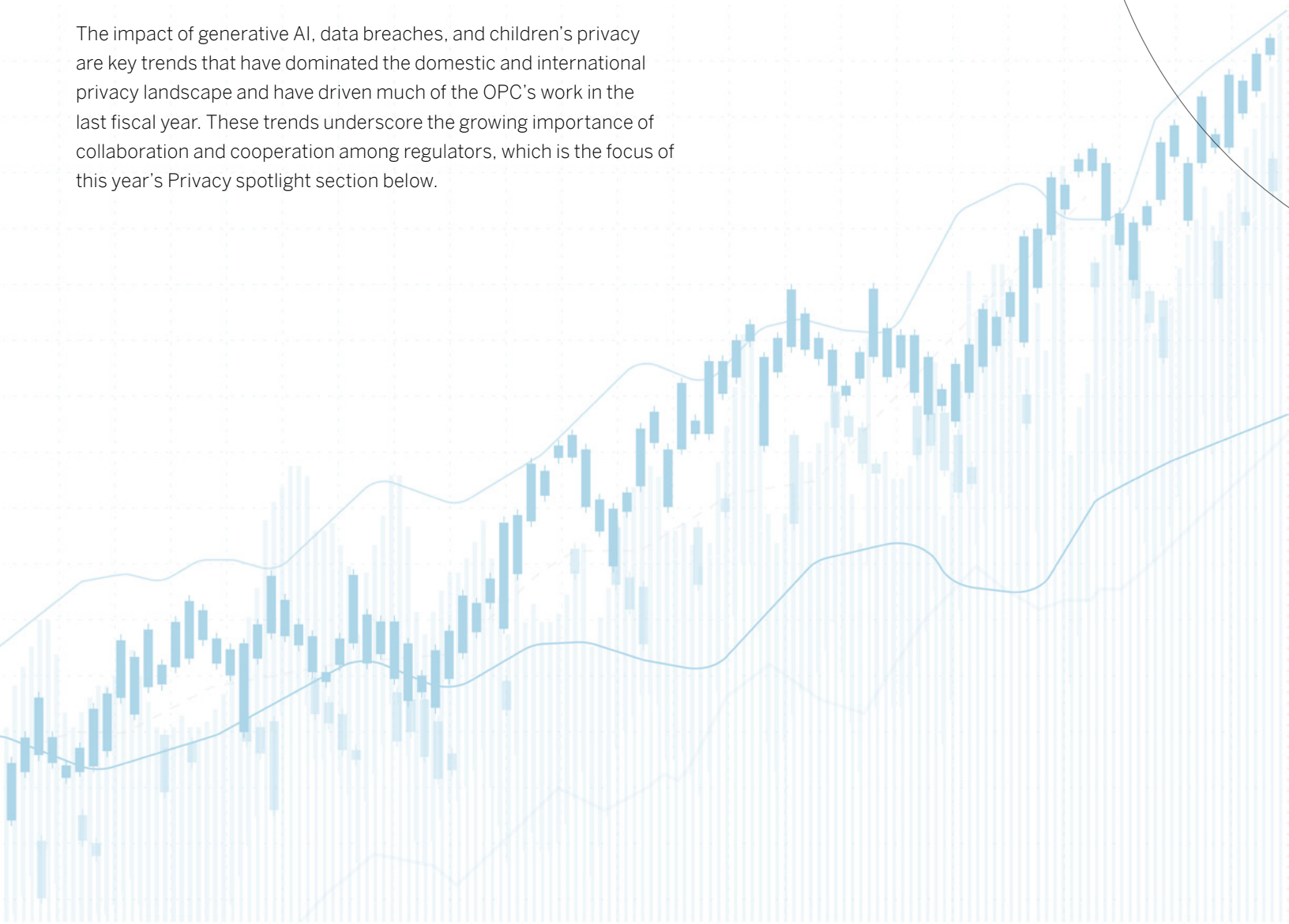
March **2025**

Privacy Commissioner launches breach risk self-assessment tool for organizations

The new online tool will help businesses and federal institutions that experience a privacy breach to assess whether the breach is likely to create a real risk of significant harm to individuals.

Top trends in privacy

The impact of generative AI, data breaches, and children's privacy are key trends that have dominated the domestic and international privacy landscape and have driven much of the OPC's work in the last fiscal year. These trends underscore the growing importance of collaboration and cooperation among regulators, which is the focus of this year's Privacy spotlight section below.



Artificial intelligence and privacy

Individuals

As generative AI is increasingly integrated and used in the applications, programs and services that individuals use on a regular basis, and as individuals continue to discover many different uses for AI tools in their everyday lives, enormous volumes of personal information are being collected.

According to the OPC's latest survey of Canadians (2024-2025):

- **83% of Canadians** have some level of concern about their privacy when using AI tools (34% are extremely concerned)
- **88%** are at least somewhat concerned about their personal information being used to train AI systems (42% are extremely concerned)

According to a study by Canadian and American researchers discussed at the first Conference on Language Modeling last year, a sampling of unidentified, consenting users were found to have disclosed enough sensitive information to an AI chatbot for researchers to positively identify them or the subject of the query (Mireshghallah, N, Antoniak, M., More, Y., Yejin, C., & Farnadi, G. (2024) Trust No Bot: Discovering Personal Disclosures in Human-LLM Conversations in the Wild. 10.48550/arXiv.2407.11438).

In the results, the researchers found that:

- **More than 70% of queries** contained personally identifiable information, and **almost 15%** mentioned a sensitive topic, such as sexual preferences or drug use.
- **Around 50% of translation queries** contained some form of personally identifiable information.

AI use in the federal government

Some federal government institutions are exploring the use of AI to streamline or automate routine tasks to better serve Canadians. In March 2025, the government released its Artificial Intelligence Strategy for the Federal Public Service.

Government departments that sought advice from the OPC over the last year are already using or expressed an interest in using AI for a variety of functions, including:

- Chatbots;
- Automating searches of multiple client files to determine benefits eligibility;
- Automated document sorting and categorizing;
- Assisting with facial recognition programs;
- Initial evaluations of candidates during staffing processes and tracking employment applications.

Breaches

With a threat environment that is constantly evolving, data breaches continue to be a significant issue of concern. It is essential that both public institutions and private organizations prioritize information security, as there can be serious consequences for individuals whose personal information is impacted by a privacy breach.

The stakes are also high for organizations. Globally, a report by IBM released in July 2024 says that the average cost of a data breach for a business reached about $4.88 million US in 2024 (IBM Report: Escalating Data Breach Disruption Pushes Costs to New Highs, 2024).

The OPC saw a similar volume of breach reports received in 2024-2025 under both Acts compared to the previous fiscal year, with a small increase (7%) in the public sector. Compared to the previous year, the number of affected individuals under the Privacy Act grew by more than 124% while the number of affected individuals decreased by 20% under PIPEDA.

As stewards of Canadians' sensitive personal information, several government departments and agencies are attractive targets for malicious actors.

AI also has an impact on breaches. According to a recent Canadian Centre for Cyber Security report, AI technologies "are almost certainly lowering the barriers to entry and enhancing the quality, scale, and precision of malicious cyber threat activity." The report adds that cybercriminals are themselves using AI to support their operations.

- **Four in 10 Canadians (43%)** said that they have been affected by a privacy breach, according to the OPC's latest survey of Canadians.

- **Approximately 20 million individual accounts** were affected by breaches that were reported to the OPC in 2024-2025.

In 2024-2025, the OPC launched a new online intake form for private- and public-sector organizations to report breaches.

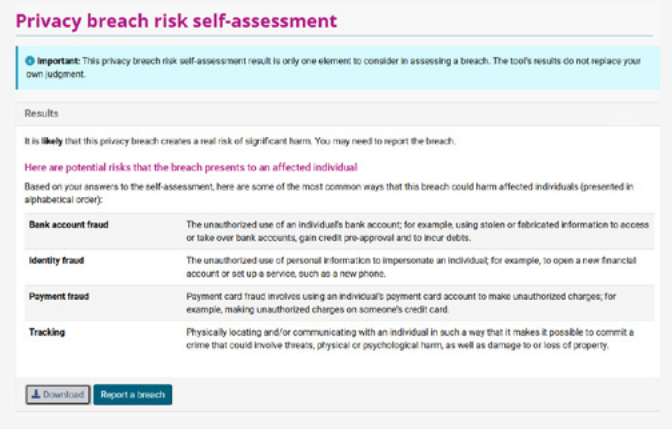
While legislative obligations differ under PIPEDA and the *Privacy Act* as pertains to breach reporting, all organizations are encouraged to use the new online tool to support efficient and timely reporting. For federal institutions, the new tool offers an added convenience by ensuring that breach reports are sent to both the OPC and the Treasury Board of Canada Secretariat (TBS) simultaneously.

The OPC also launched a new online privacy risk-assessment tool in March 2025. The Privacy Breach Risk Self-Assessment Tool is a user-friendly, web-based application that guides organizations through a series of questions to assist them in assessing the real risk of significant harm, which includes an examination of the sensitivity of the personal information that was involved in a data breach, and the probability that it will be misused.

Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, financial loss, identity theft, negative effects on one's credit record, and damage to, or loss of, property.

Identity theft, scams, hacking or other unauthorized access, be it deliberate or accidental, may result in a privacy breach, and such breaches could include sensitive information such as personal health or financial data.

The tool is meant to help private- and public-sector organizations conduct a risk assessment following a data breach and to assist them in determining their next steps, including notifying affected individuals and reporting a breach to the OPC.



Youth privacy

As young people continue to embrace new technologies and experience much of their lives online, privacy remains an important priority to ensure their safety in a digital world.

According to MTM Junior, Keep Scrolling for More - Kids, Teens and Social Media (2024):

- **52% of children aged 7 to 11** use social media every week (of these, 35% use it daily)
- **95% of youth aged 12 to 17** use social media every week (of these, 84% use it daily)
- **Over 1 in 5 social media users aged 7 to 17** have written comments, and 1 in 6 have posted photos and videos
- **79% of children aged 2 to 17** in Canada had played a video game in the past month (MTM Junior, Pixel Playgrounds: Exploring the World of Kids' Gaming (2024))

In a recent OPC online survey of parents (February 2025):

Privacy concern

- **91% of parents** have some level of concern about the personal information that companies are collecting from their children
- **85%** are at least somewhat concerned about the amount of personal information that their children share online
- **74%** say that they have little-to-no trust that businesses would protect their children's personal information

Parent-child discussions about privacy

- **45% of parents** say that they discuss online privacy with their children at least once a month
- **33%** say that they do so a couple of times a year

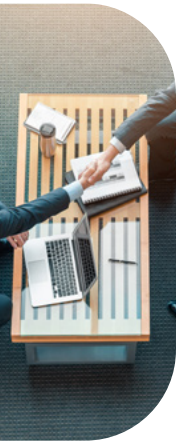
Privacy spotlight: Collaboration

The growth of global digital platforms and generative AI, and the unparalleled volume of personal information that is being collected and shared across borders, have introduced a new magnitude of complexity that has transformed the privacy landscape.

Domestic and international collaboration and cooperation among regulators, public institutions, industry, and civil society is essential to addressing global privacy challenges.

Sharing knowledge and expertise, jointly examining emerging issues, and working together to advance common standards provide greater consistency for organizations operating across jurisdictions and better privacy protections for individuals.

