Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

2022-2023

Protecting and promoting privacy in a digital 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.

2022-2023 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

September 19, 2023

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, 2022 to March 31, 2023. This tabling is done pursuant to section 38 of the *Privacy Act* and section 25 of the *Personal Information Protection and Electronic Documents Act*.

Sincerely,

Original signed by

Philippe Dufresne
Commissioner

Letter to the Speaker of the House of Commons

September 19, 2023

The Honourable Anthony Rota, 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, 2022 to March 31, 2023. This tabling is done pursuant to section 38 of the *Privacy Act* and section 25 of the *Personal Information Protection and Electronic Documents Act*.

Sincerely,

Original signed by

Philippe Dufresne
Commissioner

Table of Contents

Commissioner's message

I am pleased to submit my Office's 2022-2023 Annual Report to Parliament, highlighting the work of the Office of the Privacy Commissioner of Canada (OPC).

This report details the important work that my Office is doing to protect and promote the fundamental privacy rights of Canadians. It covers both the *Privacy Act*, which applies to the personal information handling practices of government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Canada's federal private sector privacy law.

In the first year of my mandate as Canada's Privacy Commissioner, I promoted my vision of privacy based on 3 key pillars:

- First, privacy is a fundamental right, which means that it must be treated as a priority. It also means that in clear cases of conflict with private and public interests, privacy should prevail.

- Second, privacy supports both the public interest and Canada's innovation and competitiveness. It is not a zero-sum game between privacy rights and public and private interests; we can have both, and Canadians deserve nothing less.

- Third, privacy accelerates the trust that Canadians have in their institutions and in their participation as digital citizens. Creating a culture of privacy, and being seen to be doing so, generates trust and engagement with our public institutions, which is good for the public interest, and also sustains trust and loyalty from clients and customers, which is good for innovation and economic success.

This vision frames how I look at privacy issues, and how my Office considers and responds to the opportunities and challenges of our time in the face of unprecedented technological development. It has also shaped my Office's strategic priorities, which include:

1. keeping up with and staying ahead of technological advancements and their impact on privacy, particularly with respect to artificial intelligence (AI) and generative AI;

2. protecting children's privacy so that they can benefit from technology and be active online safely and free from fear that they may be targeted, manipulated, or harmed as a result; and

3. preparing for potential law reform should Bill C-27, the *Digital Charter Implementation Act*, be adopted by Parliament.

To implement and achieve this vision, the OPC remains committed to strong advocacy, enforcement, protection, promotion and education on an ongoing basis. We also continue to engage with privacy stakeholders and champions from across Canada representing government, businesses, civil society, consumers, academics, and equity-deserving groups, as well as with our global and domestic counterparts.

Privacy touches all aspects of our lives and world. Children's rights, competition, broadcasting, cybersecurity, democratic rights, international trade, national security, equality rights, public health, ethical corporate practices and the rule of law – all of these have important privacy implications and impacts.

The right to protect our personal information is also foundational to our individual dignity, and our ability to enjoy so many other fundamental rights and freedoms. The right to decide whether, when and how to share information about ourselves is essential – even more so in today's increasingly digital world.

We know that privacy matters to Canadians more today than ever before, and that they are concerned about the impact of technology on their privacy. Our latest survey of Canadians found that 93% have some level of concern about protecting their personal privacy, and that half do not feel that they have enough information to understand the privacy implications of new technologies.

Meanwhile, only 4 in 10 Canadians feel that businesses generally respect their privacy. Social media companies, big tech, retailers and the telecommunications industry are among the sectors that Canadians are most concerned about, according to our poll. They were also the subject of more than a quarter of the complaints that we received last year.

This is why the work that my Office is doing to both promote and protect privacy rights is so important. These figures tell us that Canadians want and need to trust that their privacy rights are being protected so that they can feel confident about participating freely in the digital economy. They also show that my Office has an important role to play because we know that organizations themselves are having to adapt to the scale and pace of technological change, and that we can help them to operate and innovate in a privacy-protective manner that will generate trust.

As you will see in the pages that follow, over the last year, my Office conducted important investigations, engaged in ground-breaking policy work, provided advice and guidance to organizations in both the public and private sectors, and played a leadership role in national and international privacy networks, consulting and collaborating with key stakeholders globally and domestically. We also provided valuable advice and recommendations to Parliament on law reform and privacy matters of public interest and importance.

The work that my Office is doing delivers concrete results that have meaningful impacts for Canadians and privacy in Canada, and I am so grateful to be working with such an impressive team in delivering on this important mandate.

I look forward to continuing our efforts to promote a better understanding of the fundamental right to privacy in Canada and around the world, to ensuring that privacy rights are respected and prioritized by government institutions and businesses alike, and to positioning Canada as a global leader on privacy.

Philippe Dufresne
Privacy Commissioner of Canada

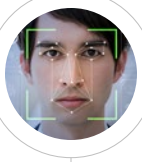
Timeline

April **2022**

Public interest disclosure guidance

OPC issues guidance for federal institutions on disclosures of personal information under paragraph 8(2)(m) of the *Privacy Act*.

May **2022**



Joint statement on facial recognition technology

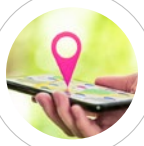
Canadian privacy regulators recommend legislators develop a legal framework that establishes clear and explicit circumstances for police use of facial recognition technology (FRT). 5 months later, OPC responds to conclusions in ETHI study on FRT.

May **2022**

OPC issues Interpretation Bulletin on sensitive information

New compliance guidance seeks to clarify what constitutes sensitive personal information and how it should be protected.

June **2022**



Results of Tim Hortons investigation released

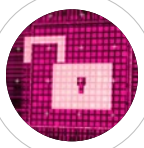
Joint investigation finds that Tim Hortons app violated privacy laws by collecting "vast amounts" of sensitive location data.

June **2022**

Philippe Dufresne appointed Canada's new Privacy Commissioner

Soon after, unveils the 3 pillars of his vision for privacy: Privacy as a fundamental right; privacy in support of the public interest and Canada's innovation and competitiveness; and privacy as an accelerator of Canadians' trust in their institutions and in their participation as digital citizens.

June **2022**



Global data protection authorities release guidance on credential stuffing

Guidance seeks to help businesses and individuals protect themselves against cyber-attacks that exploit password re-use.

July **2022**

Privacy Act Extension Order No. 3 takes effect

Foreign nationals outside Canada now have the right under the *Privacy Act* to access their personal information being held by federal government institutions.

OPC responds to CBSA consultation on proposed regulations for examining documents stored on personal digital devices

Nearly 2 months after testifying before a Senate committee on Bill S-7, the OPC offers submission highlighting procedural and accountability requirements that it believes are still missing from the Bill and should be included within the legal framework.

July **2022**

August **2022**

Privacy Commissioner testifies before Parliamentary committee studying RCMP investigative tools

Commissioner Dufresne addresses his Office's engagement with the RCMP regarding the use of covert data collection tools as well as the RCMP's obligations under Canada's federal public sector privacy law. 3 months later, Commissioner responds to committee's final report.