This is a theme that is woven into the fabric of Commissioner Dufresne's 2024-2027 strategic plan.



Domestic collaboration

The OPC works with provincial and territorial privacy regulators to maximize its impact. Some recent highlights include the collaborative development and launch of joint principles for responsible, trustworthy and privacy-protective generative AI technologies, and joint resolutions on responsible information-sharing in situations involving intimate partner violence, and on identifying and mitigating harms from privacy-related deceptive design patterns.

The provinces of Quebec, British Columbia, and Alberta have private-sector privacy laws that have been deemed substantially similar to PIPEDA. PIPEDA allows the OPC to work closely with these provinces on investigations such as those that are ongoing into OpenAI, the company behind AI-powered chatbot ChatGPT, and TikTok.

International collaboration

Despite different cultures, legal foundations, and socio-economic realities amongst data protection regulating nations, international collaboration has grown in response to the global nature of modern data flows.

This reflects a shared goal to protect individuals' fundamental right to privacy no matter where they or their data may travel. Individuals must have confidence that organizations are prioritizing the protection of their personal information to enable them to enjoy the benefits of the digital world.

International collaboration allows the OPC to be at the leading edge of the fast-paced environment to best inform and advise Canadians, parliamentarians, as well as institutions and organizations on privacy matters.

In the past year, this has included global leadership on privacy protection through engagements with international counterparts such as the G7 Data Protection and Privacy Authorities Roundtable, the Global Privacy Assembly (GPA), the Asia Pacific Privacy Authorities (APPA), and the Global Privacy Enforcement Network (GPEN). Efforts have focused on advancing the role of data protection and privacy authorities in the regulation of AI, youth privacy, and addressing privacy in the age of data, and coordination of this past year's annual GPEN privacy sweep, which focused on online deceptive design patterns.

In February 2025, Commissioner Dufresne, in his role as Chair of the GPA's Working Group on Data Protection and Other Rights and Freedoms, announced the co-winners of the first Privacy and Human Rights Award. A collaboration with the GPA and the international human rights organization Access Now, the award celebrates outstanding leadership by organizations around the world that have made a significant contribution in the fields of privacy, data protection, and other fundamental rights.

Moreover, the Privacy Commissioner engages in bilateral partnerships through Memorandums of Understanding such as those signed this year with the U.S. Federal Communications Commission, the Nigeria Data Protection Commission, and the Brazilian National Data Protection Authority.

With technology evolving at such a rapid pace, leveraging international partnerships through joint initiatives is an important way in which we can protect Canadians. This includes, for example, the joint investigation launched in June 2024 in collaboration with the UK Information Commissioner into a data breach at global direct-to-consumer genetic testing company 23andMe.

Cross-regulatory collaboration

Cross-regulatory collaboration is of growing importance in an increasingly complex digital environment.

The dominance of tech giants, global digital platforms and social media; the volume of personal information in their holdings; and their disruptive impact on information, competition, copyright, and telecommunications, have changed the landscape, making privacy one of many intersecting regulatory factors to be considered.

To that end, the OPC was one of the founders, in 2023, of the Canadian Digital Regulators Forum, along with the Canadian Radio-television and Telecommunications Commission, and the Competition Bureau. The Copyright Board joined the group in 2024.

Commissioner Dufresne assumed the role of Chair of the Forum in May 2024. Since then, the Forum has focused on exploring how the proliferation of synthetic media, including deepfakes, impacts each of their respective mandates. Given the scale and global nature of digital markets and the speed at which they innovate, the Forum has also sought to strengthen its partnerships by joining the International Network of Digital Regulation Cooperation (INDRC), which connects cross-regulatory organizations from around the world.

Working with **industry**

Commissioner Dufresne has noted that just as data fuels innovation, innovation must be used to protect data. One way to achieve this goal is for the OPC to engage with businesses, particularly those developing and using new technologies, to ensure that they are aware of their privacy obligations under PIPEDA and to help them embed privacy into their business practices.

In addition to the above, the OPC continues to collaborate in this domain. An example is the concluding joint statement on data scraping and the protection of privacy that the Commissioner signed with 15 other members of the GPA's International Enforcement Cooperation Working Group, which sets out expectations regarding what organizations should do to ensure that individuals are protected from unlawful data scraping.

The joint statement marked the culmination of an important engagement between regulators and industry data stakeholders. Major social media companies were invited to comment on how they comply with privacy legislation.

Deceptive design

Deceptive-design patterns that encourage people to give away more personal information online than they want to or should was an issue of focus for the OPC and its domestic and international partners in 2024-2025.

In fact, it was the subject of the 2024 GPEN privacy Sweep, as well as a joint resolution that was adopted by Commissioner Dufresne and his provincial and territorial counterparts in October 2024.

The resolution called on public- and private-sector organizations to avoid using deceptive design patterns, and to limit users' exposure to these patterns by building privacy into their design frameworks.

The sweep, which involved 26 privacy enforcement authorities from across Canada and around the world, found that 97% of the more than 1,000 websites and apps that were reviewed were using at least one of the following deceptive design patterns:

- complex and confusing language;
- interface interference – design elements that distract, influence or confuse users, for example by making it easier to accept targeting or advertising cookies than to reject them;
- nagging – like frequent pop-ups asking users to sign up for an account, provide an email address or switch to an app;
- obstruction – which may involve making it difficult to find privacy settings and information; and
- forced action – such as requiring users to divulge more personal information when trying to delete their account than they had to provide when they created it.

The OPC, along with its counterparts from British Columbia and Alberta, also examined 67 websites that are specifically targeted at children. They found that sites and apps geared toward children were more likely than those targeted at the general population to use certain types of deceptive design patterns, such as interface interference and nagging.

Both the global report and the OPC's report are available on the OPC website, along with tips for individuals and businesses.

Following the publication of its report, the OPC wrote to 27 organizations to communicate the observations made during the sweep and to encourage them to review their websites and apps for deceptive design patterns. Following this engagement, nearly three quarters of those organizations committed to implementing improvements to avoid deceptive-design patterns and using more privacy-protective design.

Recognizing the growing intersection between privacy and other regulatory spheres, this past year's sweep was the first to be coordinated with the International Consumer Protection and Enforcement Network. The network represents consumer protection authorities from around the world, including Canada's Competition Bureau.

Privacy Act: A year in review

In its 2024-2025 public sector work, the OPC was increasingly sought after to provide guidance to government departments planning to implement AI for a variety of purposes. This trend is expected to accelerate given the March 2025 launch of the federal government's AI Strategy for the Federal Public Service. The OPC provided input and advice to federal institutions to strengthen protections related to privacy and the use of personal information.

The OPC also continued to work with federal institutions through its outreach and speaking events to support departmental understanding of privacy risks and help build capacity to manage personal information responsibly.

In terms of its work enforcing the *Privacy Act*, in 2024-2025 the OPC received – and accepted – the largest-ever number of complaints under the *Privacy Act*.

Overall, the OPC received 11% more complaints under the *Privacy Act* in 2024-2025 than in the previous fiscal year, 1,942 compared to 1,749, and accepted 1,279, an increase of 15% compared to 1,113 accepted in the previous year. There are no specific factors that have been observed that led to the increase this year, as complaints rose across all categories.

Time limit complaints – that is, complaints submitted when institutions do not respond to personal information requests within the time period set out in legislation – remained the largest segment. The OPC accepted 653 time-limit complaints this fiscal year, an increase of 8% compared to the previous fiscal year, when the OPC accepted 603 time-limit complaints.

Access complaints – which relate to an institution allegedly having denied an individual access to their personal information – was the second-largest issue, with 331 complaints. Another 174 complaints related to the collection, use, disclosure, retention, and disposal of personal information.

Similar to the previous fiscal year, the largest proportion of complaints accepted in 2024-2025 involved the Royal Canadian Mounted Police (RCMP) (274, or 21%), followed by Correctional Service Canada (226, or 18%) and Immigration, Refugees and Citizenship Canada (IRCC) (136, or 11%).

Meanwhile, the OPC closed 1,317 complaints, an increase of 3% from the previous fiscal year.

At the beginning of the fiscal year, 86 investigations under the *Privacy Act* were older than 12 months – 18% of all active investigations. By the end of the fiscal year, the backlog had declined to 25, or 6% of all active investigations. The OPC is continually working to identify innovative ways to improve efficiencies in the compliance process, including through restructuring the sector as outlined in the OPC's transformation plan, which will come into full effect in 2025-2026.

The following section highlights key initiatives under the *Privacy Act* in 2024-2025.

Privacy by the numbers

Privacy Act

Type	Number
Complaints accepted	1,279
Well-founded complaints	431
Complaints closed through early resolution	746
Complaints closed through standard investigation	571
Data breach reports received	615
New advisory consultations opened with government institutions	108
Privacy impact assessments (PIAs) received	138
Letters of recommendation and advice provided to government institutions following PIA review or consultation	119
Public interest disclosures by federal organizations	658

Top institutions by number of complaints accepted

Respondent	Number
Royal Canadian Mounted Police	274
Correctional Service Canada	226
Immigration, Refugees and Citizenship Canada	136
Canada Border Services Agency	107
Department of National Defence	95
Canada Revenue Agency	82
Canadian Security Intelligence Service	70
Canada Post Corporation	33
Employment and Social Development Canada	29
Global Affairs Canada	26
Total	**1,078**

Early resolution

Early resolution continued to be an important investigative tool for resolving low-complexity, non-systemic complaints.

The number of *Privacy Act* complaints closed through early resolution in 2024-2025 was 746, a 16% increase from the previous year.

Early resolution is a good example of how collaboration with complainants and respondents can help to achieve compliance more efficiently. This approach uses engagement and negotiation to reach a timely outcome.

In 2024-2025, the OPC addressed 91% (1,194) of all complaints under the *Privacy Act* through either early resolution, or summary investigations, which are shorter investigations that conclude with a brief report or letter of findings.

Percentage of all *Privacy Act* complaints closed in early resolution

Fiscal year	Percentage
2024-2025	57%
2023-2024	50%
2022-2023	47%
2021-2022	40%
2020-2021	52%

Members of the OPC's Government Advisory Directorate at the Canadian Access and Privacy Association Annual Conference in Ottawa.

Government advisory work

Consultations with law enforcement and intelligence communities

The OPC focused its government advisory efforts on working more closely with federal law enforcement and intelligence communities in 2024-2025, consulting and providing advice on initiatives that could impact the privacy of Canadians.

As part of this work, the OPC engaged with the RCMP on a number of topics, including protecting personal information as municipal police services take over former RCMP-contracted police services in some communities; the RCMP's use of open-source information; its facial recognition policy; and its proposed plan to use genetic genealogy for investigative purposes.

Discussions on the privacy risks surrounding the use of body-worn cameras continued as the RCMP provided as many as 15,000 body-worn cameras to federal police and contracted police forces across the country.

The OPC will continue to work with federal institutions that are considering using body-worn cameras to ensure that privacy issues are addressed. This includes taking into consideration necessity and proportionality, limiting uses, ensuring justifiable retention periods, facilitating access to images for affected individuals, and ensuring that personal information collected incidentally is protected.

National digital identity initiative

The OPC engaged with Employment and Social Development Canada (ESDC), TBS, Innovation, Science and Economic Development (ISED), and Shared Services Canada (SSC) as lead departments involved in implementing various elements of a centralized national digital identity initiative.