OPC publishes survey of Canadian businesses on privacy-related issues

Survey shows a drop in the number of businesses that have designated a privacy officer, developed internal policies for staff to address privacy obligations and put in place procedures for customers to request access to their data compared to previous survey.

August **2022**

September **2022**

G7 regulators discuss data protection and the flow of data across borders

The OPC presents a discussion paper on the de-identification of data which involves removing personal information from a data set so that individuals are less identifiable.

Domestic privacy authorities pass resolutions on securing public trust in digital healthcare and ensuring that digital ID ecosystems are designed with privacy in mind

Canadian privacy authorities call on governments to phase out use of unencrypted email and fax machines, and to ensure that the right to privacy and transparency are fully respected throughout the design, operation and ongoing evolution of a digital identity ecosystem.

September **2022**

October **2022**

OPC issues Tech-Know blog on synthetic data

Post looks at this privacy enhancing technology that dates back to the 1980s but has been playing a significant role in recent advancements in artificial intelligence and machine learning.

October **2022**

International privacy regulators endorse resolutions on cybersecurity and facial recognition during 44th Global Privacy Assembly

OPC wins award for tool developed to offer organizations an automated solution to assess if a privacy breach presents a real risk of significant harm (RRROSH) to affected individuals.

November **2022**

OPC publishes new tips for protecting web-connected cameras

Guidance seeks to help individuals keep the images gathered by web-connected cameras, such as baby monitors and home security systems, private.

December **2022**

Data protection authorities from Asia Pacific region discuss privacy issues, best practices

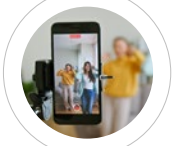
Commissioner Dufresne moderates roundtable on experiences and contributions of privacy regulators in protecting and promoting privacy during the pandemic.

January **2023**

OPC releases results of Home Depot investigation

Investigation finds that the company failed to obtain customer consent before sharing e-receipts containing personal data with Meta.

February **2023**



Commissioners launch joint investigation into TikTok

Privacy protection authorities for Canada, Québec, British Columbia and Alberta announce that they will examine whether TikTok obtained valid consent for the collection, use and disclosure of personal information from its younger users.

Privacy Act: A year in review

The COVID-19 pandemic continued to be a major factor in the OPC's work in 2022-23. We concluded a series of investigations under the *Privacy Act* relating to the pandemic and continued our consultations on a variety of pandemic-related federal programs. A Special Report to Parliament tabled in the spring of 2023 summarized much of this work, including investigations into vaccine mandates and the ArriveCAN app.

Government agencies continue to leverage digital tools and technologies put in place before the pandemic, as well as pandemic-related control measures, for ongoing and post-pandemic uses. Some of our work this year involved investigations and government engagements related to the privacy and security implications of digital tools, the use of biometrics initiatives in immigration programs and identification of travellers at the border.

The OPC continued to investigate and address privacy issues with important impacts for Canadians – such as the handling of personal information in specific employment-related matters and in relation to individuals' right of access to personal information about them held by the government. Our report highlights lessons from some of these investigations.

In most cases where the OPC identified issues or contraventions of the Act, government institutions committed to addressing the issues. However, in certain important cases highlighted below, federal institutions were unwilling to do so.

The OPC also examined its own processes for handling complaints and identified ways in which it could be more efficient and expeditious.

The *Privacy Act* celebrates its 40th anniversary in 2023. The government has expressed its intention to update this law, which was ground-breaking when passed in 1983 but has not been significantly updated since. The OPC looks forward to lending our expertise to the project of developing legislation that is responsive to our current digital reality.

The following section highlights key initiatives under the *Privacy Act* in 2022-23.

Privacy by the numbers

Privacy Act

Complaints accepted	1,241
Well-founded complaints	434
Complaints closed through early resolution	469
Complaints closed through standard investigation	530
Data breach reports received	298
New advisory consultations opened with government institutions	73
Privacy impact assessments (PIAs) received	110
Advice provided to government institutions following PIA review or consultation	74
Public interest disclosures by federal organizations	761

Government Advisory work

Members of OPC's Government Advisory Directorate at APEX 2023.

Pandemic-related initiatives

The OPC consulted closely with federal institutions on COVID-19-related programs and activities throughout the pandemic. For example, our Government Advisory Directorate consulted with Immigration, Refugees and Citizenship Canada (IRCC), the Canada Border Services Agency (CBSA), Health Canada, the Public Health Agency of Canada (PHAC) and Employment and Social Development Canada (ESDC) on files related to border health measures. Examples include quarantine case management, border testing, tracking vaccine sentiment, infection tracking and tracing and data management related to pandemic benefits and economic stimulus programs.

Some of our work involved reviewing the use of technologies and processes that were originally developed in response to the pandemic for ongoing border and immigration management.

The OPC also consulted with the Treasury Board of Canada Secretariat (TBS) on new government-wide pandemic policies, as well as with multiple institutions on how they operationalized those policies related to vaccine mandates, attestation and compliance verification. Later, our Office consulted with government on the return-to-work policy and hybrid work model and made recommendations emphasizing the need to consider privacy when developing processes to monitor workplace attendance.

Our advice has focused on ensuring that institutions had clear legal authority to collect, use and disclose personal information for COVID-19 related activities and stressed the importance of transparency to the public. For instance, the OPC recommended that all new, follow-up or ongoing uses of personal information collected for pandemic purposes be clearly described in institutional privacy impact assessments (PIAs). Our Office also stressed that the collection of personal information be necessary, proportional and time-limited. The OPC further recommended that personal information collected specifically for COVID-19 infection control and vaccination mandate purposes be purged when no longer needed.

Biometrics and facial recognition

The OPC continued to consult with the CBSA on its multi-year plan to introduce new digital tools and technologies for border management and traveller identification.

For example, our Office worked with the CBSA on various new biometrics initiatives, including pilot projects using facial recognition and digital identification credentials to verify passenger identity at boarding gates in collaboration with private-sector air carriers. The OPC also consulted with Transport Canada in its regulatory capacity on the development of a privacy framework for the use of digital identification credentials by air carriers to identify passengers boarding flights.

Similarly, our Office consulted IRCC on the increased use of digital and analytical tools in immigration and passport programs. This included consulting on an online passport application pilot project that would allow simple renewals for clients who already have a verifiable photo in the IRCC database that can be used with facial recognition technology. Finally, the OPC received and is assessing a PIA from IRCC on its adoption of remote virtual interviewing during the immigration application process.

TBS data strategy renewal

The OPC continues to provide advice to the TBS Office of the Chief Information Officer on an evolving data strategy as the federal government moves forward with its plan to promote and expand data-driven services across departments. Our Office has stressed that efforts to streamline services and increase efficiency must not come at the expense of privacy.

The OPC looks forward to continued dialogue with TBS in key areas such as de-identification, data aggregation, data for equity, Indigenous data sovereignty and automatic data processing.

Surveillance technologies

The OPC has engaged extensively with the Royal Canadian Mounted Police (RCMP) on its use of new and emerging surveillance techniques and technologies. Following media reports, it reached out to the RCMP for a briefing on its use of On-Device Investigative Tools (ODITs). Our Office noted that, despite requirements under the TBS Directive on Privacy Impact Assessment and the Policy on Privacy Protection, the RCMP had not submitted a PIA to us or notified us of the program. During an appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI), Commissioner Dufresne stressed that these obligations – currently only policies – should be codified in the *Privacy Act* with clear and binding statutory provisions. At the time of writing this report, the RCMP indicated that it was working on a PIA, which we looked forward to reviewing.

Finally, we provided feedback to the RCMP on the access, retention and safeguarding of personal information in the body-worn camera image management system.

Outreach to build privacy capacity in federal institutions

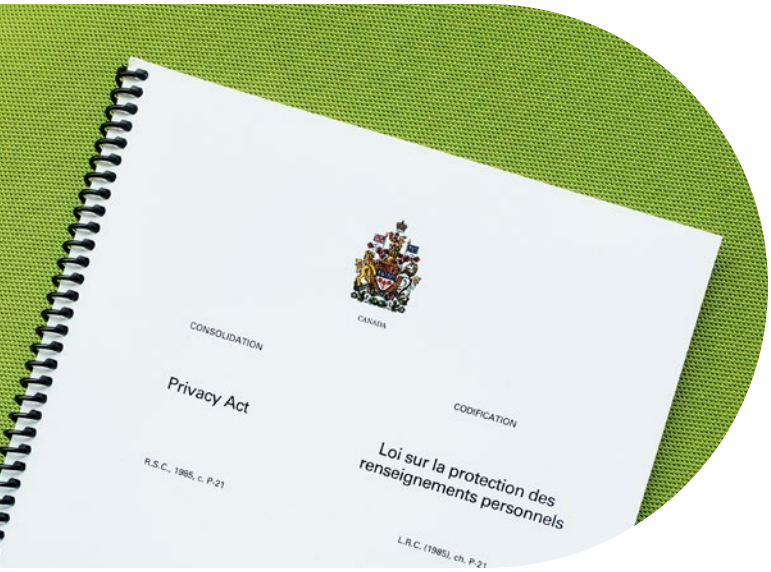
The OPC conducted several outreach and capacity-building sessions for public servants, including one on privacy as the foundation of trust in government services, which drew more than 450 participants from multiple government departments. Similarly, more than 400 public servants participated in our session on the use of artificial intelligence and biometrics, and more than 350 took part in our session on the development of PIAs.

FURTHER READING

Special Report to Parliament: Protecting Privacy in a Pandemic

Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of Device Investigation Tools Used by the RCMP

Privacy Act compliance actions



Top 10 institutions by complaints accepted	
Respondent	**Number**
Royal Canadian Mounted Police	262
Correctional Service Canada	199
Immigration, Refugees and Citizenship Canada	131
Canada Revenue Agency	79
Canada Border Services Agency	78
Department of National Defence	74
Employment and Social Development Canada	54
Public Services and Procurement Canada	36
Global Affairs Canada	26
Canada Post Corporation	23
Total	**962**

In 2022-23, the OPC concluded a series of investigations relating to COVID-19 which were described in a special report to Parliament tabled in the spring of 2023.

The number of complaints that we accepted under the *Privacy Act* in general continues to increase – in 2022-23 we accepted 1,241 complaints, an increase of 37% over the 906 accepted in 2021-22.

The federal institutions leading the list with the most complaints are the RCMP (262), Correctional Service Canada (CSC) (199), and IRCC (131), followed by the Canada Revenue Agency (CRA) (79), the CBSA (78) and the Department of National Defence (DND) (74).

Our Office received 298 reports of breaches primarily relating to the loss of personal information (44%) and unauthorized disclosure (33%).

The *Privacy Act* Extension Order No.3 came into effect in July 2022 giving foreign nationals outside Canada the right to request access to their personal information held by organizations subject to the Act, to request that the information be corrected when necessary and to submit a complaint to the OPC if those organizations did not act on their requests.

So far, the OPC has received a modest number of complaints as a result of the extension order. We continue to monitor the situation. As institutions process more requests under the order, these may evolve into complaints.

As the backlog of unassigned complaints continued to grow, this year the OPC carried out a diagnostic review of its processes to identify areas for improvement. (See text box on next page.)

FURTHER READING

Privacy Act Extension Order, No. 3

Diagnostic review tackles *Privacy Act* and PIPEDA complaint backlogs

Complaints are a critically important recourse available to Canadians to exercise their privacy rights. In 2022-23, the OPC undertook an initiative to provide Canadians with more timely resolution of complaints.

A diagnostic review helped to identify new ways to allocate resources, adjust our processing and risk protocols and enhance efficiency to address a backlog of complaints made under the *Privacy Act* and PIPEDA.

In recent years, an increasing concern among Canadians about their privacy rights and the heightened complexity of technology have impacted our ability to address complaints quickly. This has resulted in a complaint backlog. While a temporary budget increase allowed us to reduce our investigative backlog by 91% between 2019 and 2021, a new backlog of complaints emerged once that funding ended. This new backlog largely related to challenges in processing the volume of incoming complaints for assignment, which in turn, impacts the overall investigation treatment time.

The diagnostic review resulted in a number of efficiency strategies, including resource allocation adjustments, making greater use of formal powers and authorities, adjusting delegations to support timely complaint processing and exploring options for automation to help staff work more efficiently.

Our Office has already begun to implement these measures, which led to the elimination of the unassigned complaints queue by the end of the fiscal year.

Time limit investigations

Federal institutions are required to grant access to the personal information they hold about an individual when that person requests it. The OPC can be called in to investigate when they do not do so.

Our Office has been able to reduce our investigative treatment times significantly using the "deemed refusal" approach: if a federal institution does not grant access within a set period of time, we consider it to have refused access. This approach has had the positive impact of incentivizing institutions to respond to access requests in a more reasonable timeframe. When they do not, complainants have the right to take the matter to Federal Court after the OPC's investigation.

Time limit investigations treatment times	
Fiscal year	**Average treatment time in months**
2022-23	2.10
2021-22	2.91
2020-21	5.04
2019-20	7.50
2018-19	6.98

Early resolution

The OPC tries to resolve low-complexity, non-systemic cases using early resolution – a negotiated or mediated investigative approach to resolve cases efficiently with the best outcome for all involved. In these cases, our Office does not issue a formal finding.

Percentage of all complaints closed in early resolution	
Fiscal year	**Percentage**
2022-23	47%
2021-22	40%
2020-21	52%
2019-20	25%
2018-19	32%

Ensuring privacy protection in public-private partnerships

Government agencies are increasingly looking to the private sector for partnerships and innovative tools to meet specific public policy goals.

Our work in this area, such as our investigation into PHAC's use of mobility data provided by Telus and BlueDot during the pandemic, has highlighted gaps in the current legal framework and exposed a need for greater transparency in public-private partnerships.

Federal institutions that want to contract with private companies to collect personal information must do their due diligence before beginning collection. Not only must they ensure that they meet their own legal responsibilities, they ought to also make sure that the company's collection and disclosure of personal information does not contravene privacy laws such as PIPEDA.