The OPC emphasized the importance of considering the sensitivity of the personal information involved and the impact that a breach would have on individuals, and recommended that the institutions take precautions such as conducting comprehensive privacy impact assessments and implementing robust security safeguards for the information technology systems that manage this sensitive data.

Uptake of AI by government institutions

AI is being used or considered across government for a variety of purposes, such as the administration and management of client benefits; initial assessments of candidates during staffing processes; and in facial recognition systems for immigration enforcement.

Veterans Affairs Canada consulted with the OPC on a pilot project that uses generative AI to create summaries of relevant client information with data taken from service health records, medical questionnaires, and medical reports, to assist in decision-making on disability benefits applications. In addition to recommending that a privacy impact assessment be carried out, the OPC advised the department to consider using increased public communications regarding the uses of AI to support transparency.

TBS consulted the OPC while it was developing its AI Strategy for the Federal Public Service. The OPC will continue to work with TBS and other institutions in the coming months on the responsible use of AI. This will help ensure that when AI is integrated into government programs or services, the implications on individuals and their personal information are carefully considered before the technology is adopted. This includes advising federal entities to ensure, through their contracting practices, that third-party providers of AI comply with their obligations under PIPEDA. Uses of AI must also be appropriate, ethical, and consistent with privacy law.

Outreach to federal government institutions

The OPC held 18 government advisory events in 2024-2025, which were widely attended by ATIP officials across government. These events reached employees of half of all federal government departments and agencies that are covered under the *Privacy Act*.

The OPC also collaborated with TBS on two Canada School of Public Service webinars; one that focused on privacy in the workplace, and another on privacy in government contracting.

In addition, the OPC organized a special event for federal Chief Privacy Officers and Chief Information Officers to encourage greater collaboration between these communities. In his remarks, Commissioner Dufresne noted that the collective expertise and shared values of the two public service groups will be key to protecting and preserving the trust that Canadians hold in government institutions, programs, and services. A highlight of the event was a fireside chat between Commissioner Dufresne and the Government of Canada's Chief Information Officer, Dominic Rochon.

Public-interest disclosures

The *Privacy Act*, the *Department of Employment and Social Development Act*, and the *Customs Act* allow federal institutions to disclose personal information that would otherwise be prohibited from disclosure in situations where the public interest in disclosure clearly outweighs any invasion of privacy, or where it would clearly benefit the individual to whom the information relates. This includes cases where health, safety or security may be at risk. The Privacy Commissioner must be notified when such disclosures are made.

During 2024-2025, the OPC received more than 600 public-interest disclosure notifications. The majority of these involved individuals in distress whom Service Canada officials determined would benefit from wellness checks by local police.

Privacy Act investigations

The following is an overview of some of the investigations that the OPC closed this year:

Canada Revenue Agency fails to adequately protect adopted child's personal information

The OPC investigated a complaint alleging that the Canada Revenue Agency (CRA) inappropriately revealed information about an adopted child to their biological parent. The case highlights the importance of safeguarding children's information and properly training employees who handle sensitive data.

The investigation found that the child, whose name was changed for safety reasons, was adopted in a closed process, with no communication between the adoptive and biological families.

The complainant, the adoptive parent, applied for the Canada Child Tax Benefit using the child's new name. Later, the biological parent also applied for the benefit using the child's birth name. The child's Dependent Identification Number, which existed before either the adoptive or biological parent applied for benefits, was subsequently – and erroneously – linked to the accounts of both the adoptive and biological parents.

According to evidence that was gathered during the investigation, years after the adoption, a CRA employee disclosed the child's full adoptive name to the biological parent when they called about an unrelated matter. The biological parent was then able to use this name to find and initiate contact with the child, causing considerable psychological and legal repercussions for the adoptive family.

While the CRA acknowledged that its employee did not follow the proper internal procedures, the OPC investigation found that the CRA's procedures did not include a mechanism for flagging a safety risk for adopted children.

The OPC recommended that the CRA review and update its procedures. It also recommended that employees be trained on the potential harms that may arise if an adopted child's personal information is breached. In addition, the OPC recommended that the CRA implement oversight measures to ensure that the new procedures are implemented consistently and being followed by its employees.

After the report of findings was issued, the CRA agreed to implement two of the OPC's three recommendations, committing to reviewing and revising its existing procedures and providing comprehensive training to its employees. However, it declined to implement the recommended oversight measures to monitor compliance with the new procedures for one year following the implementation of our recommendations.

Further reading

Investigation into the disclosure of an adopted child's name to their biological mother by the Canada Revenue Agency

OPC investigation finds National Security and Intelligence Review Agency Secretariat's access to polygraph records lawful

The OPC received six complaints after the National Security and Intelligence Review Agency (NSIRA) began a review of the Internal Security Program at the Communications Security Establishment Canada (CSE). The NSIRA review included the first-ever evaluation of the CSE's use of the polygraph in security screening processes.

The complaints concerned NSIRA's access to polygraph examination materials involving a sampling of CSE employees. The complainants questioned NSIRA's authority to collect this personal information, which they deemed very sensitive, and felt that the review could have been accomplished without this access.

There is a legal distinction to be made between the Review Agency itself and the NSIRA Secretariat. Only the Secretariat is a government institution subject to the *Privacy Act*.

The Secretariat plays a substantive role in assisting the Review Agency in fulfilling its mandate, and its activities in support of reviews are subject to the *Privacy Act*. The OPC's investigation therefore examined how the NSIRA Secretariat handled personal information in support of NSIRA's review of CSE.

The investigation found that NSIRA took steps to collaborate with CSE to implement safeguards and to anonymize personal information. These measures significantly reduced the risk that subjects could be re-identified.

The investigation also found that the source material at issue in the complaints – the polygraph examination recordings – were sufficiently anonymized (e.g., faces blurred) such that they did not contain personal information. Likewise, notes that were taken during the review contained no personal information.

In light of the measures taken, and given NSIRA's broad right of access under the *National Security and Intelligence Review Agency Act* and the Secretariat's role in assisting NSIRA in fulfilling its mandate, the OPC found that the complaint about collection was not well-founded.

The OPC did, however, raise concerns with the timeliness of the NSIRA Secretariat's requests to TBS for the approval of several changes respecting Personal Information Banks (PIBs), including the establishment of a new review-specific PIB. The OPC review found that the NSIRA Secretariat had not fulfilled its obligations under section 10 of the *Privacy Act* when the CSE review began. That said, given that the PIB request has since been submitted to TBS, the OPC found that this issue was well-founded and resolved. The NSIRA Secretariat committed to collaborating with TBS on a priority basis to obtain approvals of the PIBs.

Further reading

Investigation of the National Security and Intelligence Review Agency Secretariat in relation to the collection of personal information pursuant to the National Security and Intelligence Review Agency's review of the Communications Security Establishment

Department appropriately declined to delete personal information

The OPC received a complaint that a government institution had refused to dispose of a former employee's information at their request.

The employee had provided the information as part of an accommodation request. When the employee asked that the department dispose of the information, it declined, citing retention requirements under the *Privacy Act*, as well as a Department of Justice litigation hold impacting the personal information at issue.

The Department of Justice had sent a litigation hold notice related to a proposed class action to various departments, including to the respondent. The notice described in detail the scope of the hold – that is, the material relevant to the litigation that had to be preserved.

In this investigation, the OPC first noted that the regulations governing the *Privacy Act* state that the retention period for the employee's personal information is two years. While the regulations do not include a provision that explicitly requires institutions to dispose of personal information, they have discretion to do so before the two-year period has elapsed if the individual consents. In the absence of a litigation hold, the department could have done as the complainant asked.

Under the circumstances, however, the OPC found that the retention and refusal to dispose did not contravene the *Privacy Act*, because the litigation hold created a legal obligation to preserve the information.

Canada Border Services Agency did not obtain complainant's consent for disclosure of their personal information to TV show

An OPC investigation determined that a personal search carried out by the Canada Border Services Agency (CBSA) was disclosed in real time to employees of a TV production company without the individual's consent.

The complainant was referred for secondary inspection by the CBSA, after which border agents determined that they had grounds to conduct a personal search – one where the individual was taken to a private room for a thorough search. The complaint that was filed was related to raw footage that was captured by the production company in connection with that search.

The OPC's review of the footage confirmed that, while the personal search was not recorded on video, microphones were worn by the officers during the search, thus disclosing the audio of the search in real time to those outside the search room, including members of the production company.

The OPC's investigation also found that a member of the production company may have been able to view what was happening inside the room. This finding was based on the evidence gathered, including comments made by individuals outside the room captured on the recording.

The OPC concluded that the personal information collected by the CBSA during the search itself related directly to the CBSA's operating programs and activities, and that the collection was therefore consistent with the *Privacy Act*.

However, the OPC also found that the CBSA did not obtain the valid consent of the complainant to disclose their personal information to the production company in connection with the search.

The OPC also raised concerns regarding the problematic nature of the disclosure in this case. Given the privacy implications surrounding personal searches at the border, the real-time disclosure of the complainant's personal search represented a serious invasion of privacy.

The CBSA accepted the OPC's recommendations to enhance protections and controls around personal searches and has agreed to implement them.

Other investigations

Other *Privacy Act* investigations that the OPC completed this year include the following. The reports of findings are available on the OPC website.

- Department of National Defence denied a soldier's estate access to deceased's personal information, to which the estate was entitled.
- OPC concludes that it was reasonable for Immigration, Refugees and Citizenship Canada to deny a father access to his child's personal information.
- OPC finds claim that the Canada Revenue Agency denied complainant access to their personal information was well-founded.

Privacy Act breaches

In 2024-2025, 615 breach reports were received from government institutions, up from 561 the previous year, while the number of people affected grew twice over, from 138,434 individuals to 309,865 individuals. This increase is due to the rising number of breaches reported to the OPC overall, as well as the thousands of individuals affected by incidents covered by three breach reports submitted by the CRA, which are discussed below.

Government institutions submitted 55 cyber breach reports, compared to 37 in 2023-2024.

In 2024-2025, the OPC received breach reports from the CRA that retroactively covered breaches that dated back to 2020 – reflecting approximately 35,000 incidents. The CRA also made 67 breach reports related to other types of incidents such as misdirected communications or misuse of access privileges.

ESDC, which also collects and uses significant amounts of Canadians' personal information as part of its mandate, was once again this past year the federal institution reporting the most breaches, with 410 breach reports to the OPC. Most of these breaches related to lost passports (92%). While the OPC received fewer breach reports from CRA, these reports covered more incidents than those reported by ESDC.

In federal government institutions, mishandling of information (e.g., data entry error, misdirected correspondence, labelling error) was the cause of 508 breaches reported under the *Privacy Act*. This was followed by cyber incidents (55), employee snooping (37), and security vulnerabilities (14).

Breaches by the numbers - *Privacy Act*

Top institutions by breaches reported

Institution	Breach reports received
Employment and Social Development Canada	410
Canada Revenue Agency	117
Royal Canadian Mounted Police	23
Correctional Service Canada	17
Immigration, Refugees and Citizenship Canada	11

Cyber incident at the Financial Transactions and Reports Analysis Centre of Canada did not create a real risk of significant harm

In March 2024, the OPC received reports of a cyber incident at the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) regarding a breach of its security safeguards.

Throughout its interactions with the OPC during the investigation, FINTRAC was cooperative and forthcoming, allowing the OPC to carry out a swift assessment of the incident.