Ongoing oversight is also important, as was highlighted in our investigation of the CBSA's use of genetic genealogy through the commercial service Family Tree DNA. Changes to the way the private company or the federal institution collects, uses and discloses personal information can affect whether a federal institution's use of a service is still compliant with the privacy obligations of both.

Finally, careful effort is needed to ensure transparency. This was highlighted in the CBSA case where our Office found that the CBSA's published "personal information bank" (PIB) descriptions did not adequately explain the personal information being collected.

The growing role of public-private partnerships creates additional complexity and risk. At a minimum, we need common privacy principles enshrined in both our public- and private-sector laws, such as limiting collection, use and disclosure of personal information without consent, necessity and proportionality and ensuring meaningful transparency about flows of personal information between the private and public sectors.

Summaries of key *Privacy Act* investigations

Special report into COVID-related investigations

Our Special Report to Parliament tabled in the spring of 2023 summarized much of our COVID-related investigative work this fiscal year, including our investigations into vaccine mandates and the ArriveCAN app.

The OPC generally found that the government's response to the pandemic complied with the requirements of the *Privacy Act*. A notable exception was the CBSA's failure to take reasonable steps to ensure the accuracy of personal information in ArriveCAN that led to approximately 10,200 vaccinated individuals being erroneously notified to quarantine in the summer of 2022.

Our Office found that the public health initiatives taken and orders given were necessary and proportional in the face of an unprecedented crisis. However, our investigation allowed us to highlight practices that can and should be applied to any potential future crisis to both ensure and elevate privacy protections. Our report identified shortcomings in the government's transparency with the public, as well as gaps with respect to its assessment and documentation of necessity and proportionality for COVID-19 vaccine mandates – both in terms of assessing and documenting potentially less privacy invasive alternatives, and in terms of clarity about the objectives that the mandates were trying to achieve.

FURTHER READING

Special Report to Parliament: Protecting Privacy in a Pandemic

Canada Post fails to seek and obtain Canadians' authorization before monetizing personal information for marketing

A complaint led the OPC to investigate a Canada Post program that involves building marketing lists from various sources, including information about the shopping habits of millions of people gleaned from envelopes and packages that the postal service delivers to homes across Canada.

Under the Smartmail Marketing Program, advertisers can select "targeting attributes" for mail marketing lists at the neighbourhood level, postal code level or household level. On its website, Canada Post indicates that it can prepare marketing lists based on 1,200 available targeting attributes in categories such as demographics (for example, marital status, ethnicity), interest and behaviours (for example, golf enthusiasts, loyalty card holders) and life stage and lifestyle (for example, families with children, outdoor adventurists).

The OPC's investigation focused on Canada Post's reliance on the complainant's personal information collected from the outside of mail envelopes for the Smartmail Marketing Program. We found that this did not comply with the *Privacy Act* in that Canada Post is indirectly collecting and using personal information without the knowledge or authorization of the individual whose personal information is collected.

We found that Canada Post was required to seek authorization from Canadians before gathering and selling their personal information for marketing purposes.

The *Privacy Act* generally requires federal institutions to collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates.

Canada Post claimed that it was not using the information for administrative purposes and that individuals were implicitly authorizing the collection of information from their mail by not using an opt-out feature on the Canada Post website.

The OPC rejected those arguments and recommended that Canada Post stop using and disclosing personal information from its operational data for mail marketing activities until it could seek and obtain Canadians' authorization.

As a result of our investigation, Canada Post undertook to implement some transparency-related measures, such as updating online information about the initiative and adding brochures at retail outlets. However, these efforts only target individuals who proactively seek out the information. The OPC proposed a mail-out informing individuals of the program and offering an easy way to opt out as a solution that would satisfy our recommendation.

The *Privacy Act* does not provide the OPC with order-making powers. Our Office therefore continues to recommend that Canada Post suspend this practice until it has sought and obtained Canadians' authorization for the use of their personal information to support this third-party commercial marketing program.

FURTHER READING

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

CBSA contravened *Privacy Act* with use of genetic genealogy tool

In 2017, the CBSA sought to determine the nationality of a permanent resident of Canada in order to deport him. The CBSA obtained the individual's consent to collect a DNA sample, and then sent it to the genetic genealogy company Family Tree DNA in an unsuccessful attempt to identify relatives of the complainant and confirm his nationality. The complainant argued that this contravened his rights under the *Privacy Act*.

The OPC's investigation determined that while the CBSA did make efforts to seek the complainant's informed consent, it did not provide the complainant with key information, and therefore lacked valid authorization to collect information about him from Family Tree DNA.

We found that the CBSA also contravened the Act by disclosing personal information about the complainant to many Family Tree DNA users, both unnecessarily and on an ongoing basis. Moreover, the CBSA did not conduct a PIA before undertaking the activity, contrary to Treasury Board policy. The CBSA has since put a moratorium on its use of genetic genealogy services, and has either closed the Family Tree DNA accounts or released them to the individuals.

Our investigation report includes important lessons for law enforcement's use of biometrics generally, and genetic genealogy specifically. The OPC expects law enforcement agencies to be mindful of these important implications as they consider future use of such technologies. The special sensitivity of genetic information in a law enforcement context was recognized by lawmakers in 1997 when the *DNA Identification Act* came into force, but this does not cover the use of commercial genealogy services. The OPC encourages the government to engage in a public discussion regarding the risks and benefits of novel types of DNA use, including genetic genealogy, in a law enforcement context.

FURTHER READING

Investigation into the Canada Border Services Agency's use of genetic genealogy to try to determine country of origin for the purpose of removing a long-term detainee

CBSA disclosed too much information about an access to information requester

In response to a complaint, the OPC found that the CBSA disclosed too much information about an access-to-information requester in its ultimately unsuccessful submission to the Office of the Information Commissioner of Canada for permission to decline to respond to the individual's access requests.

Unless another disclosure authority is applicable, the *Privacy Act* requires that disclosures without an individual's consent be for the same purpose for which the personal information was originally collected by the institution or for a use consistent with that purpose.

Our investigation found that information the CBSA disclosed about the requester's history of making access requests was for a "consistent use" with the original purpose of collection (that is, to manage the CBSA's responses to those access requests) and was therefore permissible. However, we found that the disclosure of sensitive information originally collected and created by the CBSA for other purposes (and subsequently sent to the CBSA's access to information and privacy (ATIP) unit to respond to the requester's access requests) contravened the disclosure provisions of the Act given it was not for a consistent use.

After we issued the final report of the investigation, the CBSA agreed to update its guidance on disclosures for a consistent use in light of the age of its existing guidance. However, the CBSA disagreed that it had contravened the Act and did not commit to modifying its practices with respect to any future similar disclosures.

FURTHER READING

Investigation of a disclosure of personal information by Canada Border Services Agency to the Information Commissioner of Canada in support of a request pursuant to section 6.1 of the Access to Information Act (ATIA), to decline to act on 2 ATIA requests

Failure to publish a personal information bank description contravenes *Privacy Act*

The OPC investigated a complaint related to the handling of personal information under Transport Canada's Zero-Emission Vehicle (iZEV) Program, launched in May 2019.

The complaint involved multiple concerns related to the collection of the complainant's personal information. Our investigation determined that provisions of the *Privacy Act* relating to personal information banks (PIB) were contravened.

Under the Act, government institutions are responsible for ensuring that all personal information under their control that is used to make decisions about individuals is included in a PIB. The Treasury Board Secretariat is responsible for approving PIBs and ensuring their descriptions are included in a public "index of personal information." These requirements are key to accountability and transparency for government institutions that collect personal information. In this case, Transport Canada did not submit a PIB description to TBS for approval until 19 months after the program was launched. More than 2 years after, when our Office issued its final report on the investigation, TBS had still not approved it. Therefore, the complaint was well-founded.

FURTHER READING

Investigation into Transport Canada's processing of personal information under the iZEV Program, and the Treasury Board Secretariat's pending approval of the program's personal information bank (PIB)

Correctional Service Canada improperly collected information from Facebook

The spouse of a former CSC employee complained to the OPC that the agency improperly collected information from their Facebook page.

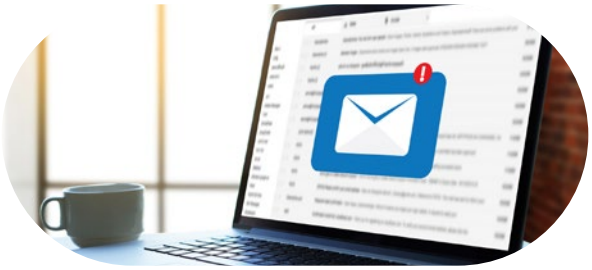
The employee's manager had been advised that the employee had been seen in photos on Facebook suggesting that the employee may have been in contravention of the COVID-19-related leave policy. The manager subsequently copied and internally circulated material from the employee's spouse's public Facebook page to seek clarity as to whether to take any related actions.

Our investigation found that a significant portion of the material collected was personal information of the complainant that had no bearing on the validity of the CSC employee's leave claims. We therefore determined that the collection contravened section 4 of the Act, which requires that personal information collected be related directly to an operating program or activity of the institution. CSC agreed to implement our recommendation to provide guidance to managers on processes to follow before collecting information in a labour relations context, in order to reduce the risk of the incidental collection of unrelated personal information of third parties.

CSC argued that the information was publicly available, however, as our Office reminded CSC, the collection-related limitations and obligations under the *Privacy Act* apply regardless of whether information is publicly available.

FURTHER READING

Investigation of Correctional Service Canada's collection and disclosure of an individual's personal information from Facebook related to an employee's 699-leave



Immigration and Refugee Board disclosed sensitive medical information to an employee's management team without consent

The incident occurred when a fitness to work report from a medical examiner contracted by the Immigration and Refugee Board (IRB) was shared in unredacted form with the employee's management team by human resources. The report included intimate personal and sensitive medical information. The TBS Occupational Health Evaluation Standard in place at the time specified that confidential medical information should not be provided to the employer unless (i) it is required to determine an appropriate accommodation and (ii) it is done with the written consent of the individual. Our investigation found that neither condition was met in this case and that this disclosure to the employee's management team therefore contravened the *Privacy Act*.

Despite our findings, the IRB declined to issue an apology to the individual for its error, or to deliver enhanced training as recommended to reduce the risk of future occurrences.

Labour relations can be complex, and errors, including high-impact ones as in this case, can occasionally occur. Acknowledging such errors, committing to learn from them and apologizing in a meaningful way to individuals harmed by such errors are key steps to demonstrating a commitment to privacy compliance. The OPC reiterates its recommendation that the IRB take meaningful action to remedy this *Privacy Act* contravention.

FURTHER READING

Investigation of a disclosure of the complainant's fitness to work report, including intimate personal and sensitive medical information, to their management team within the Immigration and Refugee Board of Canada

Privacy Act breaches

In the public sector, breach reporting is mandatory at the policy level, but not required by law as it is in the private sector.

In 2022-2023, the number of reported public-sector breaches dropped by 36%, to 298, from 463 reported in the previous year.

As in past years, the OPC continues to receive most of the reports from the same federal institutions, with the number of breaches reported by the public sector fluctuating year to year. Our Office remains concerned about under-reporting, as many of the government institutions subject to the *Privacy Act* that handle sensitive personal information have never reported a breach to us.

Nearly half of the breaches reported – 44% – cite the loss of personal information, including 134 reports from ESDC of lost passport files. Another 33% of breaches reported resulted from unauthorized disclosures, with the majority caused by employee errors –– for example, using the "CC" field instead of the "BCC" field in mass emails, misdirected correspondence and mishandling information.

Unauthorized access was a factor in 22% of the breaches reported involving employees accessing information without access privileges, misusing privileges to access information or falling for social engineering ploys.

Whether unintentional or malicious, these kinds of errors demonstrate the need to strengthen the implementation of privacy policies by ensuring that employees who deal with sensitive personal information are properly trained and that technological safeguards are implemented in a timely manner.

Only 1 reported public-sector breach involved a cyber-attack. This contrasts markedly with the private sector, where 278 cyber breaches were reported last year. As our Office has noted in past reports, the OPC has concerns about the under-reporting of cyber-attacks involving personal information, particularly in light of the Communications Security Establishment reporting that it blocks billions of cyber attempts per day against Government of Canada networks.

Further, a recent report of the Auditor General of Canada on the Cybersecurity of Personal Information in the Cloud indicated "cyber security breaches are on the rise, and strong controls to prevent, detect and respond to them can reduce the risk of breaches and limit compromises of Canadians' personal information when they do occur." Reporting breaches to our Office allows organizations to benefit from our expertise in addressing and mitigating breaches involving personal information.

Top 5 institutions by breaches reported	
Institution	**Breaches reported**
Employment and Social Development Canada	196
Canada Revenue Agency	30
Correctional Service Canada	14
Public Service Commission of Canada	10
Immigration, Refugees and Citizenship Canada	7

Privacy Act breach-related investigations

IRCC email breach creates risk of harm

Hundreds of individuals seeking guidance on emergency measures relating to the devolving situation in Afghanistan were put at risk when the IRCC erroneously included their email addresses in the "TO" field instead of the "BCC" field of its email response. The disclosures affected 636 individuals, and included their email addresses, in certain cases a thumbnail photo, along with the fact that they had inquired about emergency measures. In the circumstances, all of this constituted sensitive information.

While the department took immediate steps to mitigate the effects of the breach, the risk of significant harm to these individuals could not be fully eliminated.

The OPC found that the IRCC took positive steps to reduce the risk of a similar incident, including revising its email procedures, integrating a "2 pairs of eyes" rule, and instituting a webform to provide a secure method of communication with the department.

Our report underscored to the IRCC that it must have robust protections and procedures in place to ensure that a human error would not result in a breach. The IRCC has since implemented technological measures to mitigate the risk of misdirected email correspondence and to ensure the protection of client information. The OPC is satisfied with the IRCC's response.