Following its review, the OPC found that the breach did not create a real risk of significant harm because the personal information involved had been encrypted and there was no evidence to suggest that the threat actor had been able to decrypt it.

Thousands affected by breaches at the Canada Revenue Agency

In May 2024, the OPC received a breach report from the CRA, retroactively covering the period from May 2020 to November 2023, which captured 31,393 separate incidents. The OPC met regularly with the CRA to stay up to date on the actions that it had been taking to address the breaches.

Following the receipt of a complaint in October 2024, Commissioner Dufresne launched an investigation into these breaches.

Since May 2024, the CRA has submitted additional breach reports capturing approximately 4,000 incidents.

These privacy breaches at the CRA underscore not only the risk to personal information, but also the importance that must be placed on addressing and mitigating all breaches, including cyber incidents.

Appearing before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) in the context of its study of Privacy Breaches at the Canada Revenue Agency, Commissioner Dufresne noted that as stewards of sensitive personal information, government institutions are attractive targets for malicious actors and must therefore continuously adapt to the evolving threat environment.

The Commissioner also highlighted the OPC's regular engagement with federal institutions, including advice and guidance to support efforts to address and mitigate the risks posed by breaches, as well as prevent, contain and report breaches. He further noted that each engagement and compliance activity plays an important role in supporting and advancing privacy protection across the Government of Canada, which is increasingly complex and significant in this digital era.

Further reading

Privacy Commissioner discusses breaches at the Canada Revenue Agency during appearance before parliamentary committee

Loss of unencrypted USB device a serious breach for RCMP

The OPC investigated the loss of an unencrypted USB storage device containing the personal information of more than 1,700 individuals, including names and other personal information of victims, witnesses, informants, RCMP members, and employees.

The RCMP detachment learned from a confidential informant three weeks after the loss that the data on the device was being offered for sale by members of the criminal community. The detachment then reported the missing device to RCMP National Headquarters, which in turn reported the loss to the OPC.

During the investigation, the OPC received additional breach reports of other lost unencrypted USB devices – the use of which is contrary to the RCMP's own standards.

Given the nature and sensitivity of the personal information that the RCMP handles on a daily basis, the OPC recommended that the RCMP put in place strict security measures around the use of USB storage devices.

The RCMP agreed in principle to the OPC's recommendations to strengthen safeguards but, at the time of writing, had still not committed to implementing the recommendations within a specific timeline.

Further reading

Investigation of the loss of an unencrypted Universal Serial Bus (USB) storage device by the Royal Canadian Mounted Police

Follow-up on investigation into a major privacy breach at the Canada Revenue Agency and Employment and Social Development Canada

In February 2024, the Commissioner tabled a special report in Parliament with his findings and recommendations regarding an investigation on a breach affecting vast amounts of personal information. The investigation 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 and had not taken the necessary steps to promptly detect and contain the breach. Both institutions accepted all the recommendations made by the OPC and committed to their implementation within one year – by February 14, 2025.

Over the last year, the OPC has been tracking the progress that the CRA and ESDC made in implementing its recommendations following the investigation.

Both the CRA and ESDC were late in implementing some of the OPC's recommendations. The OPC will continue to engage with both institutions on the implementation of all the recommendations.

PIPEDA:
A year in review

Collaboration was a key theme of the OPC's private-sector work in 2024-2025 and included new and ongoing investigations and other compliance actions under PIPEDA that represented joint efforts with domestic and international counterparts.

Among these, the OPC initiated an investigation with its counterparts in British Columbia and Alberta into Certn, a company that offers background check services, including tenant screening services to landlords.

Commissioner Dufresne also partnered with his counterpart in the United Kingdom, the UK Information Commissioner, to launch an investigation into a data breach at 23andMe, a global direct-to-consumer genetic testing company. The Offices launched this investigation in June 2024 to leverage their combined resources and expertise to assess a breach of highly sensitive information.

In the past year, the OPC also continued work on joint investigations with provincial regulators in Quebec, British Columbia, and Alberta into the privacy practices of TikTok, in particular as they relate to children, and OpenAI, the company behind ChatGPT.

The OPC has made strides on its second strategic priority, meant to address the privacy impact of new technologies. This includes the investigations into TikTok and OpenAI, as well as an engagement with LinkedIn. In the latter case, the company voluntarily paused its practice of using the personal information of Canadian members to train its generative AI models while it worked to respond to the OPC's questions. In February 2025, in response to a complaint, the Commissioner also began an investigation in relation to X Corp.'s collection, use, and disclosure of data for AI development.

The OPC received 1,458 complaints under PIPEDA in 2024-2025, an increase of 32% over the previous fiscal year, and accepted 446. As with the increase in complaints under the *Privacy Act*, the rise in complaints under PIPEDA is not associated with a specific issue and complaints were spread out across the various categories.

At the beginning of the fiscal year, 66 investigations under PIPEDA were older than 12 months – 21% of all active investigations. By the end of the fiscal year, the backlog had declined to 41, or 14% of all active investigations. As in 2023-2024, the majority of complaints were related to the financial services sector (111) – a volume that is consistent with the past three years.

Other sectors that received high numbers of complaints were services (90) (e.g., real estate services, repair and maintenance, credit bureaus), Internet, which includes Internet service providers and online information distribution services (e.g. news, software, and mobile app publishers, directories, search portals and social media sites) (53), and sales (35) (e.g., retail, car dealerships, online sales). Most of these complaints related to how organizations collected, used and disclosed, or retained personal information, as well as challenges in obtaining access to the personal information held by the organizations.

Other investigations started in 2024-2025 that were ongoing at the time of writing include:

- In November 2024, the OPC began an investigation into the World Anti-Doping Agency (WADA), which is responsible for overseeing anti-doping programs and monitoring compliance with the World-Anti-Doping Code. The investigation was launched following the receipt of a complaint about the agency's handling of biological samples collected from athletes. The complainant alleged that WADA had disclosed personal information to international sporting federations, and that the information was being used for the purpose of assessing athletes' sex-based eligibility without their knowledge or consent and for a purpose that would not be considered appropriate under PIPEDA.

- In July 2024, after receiving several complaints from individuals alleging that they had not been able to delete their PC Optimum accounts, the OPC opened an investigation into Loblaws.

The following section highlights key outcomes under PIPEDA in 2024-2025.

Privacy by the numbers

PIPEDA

Type	Number
Complaints accepted	446
Well-founded complaints	39
Complaints closed through early resolution	331
Complaints closed through standard investigation	107
Data breach reports received	686
Advisory engagements with private-sector organizations	17

Early resolution

Early resolution continued to be an important investigative tool for resolving low-complexity, non-systemic complaints under PIPEDA.

In 2024-2025, the OPC addressed 89% of all accepted complaints under PIPEDA through either early resolution, or summary investigations, which are shorter investigations that conclude with a brief report or letter of findings. Under PIPEDA, this translates into 388 complaints closed through early resolution or summary investigations.

Percentage of all PIPEDA complaints closed in early resolution

Fiscal year	Percentage
2024-2025	76%
2023-2024	90%
2022-2023	73%
2021-2022	85%
2020-2021	71%

PIPEDA advice and outreach to businesses

Members of the OPC's Business Advisory Directorate at the 2024 Startup Canada Tour exhibit in Moncton.

The OPC provides advice to businesses to help them ensure that their initiatives and practices for managing personal information comply with PIPEDA.

The number of advisory consultations carried out with businesses seeking advice in 2024-2025, 17, was largely consistent with the previous year (16). We did see an increase in the percentage of files where businesses were seeking advice from the OPC regarding the adoption of AI, from 40% in 2023-2024, to 59% in 2024-2025. This increase was not surprising, given the fast adoption of AI technology by businesses of all sizes.

The OPC also conducted in-person and virtual presentations and privacy clinics in various regions of the country in close collaboration with innovation hubs and accelerators.

This included outreach visits to Winnipeg, Halifax, Moncton, and St. John's. OPC staff met with 200 tech startups, small and medium-sized enterprises (SMEs), new entrepreneurs and other stakeholders at various outreach events. At these, the OPC provided information and advice about PIPEDA, such as how it applies to technologies like AI, facial recognition, and third-party cloud-based data management tools.

In June 2024, the OPC also held its annual privacy forum in Toronto. The forum provides organizations, privacy professionals, and private-sector stakeholders with an opportunity to interact with federal and provincial regulators and to share perspectives on privacy and data protection matters. Members of the business community, including privacy officers in key sectors and industry associations, legal practitioners specializing in privacy law, as well as other privacy professionals, attended the event. The forum coincides with the annual International Association of Privacy Professionals (IAPP) Canada Privacy Symposium.

In addition, the OPC acquired responsibility for a new oversight function as a result of the implementation of new regulatory amendments to strengthen Canada's Anti-Money Laundering and Anti-Terrorist Financing framework in March 2025. The OPC is responsible for reviewing and approving codes of practice governing reporting entities subject to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA). The codes apply to the sharing of personal information between reporting entities without an individual's consent under section 11.01 of the PCMLTFA.

PIPEDA breaches

The number of breach reports received under PIPEDA in 2024-2025 was consistent with the previous year – from 693 to 686. Approximately 20 million individual Canadian accounts were affected by these reported breaches, which, while less than the 25 million accounts affected the previous fiscal year, remains concerningly high.

Some breaches can have an extremely wide impact – for example, a cyberattack on a third-party service provider may be counted as a single breach, but its impact could be felt across many of its client organizations.

Under PIPEDA, the largest affected sector was the financial sector. Within that sector, unauthorized access was a key issue and accounted for almost a third (172) of the unauthorized access-related breach reports that the OPC received for all industry sectors combined (555). Unauthorized access can include cyber incidents, social engineering attacks or employees misusing their access privileges.

Other sectors reporting high numbers of breaches involving unauthorized access were telecommunications (75), services (59), which can include collection agencies and credit bureaus, educational institutions and services, investigation and security services, real estate and services such as employment, travel agencies, and repair companies, manufacturing (44) and insurance (25).

The OPC also continues to see a growing trend of supply-chain attacks. These are breaches at service providers and software developers operating on behalf of client organizations that have a potential impact on clients of all the companies in the chain. For example, a breach at one service provider for the pharmaceutical industry affected more than 50 organizations in Canada.

Breaches by the numbers - PIPEDA

Top sectors by percentage of total breaches reported

Industry sector	2021-2022	2022-2023	2023-2024	2024-2025
Financial sector	20%	27%	25%	31%
Telecommunications	14%	17%	17%	12%
Services	5%	4%	8%	11%
Insurance	8%	9%	7%	7%
Manufacturing	8%	4%	7%	7%

Percentage of breaches reported by type

Breach type	2021-2022	2022-2023	2023-2024	2024-2025
Unauthorized access	65%	66%	75%	81%
Unauthorized disclosure	25%	25%	18%	13%
Loss	7%	4%	3%	3%
Theft	3%	4%	3%	3%

Joint investigation with UK counterpart into 23andMe breach

In June 2024, Commissioner Dufresne and UK Information Commissioner John Edwards launched a joint investigation into a breach at global direct-to-consumer genetic testing company 23andMe.

23andMe is a custodian of highly sensitive personal information including genetic information, like DNA, which does not change over time. DNA can reveal information about an individual and their family members, including about their health, ethnicity, and biological relationships. This makes public trust in these services essential. The investigation has enabled both offices to leverage their combined resources and expertise and reflects Commissioner Dufresne's commitment to collaboration to protect individuals' fundamental right to privacy.