FURTHER READING

Investigation into a privacy breach at IRCC

TBS breach of Phoenix information reveals assessment concerns

TBS sent 2 mass emails in error to approximately 400 individuals who had filed claims for "severe Phoenix impacts." This claims process is available to individuals who, because of Phoenix pay issues, experienced severe personal or financial hardship. The recipients' email addresses were in the "CC" field, thereby visible to all other recipients.

Twenty individuals filed complaints with the OPC. Several complainants indicated that they had not previously shared with others that they had suffered Phoenix-related hardships and that being exposed by this breach was both humiliating and stressful.

Our investigation found that TBS had contravened the *Privacy Act*, in that the disclosure of personal information was not authorized.

TBS did not report the breach to our Office, having concluded that it was not material and could not be expected to cause serious injury or harm to those affected. We disagreed with TBS. We found that a proper assessment of harm needs to be holistic, taking into consideration a broad range of factors, including, at a minimum, the recipient(s) of the breached personal information, the sensitivity of the personal information involved, and the probability that the personal information has been, is being, or could be misused. We recommended that TBS remind staff of their obligation to properly handle personal information and that it explore more secure means of communicating with stakeholders. TBS accepted these recommendations.

We also recommended that TBS incorporate our findings in its policy and guidance instruments to more consistently and accurately assess the harm and the materiality of breaches. In response, TBS stated that it published significant updates to the policy suite on privacy protection in October 2022. While the OPC welcomes many of the policy changes, we remain concerned with the interpretation of the materiality and the conduct of harm assessments.

Given TBS's leadership role, we would have expected TBS to have recognized and acknowledged the materiality of this breach under either its old or new policy definitions and we encourage them to incorporate such analysis into its policy instruments.

FURTHER READING

Investigation into complaint that TBS improperly disclosed personal information via email

Compliance monitoring unit activities

The OPC's investigative reports of finding often include recommendations to bring institutions into compliance with applicable privacy legislation.

Depending on the recommendations, the OPC uses its formal compliance monitoring function to ensure that institutions have met or are able to meet commitments made to our Office. The timeframes for implementing recommendations can vary, with the total caseload of the compliance monitoring unit typically including files from past years that are still active.

In 2022-23, 8 new *Privacy Act* files were directed to the unit.

The *Privacy Act* files closed in 2022-23 include the following:

RCMP use of facial recognition technology

Branches of the RCMP, including its new National Technology Onboarding Program and the Access to Information and Privacy Branch, actively engaged with the OPC after our Office investigated the RCMP's use of Clearview AI's facial recognition technology.

Ultimately, the OPC was satisfied that the RCMP had implemented our recommendations and taken positive steps towards creating a culture that embraces compliance when onboarding new technologies that collect personal information.

FURTHER READING

Police use of facial recognition technology in Canada and the way forward - Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology

Passport protection practices

A 2021 examination by our Office identified several ways to improve the management of documents in the Passport Program. IRCC, ESDC, Global Affairs Canada and Canada Post worked together to implement our recommendations, resulting in, among other measures, common guidance for assessing whether a passport breach needs to be reported.

FURTHER READING

Review of passport protection practices of 4 federal institutions

PIPEDA:
A year in review

The investigations that our Office undertakes under PIPEDA range from interactions between small businesses and individuals – for example, landlords and tenants – to the manner in which global organizations treat the personal information of millions of users.

High-profile investigations completed in 2022-23 involved Tim Hortons' collection and use of geolocation data via its mobile app, and Home Depot of Canada Inc's disclosure of in-store customers' purchase-related information with Meta Platforms Inc., which owns Facebook.

Along with our counterparts in Quebec, British Columbia and Alberta, the OPC launched an investigation into TikTok to examine whether the company obtained valid consent, in particular from its many younger users.

In early April 2023, the OPC also announced an investigation into OpenAI's information handling practices via ChatGPT, its artificial intelligence-powered chatbot, following a complaint. In May, the OPC broadened the scope of the investigation and indicated that it would now be a joint Commissioner-initiated investigation with our provincial counterparts in British Columbia, Alberta and Quebec.

In all investigations, our focus remains on the need to protect Canadians' fundamental right to privacy and to foster increased trust in the Canadian digital economy by helping private-sector organizations comply with privacy law. To that end, our Office also conducts outreach activities to help businesses better understand their obligations under the law.

The following section highlights key outcomes under PIPEDA in 2022-23.

FURTHER READING

- Tim Hortons report of findings
- Commissioners launch joint investigation into TikTok
- OPC launches investigation into ChatGPT
- OPC to investigate ChatGPT jointly with provincial privacy authorities

Privacy by the numbers

PIPEDA

Complaints accepted	454
Well-founded complaints	19
Complaints closed through early resolution	282
Complaints closed through standard investigation	102
Data breach reports received	681
Advisory engagements with private-sector organizations	15

PIPEDA compliance actions

This year, our Office received and accepted 454 complaints under PIPEDA, an increase of 6% over the previous year. Most of the complaints were against businesses in the financial sector (116) and the Internet (55) and telecommunications industries (38), while the top complaint category was access to personal information.

Percentage of all complaints closed in early resolution	
Fiscal Year	**Percentage of complaints**
2022-23	73%
2021-22	85%
2020-21	71%
2019-20	69%
2018-19	63%

Our Office closed 384 complaints in 2022-23, up from 358 in 2021-22.

The OPC resolved 73% of complaints through early resolution.

While our Office continues to work on improving treatment times, faced with increasingly complex complaints and constrained investigative resources, our investigative backlog grew, and our overall treatment times for PIPEDA cases increased by 18% in 2022-23 to 9.2 months, from 7.8 months the previous year.

As mentioned earlier in this report, a diagnostic review of our investigative processes has helped us to determine what improvements can be made to increase efficiencies and mitigate against complaint backlogs.

For more details, please see Diagnostic review tackles *Privacy Act* and PIPEDA complaint backlogs.

PIPEDA investigations

Home Depot shared customers' information with Meta without consent

Our investigation into Home Depot's information-sharing practices serves as a reminder to businesses to obtain valid consent before sharing customers' personal information.

In this case, an individual complained to our Office after finding out that Meta Platforms Inc. – the owner of Facebook – had information related to in-store purchases that he had made at Home Depot.

Home Depot confirmed that when a customer provided an email address in order to receive an e-receipt for in-store purchases, Home Depot forwarded the encoded email address and some purchase details to Meta through a business tool known as "Offline Conversions." If the customer had a Facebook account, Meta would compare purchase information to ads delivered to that customer on Facebook to measure the effectiveness of those ads. Meta provided aggregated results of the analysis to Home Depot and was also able to use the customer's information for its own purposes, including targeted ads.

Our Office found that customers would not reasonably expect their information to be shared with a third party, and that the retailer should have obtained express opt-in consent.

Home Depot was cooperative with our investigation. It committed to implement our recommendations and

discontinued the use of the Offline Conversions tool in October 2022.

FURTHER READING

Investigation into Home Depot of Canada Inc.'s compliance with PIPEDA

Statement by the Privacy Commissioner of Canada following an investigation into Home Depot of Canada Inc.'s compliance with PIPEDA

Early resolution success story

Early resolution is an integral investigative tool used by the OPC to resolve complaints of a less systemic nature with greater efficiency and expediency. Where possible, the OPC tries to resolve complaints using negotiation or mediation techniques that, in our experience, generally provide the optimal outcome for the parties involved. In these cases, our Office does not issue a formal finding.

Here is an example of a case that was resolved this year using this approach:

Respondent reminded of proper procedure for responding to access requests

The complainant was unsatisfied with their landlord's response to an access request, saying that the landlord had omitted a series of video recordings that they were seeking.

The landlord advised that the employee who would have handled this request had departed. The landlord processed the request and apologized to the complainant for the nature of its previous responses. The landlord also implemented additional mandatory training for all staff.

The complainant considered this to be a satisfactory resolution.

PIPEDA breaches

The OPC received 681 breach reports affecting millions of Canadian accounts in 2022-2023, approximately 6% more than the previous year (645).

With so many businesses active online, our Office suspects that many breaches go unreported – even undetected – particularly by small- and medium-sized enterprises, which represent nearly 90% of the businesses in Canada.

Top 5 sectors by percentage of total breaches reported				
Industry sector	**2019-20**	**2020-21**	**2021-22**	**2022-23**
Financial	19%	22%	20%	27%
Telecommunications	17%	14%	14%	17%
Professional services	4%	8%	12%	14%
Sales and retail	14%	10%	8%	9%
Insurance	11%	9%	14%	7%

Unauthorized access accounted for 66% of all breach reports received (451). More than half of these, 278, were said to be cyberattacks initiated through malware, compromised credentials, or phishing schemes that allowed bad actors access to systems. The financial and professional services sectors were the most frequently targeted. Breaches in this latter sector often involved sensitive personal information such as social insurance numbers.

The harms to victims resulting from cyberattacks include financial loss, identity theft and reputational harm, as well as emotional distress.

The OPC advises organizations to make security a priority in order to guard against exposure to bad actors. Important security measures include enhancing protections for employee credentials, applying security patches as they become available, requiring two-factor or multi-factor authentication, and investing in cybersecurity to prevent unauthorized access.

Unauthorized disclosure, which can include misdirected correspondence, mishandling of data or a data entry error, accounted for 171 reports, or 25% of all reports received.

Percentage of breaches reported by type				
Breach type	**2019-20**	**2020-21**	**2021-22**	**2022-23**
Unauthorized access	59%	64%	65%	66%
Unauthorized disclosure	21%	28%	25%	25%
Theft	9%	5%	3%	4%
Loss	11%	3%	7%	4%

Lack of security program leads to breach of agricultural sales companies

Our investigation into a breach involving a group of agricultural sales and services companies demonstrates the need for businesses of all sizes, even those that are not focused on personal data, to dedicate attention to securing personal information under their control.

A malicious actor used valid administrator credentials to breach the systems of Agronomy Company of Canada Ltd. Because the systems of multiple Agronomy affiliates were amalgamated, the hacker was able to move throughout the network to exfiltrate client information and then install ransomware. Agronomy did not detect the intrusion until its systems had been encrypted.

When Agronomy refused to pay the ransom, its client information was put up for online auction on the dark web, before being freely released. Without a standard information management structure, Agronomy required a third-party e-discovery provider to analyze the breached dataset, taking it 8 months to confirm that the personal information of 845 clients, including names, birthdates, social insurance numbers and banking information – information collected through individual account creation forms – was affected.

Our investigation found numerous gaps in Agronomy's safeguards, including the lack of an overarching security management framework. Additional specific gaps included the storing of sensitive personal information in shared folders without internal access controls, and a lack of security tools for intrusion detection, prevention and response.

Agronomy implemented, or agreed to implement, measures to address these deficiencies, including by separating internal networks, using various third-party security services and tools, providing ongoing training to employees and creating an incident management plan. We therefore found this aspect of the complaint to be well-founded and conditionally resolved.

Small-to-medium-sized enterprises may not have in-house capacity to protect against ever-evolving cyber-threats, but service providers and automated tools can assist in adequately protecting clients' data, and in complying with PIPEDA.

With respect to other allegations raised by the complainant, we found that the company lacked key accountability measures, such as the designation of a privacy officer and implementation of certain safeguard-related privacy protocols, but that it had ensured valid consent to collect and use the complainant's personal information for the purpose of extending credit to the complainant.

FURTHER READING

Investigation into Agronomy's privacy practices related to safeguards, accountability and limiting collection of personal information

Charity needs express consent to share donors' personal information

The OPC received a complaint that a registered charity had contravened PIPEDA by failing to obtain a donor's opt-in consent before sharing their name and address in a donor list trading program. The complainant asserted that an opt-out check box on the charity's mail-in donation form was inadequate.

While charitable activities often fall outside our Office's jurisdiction, the sharing of donor lists in this case constituted a commercial activity covered by PIPEDA.

The charity said that the program provides not-for-profit organizations with an important way to reach potential donors. Organizations receiving donor information – including name and mailing address – are to use it only once to contact the individual by mail to solicit donations.

The OPC found that while donors' names and addresses did not constitute sensitive personal information in the context of the broad-based charitable organization in question, the sharing of that information would fall outside donors' reasonable expectations. The OPC also found that the information provided by the charity about the program was not sufficient to support meaningful consent.

Our Office recommended that the charity seek opt-in consent from donors, including by providing clear information on its donor form about what information would be shared and with whom. The charity agreed to implement our recommendation and later elected to exit the donor list sharing program.

FURTHER READING

Opt-in consent required for a donor list trading program

Deputy Commissioner Brent Homan receiving the Global Award for Innovation at the 44th Global Privacy Assembly meeting in Istanbul, Türkiye for the RROSH tool.

Breach tool launched

Organizations often have difficulty determining whether it is reasonable to believe that a privacy breach creates a real risk of significant harm (RROSH) to an individual, which would require reporting to the OPC.

Our Office has developed a tool to guide risk assessments. This tool is a desktop app that asks a series of questions to help determine whether it is reasonable to believe that a privacy breach creates a risk of significant harm. It does not replace human judgment, but it does provide data to inform that judgment.

The first phase of the RROSH tool was launched internally in March 2022, with a release to selected external stakeholders in 2023. Following this pilot, our Office will develop a public version of the tool, which will promote consistency and assist industry and privacy professionals in their assessment of risks flowing from a breach.

The RROSH tool received the Global Award for Innovation at the Global Privacy Assembly meeting in Istanbul, Türkiye in October 2022.

Compliance monitoring unit activities

When private-sector organizations have signed binding agreements or undertakings with the OPC or have agreed to implement our recommendations following an investigation, it is important that our Office follows up to ensure that the appropriate steps have been taken to meet these commitments.

Our compliance monitoring unit is responsible for verifying whether commitments made are being addressed according to established timelines. In 2022-23, 4 new PIPEDA files were directed to the unit.