Millions impacted worldwide by Ticketmaster breach

In July 2024, Commissioner Dufresne launched an investigation into Ticketmaster, following a cyber incident that reportedly affected more than half a billion users worldwide, including millions of Canadians.

The investigation is examining whether the company had adequate security safeguards in place to protect the personal information of impacted individuals and whether the company notified individuals in a timely fashion.

PowerSchool breach affects educational institutions, parents and students

In January 2025, the OPC became aware of a data breach at PowerSchool, an education technology software company used in many Canadian schools to manage student and teacher data.

OPC officials engaged with PowerSchool representatives promptly to determine whether the organization was taking appropriate steps to respond to the breach.

In February 2025, Commissioner Dufresne announced the launch of an investigation into the incident.

Highlights of other OPC work

The OPC carries out its mandate to protect and promote the privacy rights of Canadians in a number of ways.

In addition to overseeing compliance with the *Privacy Act* and PIPEDA, the OPC provides advice to Parliament, collaborates with international and domestic partners, promotes privacy-related research, creates guidance for Canadians, and pursues other communication and outreach activities throughout the year.

The following section provides an overview of the OPC's activities in these areas in 2024-2025.

Privacy by the numbers

Other work

Type	Number
Bills, parliamentary studies and draft regulations reviewed for privacy implications	4
Parliamentary committee appearances on privacy matters	8
Information requests	6,998
News releases and announcements	48
Speeches and presentations	100
Posts on X (Twitter)	407
X (Twitter) followers	19,318
Posts on LinkedIn	330
Followers on LinkedIn	35,160
Visits to website	2,790,429
Blog visits	30,914
Publications distributed	1,651

Advice to Parliament

An important part of the OPC's work is providing advice to Parliament on privacy-related legislation and other matters. In 2024-2025, the Commissioner appeared eight times before Parliamentary committees and made four submissions to government as detailed below.

When Parliament was prorogued in January 2025, all bills under consideration, including those that the OPC discussed before Parliamentary committees, died on the order paper. This included Bill C-27, which would have modernized Canada's federal private-sector privacy law by enacting the *Consumer Privacy Protection Act* and the *Artificial Intelligence and Data Act*.

The OPC will continue to advocate for modernized laws that recognize privacy as a fundamental right, while advancing the public interest and a strong Canadian economy.

In the interim, Canada's existing privacy laws continue to apply, including for new technologies such as generative AI, and the OPC remains committed to their application.

The appearances before Parliament included:

Appearance on transparency within the Department of National Defence and the Canadian Armed Forces

In May 2024, Commissioner Dufresne appeared before the House Standing Committee on National Defence on its study of transparency within the Department of National Defence and the Canadian Armed Forces. The Commissioner noted that transparency empowers citizens with the knowledge that they need to exercise their rights, and requires the government to be accountable for its handling of personal information.

Appearance on Bill C-69, the *Budget Implementation Act*

In his appearance before the Senate Standing Committee on Banking, Commerce and the Economy in May 2024, Commissioner Dufresne discussed new information-sharing provisions for reporting entities under the PCMLTFA. He said that it would be essential for the OPC to be consulted on the development of the regulations and for the OPC to have a "strong and visible" approval role.

Appearance on Bill S-210, *An Act to Restrict Young Persons' Online Access to Sexually Explicit Material*

Commissioner Dufresne appeared before the House Standing Committee on Public Safety and National Security in May 2024 on its study of a bill meant to protect young people from the harmful effects that come with being exposed to sexually explicit material online. The Commissioner supported the purpose of the bill, but noted that, as drafted, it could impose age-verification requirements even when the majority of a website's content is not sexually explicit. He proposed adding additional criteria to ensure that prescribed age verification methods are sufficiently privacy protective and offered to provide further advice concerning implementation should Bill S-210 be adopted.

Appearance on Bill C-26, *An Act Respecting Cyber Security*

In his November 2024 appearance before the Standing Senate Committee on National Security, Defence and Veterans Affairs during its review of Bill C-26, which addressed cyber security, Commissioner Dufresne advocated for the collection, use, or disclosure of personal information in the cybersecurity context to be limited to what is both necessary and proportionate. He also reiterated that the OPC should be notified of cyber incidents that may result in a material breach of personal information.

Appearance on privacy breaches at the Canada Revenue Agency

Cyberattacks at the CRA that led to more than 30,000 privacy breaches dating back to 2020 were the focus of Commissioner Dufresne's appearance before ETHI in December 2024. These breaches remain the subject of an OPC investigation and are discussed in detail in the section on breaches. Commissioner Dufresne shared his views on data breaches with the committee, noting that they represent one of the most significant threats to personal information globally.

Appearance on decision to order wind up of TikTok Technology Canada

Commissioner Dufresne appeared before ETHI in December 2024, as part of its study of the government's decision to order TikTok to wind up its Canadian business as a matter of national security. He noted that protecting children's right to privacy is a strategic priority for his Office.
A joint investigation launched by the OPC and its counterparts in Quebec, British Columbia, and Alberta in 2023 has been examining TikTok's privacy practices, with a focus on how they relate to younger users. The final joint investigation report is expected to be published in 2025.

Other advice

Submission to Justice Canada consultation on implementing protocol to international Convention on Cybercrime

In April 2024, the OPC provided feedback to a Department of Justice consultation on the Second Additional Protocol to the Convention on Cybercrime, known as the Budapest Convention, on enhanced cooperation and disclosure of electronic evidence. The OPC recommended options for stronger oversight, safeguards, and transparency.

ETHI report on government's use of tools capable of extracting personal data from mobile devices and computers

Commissioner Dufresne welcomed the report in October 2024, noting that it confirms the importance of amending the *Privacy Act* to ensure that privacy implications are appropriately considered and addressed as technologies are increasingly changing the ways in which personal information is collected, used, and disclosed by federal institutions.

Commissioner submits recommendations on proposed amendments to the *Canada Elections Act*

In a November 2024 submission to the House of Commons Standing Committee on Procedure and House Affairs, which was studying proposed amendments to the *Canada Elections Act* in Bill C-65, Commissioner Dufresne made recommendations to strengthen the bill and better protect electors' personal information. His recommendations included improving oversight provisions and requiring political parties to seek consent for the collection of personal information, and to report breaches.

Statement following release of report on oversight of social media platforms

Commissioner Dufresne welcomed a report from ETHI in December 2024 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 noted that many of the report's recommendations reflect the issues that he raised when he appeared before the Committee on the subject in 2023.

OPC review of FINTRAC's information handling practices

The OPC's biennial report on measures taken by FINTRAC to protect the personal information that it receives or collects under the PCMLTFA was tabled in Parliament in December 2024. The review found that FINTRAC has made progress to enhance and improve privacy protections since the OPC's last biennial review in 2021. That said, the review also noted that there is still outstanding work to be completed for FINTRAC to fully address previous findings and to enhance its controls and safeguards in relation to these same issues.

Submission on proposed amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*

In January 2025, the OPC provided feedback to a Department of Finance Canada consultation on proposed amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations*. The OPC provided recommendations to ensure the effectiveness of the OPC's new approval role for codes of practices under the PCMLTFA.

Public opinion research

Nine in 10 Canadians are at least somewhat concerned about privacy, and 36% are extremely concerned, according to the OPC's latest biennial Survey of Canadians.

A third said that their knowledge of privacy laws was good (27%) or very good (6%), while six in 10 Canadians said that they have good (45%) or very good (14%) knowledge of how to protect their privacy.

Approximately half of Canadians are confident that they have enough information to understand the impact that new technologies will have on their privacy. However, when it comes to those new technologies, 83% have some level of concern about their privacy when using AI tools, while 88% expressed concern about their personal data being used to train AI systems.

Nearly 9 in 10 Canadians have concerns about their privacy when using social media (87%), smartphones (86%), and other Internet-connected devices (84%), as well as when providing personal information or biometrics (85%), and engaging in online activities (87%).

How their personal information is used is also a concern – 91% expressed at least some concern about their data being used to create marketing profiles or to commit identity theft. Similarly, 87% are concerned about their information being used for decisions that impact their lives, such as employment, insurance claims, loans, or health coverage.

Each year the OPC conducts public opinion research, surveying businesses one year and individual Canadians the next, to gauge attitudes and concerns about privacy issues.

This year, an online survey targeting parents and teachers was also conducted to gauge their concern for children's privacy. The survey found that the vast majority of parents worry about their children's online privacy. In fact, two-thirds or more are moderately to extremely concerned, with 45% highly concerned about risks to their child from the use or misuse of their personal information. Additionally, 42% are highly concerned about the volume of personal information that companies collect about their children, 41% about their children's use of websites or apps intended for adults, and 37% about the volume of personal information their children share online.

Three quarters of teachers indicated that they have discussed privacy and the protection of personal information with their students. Only a third of teachers were aware of programs and resources that may assist with that task.

Protecting children's privacy

Several initiatives in 2024-2025 advanced Commissioner Dufresne's strategic priority of protecting children's privacy, recognizing the need to ensure that young people can benefit from technology without compromising their privacy and well-being.

The OPC undertook research to deepen its understanding of the privacy issues being experienced by young people, including their understanding of their privacy rights and the security of their personal information.

The project included outreach with young people, and surveys with parents, educators and other stakeholders.

The OPC also applied a children's privacy lens to enforcement activities and will leverage investigative findings – such as ongoing investigations into TikTok and PowerSchool – to inform organizations and to incentivize them to develop products and services with stronger privacy protections for children.

On the international front, in September 2024, the OPC joined a number of its counterparts in signing a joint statement on age assurance issued by the UK Information Commissioner's Office. The statement sets out principles intended to support age assurance that is accurate and effective, while ensuring user privacy. It includes a reminder that whatever age assurance method might be used, the process should be in the best interests of the child.

In March 2025, the OPC published What We Heard, a report on the responses to the exploratory consultation on age assurance launched in June 2024. The OPC sought the views of a wide range of stakeholders to inform its policy and guidance work on the development and use of age-assurance technologies.

Other OPC activities included:

- As part of the 2024 GPEN Sweep, the OPC and its provincial counterparts in British Columbia and Alberta looked at deceptive design patterns in websites and apps aimed at children.
- Focus groups with young people aged 13-17 in February 2025 to learn more about their views on their privacy rights and the harms that they face online.
- A 2024-2025 Contributions Program funding cycle targeting research proposals that focused on children's privacy.

Technology and AI

The dominance of tech giants, global digital platforms, and social media, and their impact on information and telecommunications, has transformed the landscape in which we live and work.

One of the key imperatives in the coming years will be to find the right ways of protecting and promoting individuals' fundamental right to privacy while harnessing new technological opportunities.

This is why addressing the privacy implications of technology, with an emphasis on AI, is one of the Commissioner's three strategic priorities guiding the OPC's work through to 2027.

Throughout 2024-2025, the OPC signed on to numerous collaborative initiatives related to privacy and AI through its partnerships with G7 regulators, the GPA, the Canadian Digital Regulators Forum, and provincial and territorial counterparts.

- In October 2024, the G7 Data Protection and Privacy Authorities Roundtable issued a statement on the role of data protection authorities in fostering trustworthy AI. The statement noted that just as data protection principles must be built into AI design, regulators must be included in the governance being developed around these technologies, as they are well positioned to address problems before they become systemic issues.

- A second statement from the G7 group focused on children and AI. It stated that the current generation of children will be the first to be raised in a world strongly influenced by AI. Therefore, it is important to give attention to the harms to which children might be particularly vulnerable, such as those that can come from AI tools that are able to generate content that can be manipulative, deceptive or capable of jeopardizing users' emotional states and decision-making.

- The OPC presented on privacy issues related to AI at numerous events such as the IAPP Canada Privacy Symposium and meetings of the GPA. The OPC has also been involved in the writing and publication of a terminology paper on anonymization, pseudonymization, and de-identification, as well as a Paper on Large Language Models, produced by the International Working Group on Data Protection in Technology, also known as the Berlin Group. It sets out some key data protection and privacy areas to consider in the context of generative AI.

Member of the OPC's outreach team at a conference of the Association canadienne d'éducation de langue française in Laval.

Promoting privacy

The OPC carries out its mission to protect and promote privacy rights through a variety of outreach activities.

Commissioner Dufresne, Deputy Commissioners, and OPC subject-matter experts frequently speak about their work to audiences that include students, stakeholders working in the field of privacy, federal institutions, private-sector organizations, and fellow domestic and international regulators.

The OPC also works to raise public awareness and understanding of privacy risks to ensure that children, youth, and adults are equipped to protect their personal information.

The OPC's website is an important resource for individuals, government, and private-sector organizations looking for information about rights and obligations under Canada's federal privacy laws.

In 2024-2025, the OPC published tips for individuals on how to identify the most common types of deceptive design patterns – techniques that encourage users to give away personal information online – as well as best practices for businesses to avoid deceptive design.

Another new tip sheet provided information on how to limit the risk of identity theft. This information was also shared with Canadians across the country through a radio campaign.

The OPC promoted educational resources for teachers through email campaigns and participated in exhibiting events attended by educators and librarians to support young people's privacy education.

The OPC reached out to individuals and businesses through its social media channels, publishing content for various awareness campaigns including Privacy Awareness Week, Cybersecurity Awareness Month, Small Business Week, Media Literacy Week, and Data Privacy Week.

Commissioner Dufresne, colleagues and delegates at the 62nd Asia Pacific Privacy Authorities Forum in Japan.

Commissioner Dufresne at the CPO-CIO Connect event in Ottawa.

International and domestic cooperation

Collaboration with other regulators – as highlighted earlier in this report – is a theme that is consistent across all of the Commissioner's strategic priorities given its increasing importance in today's globalized, data-driven economy.

During 2024-2025, the OPC worked closely with its domestic and international counterparts to develop a regulatory approach to one of the most important challenges of our time: the impact of technology, particularly AI, on privacy.

Collaborative initiatives included joint investigations, joint statements and resolutions, and a global sweep that explored deceptive design practices by apps and websites. The OPC worked with fellow information and privacy commissioners and ombuds from across the country to address issues of common concern, including AI modernization and freedom of information, constitutional and administrative law, neurotechnology, Indigenous concepts of privacy, youth privacy, and legislative modernization.

Commissioner Dufresne also contributed to advancing cooperation and advocating for greater privacy protection collaboratively with international privacy counterparts, including issuing joint statements with fellow G7 data protection and privacy authorities on fostering trustworthy AI and on AI and children. The OPC also presented a paper outlining how the different G7 jurisdictions define de-identification, pseudonymization, and anonymization. In addition, to advance efforts to standardize how personal information is shared between countries, Commissioner Dufresne along with GPA counterparts, endorsed resolutions that were co-sponsored by the OPC, including a resolution that calls on lawmakers, policy makers, and regulators to work toward ensuring that data transfer tools are standardized and interoperable. The OPC also worked with members of the APPA Forum on matters related to the safe transfer of personal information to promote trust and innovation, children's privacy, and artificial intelligence governance.

Matthew Boswell, Commissioner of Competition, Philippe Dufresne, Privacy Commissioner of Canada, and Vicky Eatrides, Chairperson and Chief Executive Officer, CRTC.

Canadian Digital Regulators Forum

In May 2024, Commissioner Dufresne assumed the role of Chair of the Canadian Digital Regulators Forum.

Comprised of the OPC, the Competition Bureau, the CRTC, and the Copyright Board, the Forum's purpose is to strengthen information sharing and collaboration on issues of common interest relating to digital markets and platforms.

In 2023, the Forum joined the International Network of Digital Regulation Cooperation (INDRC), which connects cross-regulatory organizations from around the world.

This year, the Forum has continued to grow its knowledge and understanding of the impacts of AI and how the technology may affect each of the members' regulatory spheres. For example, members collectively researched and developed a report on synthetic media – content generated by AI, including deepfakes.

During a workshop organized by the INDRC and the Organisation for Economic Co-operation and Development in November 2024, Commissioner Dufresne advocated for cross-regulatory cooperation and offered an overview of the issues being explored in the synthetic media paper.

The OPC's contribution to the joint report focuses on the circumstances in which consent may or may not be required, the impact on reputation due to fraud, how synthetic media will affect individuals' right to access their own personal information, and the ethical issues raised by the selling or creating of voice cloning technology that is known to be used to fool authentication systems.

Other highlights of the Forum's second year included participating in a panel at the Competition Summit in September 2024, where the members discussed the importance of taking a "whole of government" approach to digital markets. Members also talked about the work of the Forum during a panel at the IAPP Canada Privacy Symposium in Toronto.

Contributions Program

The 2025-2026 funding cycle for the OPC's Contributions Program was launched in late February 2025 under the theme, "Connected but exposed: exploring smart devices and privacy."

The OPC invited research proposals that focus on increasing knowledge and awareness about how devices collect, share, and use personal data. It also welcomed proposals that examine policy or legislative steps that can be taken to ensure that devices come with privacy built in.

The OPC received 37 research proposals by the March 24 submission deadline.

For the 2024-2025 cycle, the OPC funded proposals that focused on children's privacy and the privacy impacts of new technologies – two themes that align with Commissioner Dufresne's strategic priorities. Funded projects included a study that will evaluate PIPEDA's fitness to govern the use of emotional AI with children, and one that will explore the effects of deceptive design on user information privacy in commercial virtual reality applications.

The Contributions Program provides funding of up to $500,000 annually for innovative privacy research and public awareness initiatives that seek to better understand, and address key and emerging issues related to privacy. Individual submissions may be eligible for up to $100,000 per project.

Before the Courts

Over the past year, the OPC was involved in several litigation matters, including:

Privacy Commissioner of Canada v. Facebook, Inc. (A-129-23 & SCC 41538)

A 2019 OPC investigation 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 in 2020 under s. 15 of PIPEDA, seeking an order requiring Facebook to comply with the federal private-sector privacy law.

In 2023, the Federal Court dismissed the OPC's application. The OPC appealed this decision to the Federal Court of Appeal (A-129-23).

In September 2024, the Federal Court of Appeal allowed the OPC's appeal with costs and declared that Facebook's privacy practices between 2013 and 2015 breached PIPEDA. The Federal Court of Appeal required the OPC and Facebook to advise the Court within 90 days as to whether they agreed on the terms of a remedial order, failing which the Court would give further direction.

In November 2024, Facebook sought leave to appeal the decision to the Supreme Court of Canada (SCC 41538). At the time of writing, the Supreme Court of Canada's decision on the leave application was pending.

Further reading

Statement by the Privacy Commissioner welcoming the Federal Court of Appeal's decision on Facebook

Privacy Commissioner of Canada v. 9219-1568 Quebec et al, (T-702-25)

In February 2025, the OPC filed a notice of application with the Federal Court under paragraph 15(a) of PIPEDA for an order requiring Aylo, the operator of some of the world's largest pornography websites, including Pornhub, to take steps to bring itself into compliance with Canadian privacy law.

This application follows an investigation by the OPC that found significant problems with Aylo's privacy practices, which allowed highly sensitive intimate content to be collected, used, and disclosed on its websites without the knowledge or consent of all individuals depicted in the content.

The Federal Court has the authority to impose binding orders requiring an organization to correct or change its practices and comply with the law.

The OPC is seeking various forms of relief in the application, including:

- a declaration that Aylo contravened PIPEDA;
- an order requiring Aylo to implement clear and specific measures to ensure that meaningful consent is obtained directly from all individuals depicted in intimate content, including:
    - an order requiring Aylo to ensure that individuals appearing in intimate content are informed of, and understand the nature, purposes, and consequences of Aylo's collection, use, and disclosure; and
- an order requiring Aylo to delete and cease collecting any intimate content for which express, meaningful, and valid consent has not been obtained directly from each individual depicted in the content.

Further reading

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

Boland v. Canada (Attorney General), 2025 FC 523

In 2024, the OPC received a complaint under the *Privacy Act* from an individual alleging that a government institution had failed to adequately respond to their request for access to their personal information. The OPC found that the complaint was not well-founded, as the government institution had released all records that related to the request.

Unsatisfied with this finding, the individual filed an application for judicial review of the OPC's investigation, naming the Privacy Commissioner as respondent. The individual requested the OPC's investigation file pursuant to Rule 317 of the *Federal Court Rules*, which the OPC provided via the Certified Tribunal Record. The Privacy Commissioner was removed as respondent and replaced by the Attorney General of Canada pursuant to Rule 303 of the *Federal Court Rules*.

On March 20, 2025, the Federal Court dismissed the application for judicial review. The Court determined that the OPC's finding that the applicant's complaint was not well-founded was reasonable, and that the decision was justified, intelligible, and transparent. The Court further found that the OPC's investigation was procedurally fair, and that the applicant was aware of the case that they had to meet and had ample time to make submissions throughout the investigation.

S. v. Privacy Commissioner of Canada, (T-2142-24)

The OPC was named as the respondent in this application for judicial review challenging the OPC's decision that it lacked jurisdiction to investigate an access complaint concerning employment-related information held by a provincially regulated organization. The matter is ongoing.

Corporation of the Canadian Civil Liberties Association et al v. His Majesty the King in Right of Canada as Represented by the Attorney General of Canada, (CV-14-504139-00)

The Canadian Civil Liberties Association (CCLA) has challenged the constitutionality of sections 7(3)(c.1) and 9(2.1)- 9(2.4) of PIPEDA, alleging that they violate sections 2(b), 7, and 8 of the *Canadian Charter of Rights and Freedoms* because these provisions can allow disclosure of personal information to government institutions without meaningful oversight, accountability or safeguards. Amongst other forms of relief, the CCLA is seeking a declaration from the Court severing those provisions from PIPEDA so that they are no longer operative.

The OPC has been granted intervenor status in this proceeding to explain its role overseeing, and experience in applying, the provisions at issue. The OPC's factum is due in October 2025. A three-day hearing is scheduled to take place in December 2025, at the Ontario Superior Court of Justice in Toronto.

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	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded - Conditionally resolved	Well-founded - Deemed refusal	Well-founded - Resolved	Withdrawn	Total
Canada Border Services Agency	1		5	48		1			3		**58**
Canada Energy Regulator				1							**1**
Canada Mortgage and Housing Corporation			1								**1**
Canada Post Corporation			2	3	1	1					**7**
Canada Revenue Agency	2	1	9	36		3		1	3		**55**
Canadian Centre for Occupational Health and Safety				1							**1**
Canadian Food Inspection Agency			1			1					**2**
Canadian Forces Morale and Welfare Services / Non-Public Property and Staff of the Non-Public Funds, Canadian Forces				3							**3**
Canadian Heritage			1								**1**
Canadian Human Rights Commission	3			2							**5**
Canadian Security Intelligence Service	1		5	29	1	1			9		**46**
Canadian Transportation Agency				1							**1**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police				2							**2**
College of Immigration and Citizenship Consultants									1		**1**
Communications Security Establishment Canada				1							**1**
Correctional Service Canada			16	63	3	6	1		4		**93**

Appendix 2

Respondent	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded - Conditionally resolved	Well-founded - Deemed refusal	Well-founded - Resolved	Withdrawn	Total
Crown-Indigenous Relations and Northern Affairs Canada				3					1		**4**
Department of Justice Canada	1		2	7					1		**11**
Elections Canada / Office of the Chief Electoral Officer			1	1					1		**3**
Employment and Social Development Canada				17			2		3		**22**
Environment and Climate Change Canada				2							**2**
Financial Transactions and Reports Analysis Centre of Canada			1	3		1					**5**
Fisheries and Oceans Canada				5							**5**
Global Affairs Canada	1			7		2					**10**
Health Canada				5							**5**
Immigration and Refugee Board of Canada	2		1	3					1		**7**
Immigration, Refugees and Citizenship Canada	2		2	74					3		**81**
Impact Assessment Agency of Canada							1				**1**
Indigenous Services Canada				3							**3**
Innovation, Science and Economic Development Canada				6					1		**7**
Library and Archives Canada			1	2							**3**
Military Police Complaints Commission									1		**1**
National Defence			6	34	1	6	1				**48**
National Security and Intelligence Review Agency			1						3		**4**
Office of the Commissioner of Official Languages				1							**1**
Office of the Information Commissioner of Canada	1			1							**2**

Appendix 2

Respondent	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded - Conditionally resolved	Well-founded - Deemed refusal	Well-founded - Resolved	Withdrawn	Total
Office of the Superintendent of Financial Institutions Canada	1										**1**
Parks Canada Agency	1			1					1		**3**
Passport Canada			1								**1**
Prairies Economic Development Canada									1	2	**3**
Public Health Agency of Canada				1					1		**2**
Public Safety Canada			3	3	1	1					**8**
Public Service Commission of Canada										1	**1**
Public Services and Procurement Canada			2	2					1		**5**
Royal Canadian Mounted Police	4		17	98	1	7			4		**131**
Social Sciences and Humanities Research Council of Canada			1	1							**2**
Statistics Canada			1	3					1		**5**
Trans Mountain Corporation				1			1				**2**
Transport Canada			1	6							**7**
Treasury Board of Canada Secretariat				5							**5**
Veterans Affairs Canada	2		1	10		1			1		**15**
VIA Rail Canada				1							**1**
Total	22	1	82	496	8	31	6	1	45	3	**695**

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	**308**	**3.4**	**143**	**12.7**	**451**	**6.3**
Access	297	3.4	143	12.7	440	6.4
Correction - Notation	11	2.5			11	2.5
Privacy	**173**	**2.5**	**71**	**15.4**	**244**	**6.3**
Accuracy	2	1.1			2	1.1
Collection	16	4.6	10	18.7	26	10.0
Retention and disposal	5	3.5	5	18.9	10	11.2
Use and disclosure	150	2.3	56	14.4	206	5.6
Time limits	**265**	**1.8**	**357**	**3.5**	**622**	**2.8**
Extension notice	2	1.1	3	1.8	5	1.5
Time limits	263	1.8	354	3.5	617	2.8
Total	**746**	**2.6**	**571**	**7.3**	**1,317**	**4.6**

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

Complaint type	Count	Average treatment time (months)
Early resolved	**746**	**2.6**
All other investigations	**571**	**7.3**
Discontinued	22	16.7
No jurisdiction	1	4.6
Not well-founded	90	11.8
Resolved	16	8.5
Settled	8	9.2
Well-founded	33	11.1
Well-founded - Conditionally resolved	259	2.4
Well-founded - Deemed refusal	43	3.9
Well-founded - Resolved	96	13.4
Withdrawn	3	22.3
Total	**1,317**	**4.6**

Table 4 – *Privacy Act* breaches by institution

Respondent	Number of incidents
Canada Border Services Agency	5
Canada Post Corporation	1
Canada Revenue Agency	117
Communications Security Establishment Canada	1
Correctional Service Canada	17
Department of Justice Canada	1
Elections Canada / Office of the Chief Electoral Officer	1
Employment and Social Development Canada	410
Financial Consumer Agency of Canada	1
Fisheries and Oceans Canada	2
Global Affairs Canada	4
Immigration, Refugees and Citizenship Canada	11
Infrastructure Canada	1
Innovation, Science and Economic Development Canada	1
National Defence	3
National Film Board of Canada	1
Public Prosecution Service of Canada	2
Public Safety Canada	1
Public Services and Procurement Canada	1
Royal Canadian Mounted Police	23
Shared Services Canada	2
Transport Canada	2
Treasury Board of Canada Secretariat	1
Veterans Affairs Canada	4
Women and Gender Equality Canada (formerly Status of Women Canada)	2
Total	**615**

Table 5 – *Privacy Act* complaints and breaches

Category	Total
Accepted	
Access	387
Privacy	239
Time limits	653
Total complaints accepted	**1,279**
Closed through early resolution	
Access	308
Privacy	173
Time limits	265
Total	**746**
Closed through all other investigation*	
Access	143
Privacy	71
Time limits	357
Total	**571**
Total complaints closed	**1,317**
Breaches received	
Unauthorized disclosure	85
Loss	427
Theft	8
Unauthorized access	95
Total breaches received	**615**

*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	312	37%	34	10%	31	43%	377	29%
Correction – Notation	10	1%					10	1%
Privacy								
Accuracy	3	0%				0%	3	0%
Collection	13	2%			15	21%	28	2%
Retention and disposal	5	1%	1	0%	6	3%	12	1%
Use and disclosure	167	20%	9	3%	20	28%	196	15%
Time limits								
Extension notice	1		3	1%			4	0%
Time limits	341	40%	308	87%			649	51%
Total	**852**		**355**		**72**	**95%**	**1,279**	

*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	2024-2025
Royal Canadian Mounted Police	273	176	186	179	262	266	274
Correctional Service Canada	426	155	130	182	199	201	226
Immigration, Refugees and Citizenship Canada	59	44	47	49	131	110	136
Canada Border Services Agency	109	42	48	53	78	103	107
Department of National Defence	121	33	51	53	74	78	95
Canada Revenue Agency	79	63	40	48	79	76	82
Canadian Security Intelligence Service	24	15	16	14	13	23	70
Employment and Social Development Canada	39	25	41	26	54	32	29
Global Affairs Canada	20	19	18	11	26	21	26
Canada Post Corporation	29	4	22	45	23	20	33
Total	**1,179**	**576**	**599**	**660**	**939**	**930**	**1,078**

Table 8 – *Privacy Act* complaints accepted by institution

Respondent	Early resolution	Summary investigation	Investigation	Total
Agriculture and Agri-food Canada	1			**1**
Asia-Pacific Foundation of Canada	2			**2**
Atomic Energy of Canada Limited	1			**1**
Bank of Canada			1	**1**
Canada Border Services Agency	77	26	4	**107**
Canada Energy Regulator	1	1		**2**
Canada Mortgage and Housing Corporation			1	**1**
Canada Pension Plan Investment Board			2	**2**
Canada Post Corporation	26	4	3	**33**
Canada Revenue Agency	56	17	9	**82**
Canadian Broadcasting Corporation			1	**1**
Canadian Commercial Corporation	1			**1**
Canadian Food Inspection Agency	1		1	**2**
Canadian Forces Morale and Welfare Services / Non-Public Property and Staff of the Non-Public Funds, Canadian Forces	2			**2**
Canadian Human Rights Commission	2		1	**3**
Canadian Museum of History and Canadian War Museum			1	**1**
Canadian Security Intelligence Service	63	1	6	**70**
Canadian Transportation Agency	2		1	**3**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police	4			**4**
College of Immigration and Citizenship Consultants		1		**1**
Communications Security Establishment Canada		1	4	**5**
Correctional Service Canada	113	107	6	**226**
Crown-Indigenous Relations and Northern Affairs Canada	7			**7**
Department of Justice Canada	11	4		**15**
Elections Canada / Office of the Chief Electoral Officer	1			**1**

Appendix 2

Respondent	Early resolution	Summary investigation	Investigation	Total
Employment and Social Development Canada	23	4	2	**29**
Environment and Climate Change Canada	7	6		**13**
Export Development Canada	1			**1**
Financial Transactions and Reports Analysis Centre of Canada	3		1	**4**
Fisheries and Oceans Canada	5			**5**
Global Affairs Canada	15	10	1	**26**
Health Canada	7			**7**
Immigration and Refugee Board of Canada	3	2	1	**6**
Immigration, Refugees and Citizenship Canada	130	4	2	**136**
Indigenous Services Canada	16	1		**17**
Innovation, Science and Economic Development Canada	6	5		**11**
Library and Archives Canada	2			**2**
Military Police Complaints Commission	1	1		**2**
National Defence	59	34	2	**95**
National Security and Intelligence Review Agency		1		**1**
Office of the Commissioner of Official Languages	1			**1**
Office of the Information Commissioner of Canada	1			**1**
Parks Canada Agency	1		1	**2**
Parole Board of Canada	4	1		**5**
Passport Canada	1			**1**
Polar Knowledge Canada	1			**1**
PortsToronto	2			**2**
Privy Council Office		2		**2**
Public Safety Canada	3	2	2	**7**
Public Service Commission of Canada	1			**1**
Public Services and Procurement Canada	2	2	1	**5**

Appendix 2

Respondent	Early resolution	Summary investigation	Investigation	Total
Public Works and Government Services Canada	1			**1**
Quebec Port Authority	1			**1**
RCMP External Review Committee	2			**2**
Royal Canadian Mounted Police	152	108	14	**274**
Shared Services Canada	1		1	**2**
Social Sciences and Humanities Research Council of Canada		2		**2**
Statistics Canada	2			**2**
Trans Mountain Corporation	1			**1**
Transport Canada	11	2		**13**
Treasury Board of Canada Secretariat	3	3	1	**7**
Veterans Affairs Canada	11	3	2	**16**
VIA Rail Canada	1			**1**
Total	**852**	**355**	**72**	**1,279**

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

Table 9 – *Privacy Act* dispositions by complaint type

Complaint type	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded - Conditionally resolved	Well-founded - Deemed refusal	Well-founded - Resolved	Withdrawn	Total
Access	**13**	**1**	**59**	**321**	**4**	**15**	**4**	**1**	**30**	**3**	**451**
Access	13	1	59	310	4	15	4	1	30	3	**440**
Correction - Notation				11							**11**
Privacy	**9**	**0**	**23**	**175**	**4**	**16**	**2**	**0**	**15**	**0**	**244**
Accuracy				2							**2**
Collection	2		2	17	1	2			2		**26**
Retention and disposal			1	5		2			2		**10**
Use and disclosure	7		20	151	3	12	2		11		**206**
Time limits	**0**	**0**	**8**	**266**	**0**	**2**	**253**	**42**	**51**	**0**	**622**
Extension notice				2		2			1		**5**
Time limits			8	264			253	42	50		**617**
Total	**22**	**1**	**90**	**762**	**8**	**33**	**259**	**43**	**96**	**3**	**1,317**

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

Respondent	Not well-founded	Resolved	Well-founded	Well-founded - Conditionally resolved	Well-founded - Deemed refusal	Well-founded - Resolved	Total
Agriculture and Agri-food Canada		1					**1**
Canada Border Services Agency		35	1	15	11	2	**64**
Canada Energy Regulator					1		**1**
Canada Post Corporation		2		1	2		**5**
Canada Revenue Agency		18		14		7	**39**
Canadian Food Inspection Agency						1	**1**
Canadian Human Rights Commission						3	**3**
Canadian Security Intelligence Service		12				1	**13**
Canadian Transportation Agency		1					**1**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police		1					**1**
Communications Security Establishment Canada		1		1			**2**
Correctional Service Canada		35		83	1	7	**126**
Crown-Indigenous Relations and Northern Affairs Canada		1		1		2	**4**
Department of Justice Canada		6		1	1	1	**9**
Employment and Social Development Canada	1	5			1	4	**11**
Environment and Climate Change Canada		3		5		1	**9**
Global Affairs Canada		3		3	1	1	**8**
Health Canada		1					**1**
Immigration and Refugee Board of Canada	2	2		1		1	**6**
Immigration, Refugees and Citizenship Canada		59			3	1	**63**
Indigenous Services Canada		2		1			**3**
Innovation, Science and Economic Development Canada		1		4	1		**6**
Library and Archives Canada		1					**1**

Appendix 2

Respondent	Not well-founded	Resolved	Well-founded	Well-founded - Conditionally resolved	Well-founded - Deemed refusal	Well-founded - Resolved	Total
Military Police Complaints Commission		1					**1**
National Defence		15		24	10	2	**51**
Office of the Superintendent of Financial Institutions Canada						1	**1**
Parole Board of Canada		1					**1**
Polar Knowledge Canada		1					**1**
Prairies Economic Development Canada	1						**1**
Privy Council Office				2		2	**4**
Public Health Agency of Canada		1					**1**
Public Safety Canada					1		**1**
Public Service Commission of Canada	2	1					**3**
Public Services and Procurement Canada		1		1		1	**3**
Public Works and Government Services Canada		1					**1**
Royal Canadian Mounted Police	1	45	1	94	9	9	**159**
Shared Services Canada		1					**1**
Social Sciences and Humanities Research Council of Canada	1						**1**
Statistics Canada						1	**1**
Transport Canada		5		1		1	**7**
Treasury Board of Canada Secretariat				1		2	**3**
Veterans Affairs Canada		3					**3**
Total	**8**	**266**	**2**	**253**	**42**	**51**	**622**

Statistical tables related to PIPEDA

Table 1 – PIPEDA complaints accepted by industry sector

Industry sector	Number	Proportion of all complaints accepted
Accommodations	21	5%
Entertainment	9	2%
Financial sector	111	25%
Food and beverage	5	1%
Government	4	1%
Health	9	2%
Insurance	16	4%
Internet*	53	12%
Manufacturing	4	1%
Mining and oil and gas extraction	1	0%
Not for profit organizations	12	3%
Not specified	8	2%
Professionals	19	4%
Publishers (except Internet)	1	0%
Rental	1	0%
Sales/Retail	35	8%
Services**	90	20%
Telecommunications	23	5%
Transportation	22	5%
Utilities	2	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).
**This category includes collection agencies, credit bureaus, educational institutions and services (except universities and public schools), investigation and security services, other services (employment, office and administration, travel arrangement, personal care, repair and maintenance), and real estate services.

Table 2 – PIPEDA complaints accepted by complaint type

Complaint type	Number	Proportion of all complaints accepted
Access	109	24%
Accountability	5	1%
Accuracy	8	2%
Appropriate purposes	1	0%
Challenging compliance	6	1%
Collection	47	11%
Consent	58	13%
Correction/Notation	5	1%
Fees	2	0%
Identifying purposes	1	0%
Openness	9	2%
Retention	49	11%
Safeguards	28	6%
Time limits	51	11%
Use and disclosure	67	15%
Total	**446**	

Table 3 – PIPEDA investigations closed by industry sector and disposition

Industry sector	Early resolved	Declined to investigate	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded - Conditionally resolved	Well-founded - Resolved	Withdrawn	Total
Accommodations	18				1			2	1	1		**23**
Construction					1							**1**
Entertainment	7	1		1				1				**10**
Financial sector	59		4		6	1	3	2	2	6	1	**84**
Food and beverage	5											**5**
Government	2						1					**3**
Health	5		3		4			2	1	5		**20**
Insurance	11		2		2		1			4		**20**
Internet*	46						1	1			1	**49**
Manufacturing	5		1									**6**
Mining and oil and gas extraction	1											**1**
Not for profit organizations	2		1	2								**5**
Not specified	2											**2**
Professionals	16		2		2					1		**21**
Publishers (except Internet)	1							1				**2**
Rental	4											**4**
Sales/Retail	37						1	1			2	**41**
Services**	54		3		12	1				3	1	**74**
Telecommunications	30		1		3				1	3	1	**39**
Transportation	25				1			1				**27**
Utilities	1											**1**
Total	**331**	**1**	**17**	**3**	**32**	**2**	**7**	**11**	**5**	**23**	**6**	**438**

*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).
**This category includes collection agencies, credit bureaus, educational institutions and services (except universities and public schools), investigation and security services, other services (employment, office and administration, travel arrangement, personal care, repair and maintenance), and real estate services.

Table 4 – PIPEDA investigations closed by complaint type and disposition

Complaint type	Early resolved	Declined to investigate	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded - Conditionally resolved	Well-founded - Resolved	Withdrawn	Total
Access	84		6		8		1		1	10	1	**111**
Accountability	5											**5**
Accuracy	7		1									**8**
Appropriate purposes	1											**1**
Challenging compliance	4				4		1					**9**
Collection	24		1		1				1			**27**
Consent	50		4		9		1	1		5	3	**73**
Correction/Notation	5											**5**
Fees	1											**1**
Openness	2											**2**
Retention	38		2	1	1		1	1			1	**45**
Safeguards	23		1				1			2		**27**
Time limits	42	1	2	2	6	2	2	8	3	6	1	**75**
Use and disclosure	45				3			1				**49**
Total	**331**	**1**	**17**	**3**	**32**	**2**	**7**	**11**	**5**	**23**	**6**	**438**

Table 5 – PIPEDA investigations - Average treatment times by disposition

Disposition	**Number**	**Average treatment time** (months)
Early resolved	331	6.1
Declined to investigate	1	19.2
Discontinued	17	17.0
No jurisdiction	3	18.8
Not well-founded	32	16.8
Resolved	2	3.6
Settled	7	9.2
Well-founded	11	10.6
Well-founded - Conditionally resolved	5	16.3
Well-founded - Resolved	23	20.8
Withdrawn	6	28.0
Total	**438**	
Overall weighted average		8.8

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	84	6.4	27	21.6	111	10.1
Accountability	5	4.2			5	4.2
Accuracy	7	3.3	1	10.6	8	4.2
Appropriate purposes	1	3.7			1	3.7
Challenging compliance	4	7.3	5	9.2	9	8.4
Collection	24	5.6	3	22.5	27	7.5
Consent	50	7.1	23	18.7	73	10.7
Correction/Notation	5	3.6			5	3.6
Fees	1	6.4			1	6.4
Openness	2	2.2			2	2.2
Retention	38	4.9	7	8.9	45	5.5
Safeguards	23	6.4	4	27.7	27	9.6
Time limits	42	6.8	33	12.6	75	9.4
Use and disclosure	45	6.1	4	23.0	49	7.5
Total	**331**	**6.1**	**107**	**17.0**	**438**	**8.8**

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

Industry sector	Incident type				Total	Percentage of total incidents
	Loss	Theft	Unauthorized access	Unauthorized disclosure		
Accommodations	1		5		**6**	**1%**
Agriculture, forestry, fishing and hunting			1		**1**	**0%**
Construction			2		**2**	**0%**
Entertainment	1		4		**5**	**1%**
Financial sector	9	5	172	26	**212**	**31%**
Food and beverage			4		**4**	**1%**
Government			20		**20**	**3%**
Health	1	2	19	10	**32**	**5%**
Insurance	5	3	25	18	**51**	**7%**
Internet	1		8	1	**10**	**1%**
Manufacturing			44	1	**45**	**7%**
Mining and oil and gas extraction		1	7		**8**	**1%**
Not for profit organizations	2	1	22	11	**36**	**5%**
Not specified			1	1	**2**	**0%**
Professionals		2	22	2	**26**	**4%**
Publishers (except Internet)			17	2	**19**	**3%**
Rental			2		**2**	**0%**
Sales/Retail	1		34		**35**	**5%**
Services	2	3	59	11	**75**	**11%**
Telecommunications			75	7	**82**	**12%**
Transportation			10		**10**	**1%**
Utilities			2	1	**3**	**0%**
Total	**23**	**17**	**555**	**91**	**686**	

Table 8 – Number of Canadian accounts affected by incident type

Incident type	Number of Canadian accounts affected
Loss	1,550
Theft	5,939
Unauthorized access	18,493,588
Unauthorized disclosure	1,586,314
Total	**20,087,391**

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 *Personal 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* (the "*Act*"), and such outcomes may trigger the right to complain to the Ad Hoc Privacy Commissioner.

In the reporting year of April 1, 2024, to March 31, 2025, I handled 49 matters:

- Prior year complaints not yet concluded 1
- New complaints - withdrawn/abandoned 2
- New complaints investigated and concluded 20
- Complaints and inquiries redirected 24
- Public interest notification 2

The investigation of the privacy breach complaint of last year is continuing, given its relation to a larger, more complex case external to the OPC, but it is expected to be concluded next year.

There were many new complaints, most regarding unsatisfactory outcomes to access to personal information requests, where the OPC was not permitted to grant access due to the strict and limiting exemption to disclosure that I reported on in prior annual reports. Nonetheless, these reviews provide a necessary verification that rights of access and protection of privacy are always upheld and remain a good avenue in which to raise a greater awareness of how the *Act* applies to the OPC.

Of interest this year was a case I concluded where a complainant challenged the OPC's use and sharing of their personal information during the OPC's investigation of a complaint lodged by the individual. Navigating the handling of personal information in the context of OPC investigations was met with some challenge, as I could not be called upon to examine how decisions are derived or whether conclusions are correct. Rather, the focus remained on the manner in which the OPC officials accessed, used, and shared personal information when carrying out their investigative duties. The Treasury Board Secretariat's Policy on Privacy Protection provided a good source of practices and procedures when administering the *Privacy Act*, including the effective management of personal information by identifying and mitigating privacy risks where personal information is being collected, used, disclosed and retained, and the lawful disclosure of personal information where there is a clear need to know in order to perform duties and functions related to the *Act*.

As is the case for complaints I do investigate and for which I file written findings, I likewise take time to reply to those who require assistance for cases I cannot accept, such as inquiries and complaints. In those cases, I redirect individuals to the appropriate provincial or federal oversight offices. I enjoy providing this helpful public service and I look forward to continuing all of this important work 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