Files closed in 2022-23 include:

Desjardins implements a plan to protect personal information

A breach at Desjardins that occurred between 2017 and 2019, and compromised the personal information of 9.7 million accounts of people in Canada and abroad, led to a coordinated investigation by the OPC and Quebec's Commission d'accès à l'information. The investigations culminated with each Office making recommendations to Desjardins to strengthen the management of personal information under its care.

The OPC is satisfied with the actions taken by Desjardins to implement our recommendations, including those related to improvements to information security, and a data retention and destruction schedule. The report from an independent auditor indicated that the controls implemented by Desjardins comply with international standards for information systems security and privacy and are also in line with the OPC's recommendations.

FURTHER READING

Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019

MGM Resorts breach response framework

The OPC conducted an investigation into whether MGM Resorts, a U.S.-based entity that owns and operates a number of hotels and casinos located in the United States, had adequately complied with its mandatory reporting obligations under PIPEDA with respect to a breach that affected nearly 2 million Canadians. Our Office found that MGM had failed to comply with its reporting obligations. In response, MGM committed to amending its privacy breach response framework.

The OPC was satisfied that the organization implemented our recommendations. MGM has said that when it learns of a breach that may affect Canadians, it will promptly assess the breach, consistent with guidance published by the OPC, provide a report as soon as possible to our Office and notify affected individuals as soon as feasible if it is determined that there is a real risk of significant harm to affected individuals.

FURTHER READING

Investigation into MGM breach highlights how to assess risk, and need for timely assessment

PIPEDA advice and outreach to businesses

A member of OPC's Business Advisory Directorate at a business exhibit.

The OPC provides practical advice, on a confidential basis, to businesses on their practices and initiatives with significant impact on the privacy of Canadians, to help businesses comply with PIPEDA as they innovate and grow.

In addition to carrying out advisory consultations requested by businesses subject to PIPEDA, the OPC's Business Advisory Directorate also conducts privacy clinics for small and medium-sized enterprises to help them mitigate privacy risks early.

As part of our outreach to business, we created an interpretation bulletin on sensitive information that summarizes general principles for identifying and handling personal information that have emerged from court decisions and the Commissioner's findings to date.

Our Office released the results of our latest survey of businesses on privacy-related issues, which we conduct every 2 years. Fewer companies responding to this survey reported having a privacy policy, and the percentage of companies that provide privacy training has also fallen.

The OPC shares information on our research into cutting-edge technology issues through our Tech-Know blogs. Recent blogs include one on the use of synthetic data as a de-identification technique, and one that explores whether algorithms can achieve the same degree of fairness as an ethical human.

FURTHER READING

Interpretation bulletin: Sensitive Information

2021-22 Survey of Canadian businesses on privacy-related issues

Privacy Tech-Know blog: When what is old is new again – The reality of synthetic data

Privacy Tech-Know blog: When worlds collide – The possibilities and limits of algorithmic fairness

Highlights of other OPC work

Advice to Parliament

The OPC offers advice to Parliament on privacy-related matters through correspondence with Parliamentarians and appearances before House and Senate committees. In the past year this has included:

Bill C-27 submission - The *Digital Charter Implementation Act, 2022*

The OPC submitted its views and recommendations on Bill C-27, the government's proposed new private-sector privacy law, the *Consumer Privacy Protection Act*, to the House Standing Committee on Industry and Technology in May 2023.

Commissioner Dufresne called the proposed Bill a step in the right direction but said that it can and must go further in order to protect fundamental privacy rights, while also supporting the public interest and innovation.

To that end, the OPC made 15 recommendations to improve and strengthen the proposed law, including protecting children's privacy, expanding the list of violations that qualify for financial penalties, providing a right to disposal of personal information even when a retention policy is in place and requiring organizations to build privacy into the design of products and services in order to create a culture of privacy. The OPC also called for a streamlining of the process

Privacy by the numbers

Other work

Bills and parliamentary studies reviewed for privacy implications	36
Parliamentary committee appearances on private-and-public sector matters	5
Information requests	4,325
News releases and announcements	59
Speeches and presentations	57
Posts on X (Twitter)	863
X (Twitter) followers	20,330
Posts on LinkedIn	528
Followers on LinkedIn	27,545
Visits to website	3,030,181
Blog visits	52,559
Publications distributed	1,923

for reviewing the Commissioner's decisions and amending timelines to ensure that the privacy protection regime is accessible and effective.

FURTHER READING

Submission of the Office of the Privacy Commissioner of Canada on Bill C-27, the Digital Charter Implementation Act, 2022

OPC's 15 key recommendations on Bill C-27

Appearance on Bill C-47 - Privacy and political parties

Commissioner Dufresne appeared before the Standing Senate Committee on Legal and Constitutional Affairs to discuss amendments to the *Canada Elections Act* proposed in Bill C-47, the *Budget Implementation Act*, 2023.

The proposed changes would allow political parties and their affiliates to collect, use, retain, disclose and dispose of personal information in accordance with the party's own privacy policy – which they develop and revise at their own discretion. The changes do not establish minimum privacy requirements for political parties to follow when handling personal information or provide for independent oversight of their privacy practices by a third party.

The Commissioner stated that, given the importance of privacy and the sensitive nature of the information being collected, Canadians need and deserve a privacy regime for political parties that goes further than self-regulation.

The Commissioner said that political parties should be subject to specific privacy rules that are substantially similar to the requirements that are set out for the public and private sectors in the *Privacy Act* and PIPEDA, while at the same time being adapted to the unique and essential role played by political parties in the democratic process.

FURTHER READING

Appearance before the Standing Senate Committee on Legal and Constitutional Affairs (LCJC) on Bill C-47, *An Act to implement certain provisions of the budget tabled in Parliament on March 28, 2023*

Brief on the Declaration of Emergency

The OPC submitted a brief to the Special Joint Committee on the Declaration of Emergency in support of its study of the issue in 2022. It delineated key privacy principles that should factor into any assessment of measures proposed to address a public order emergency. Our brief noted the importance of developing a clear privacy governance framework to be implemented during emergencies to ensure that government institutions and private sector entities meet their obligations under both the *Privacy Act* and PIPEDA.

FURTHER READING

Submission of the Office of the Privacy Commissioner of Canada on Privacy during an Emergency

The use and impact of facial recognition technology

The OPC appeared before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on its study of the use and impact of facial recognition technology. The Committee's report on facial recognition confirmed the need to regulate privacy impactful technologies such as facial recognition and artificial intelligence, including measures proposed by the OPC, such as mandatory PIAs, enhanced oversight and public reporting and the modernization of privacy laws.

FURTHER READING

Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on their Study of the Use and Impact of Facial Recognition Technology

Statement from the Privacy Commissioner following release of ETHI report on facial recognition technology

Response to ETHI report on the collection and use of mobility data for COVID-19 tracking

The OPC appeared before the Standing Committee on Access to Information, Privacy and Ethics in February 2022 on the PHAC's collection and use of mobility data for COVID-19 tracking. When the Committee's report was released, our Office welcomed its conclusions, which underscored the need for a modernization of federal privacy laws, particularly with respect to de-identification and transparency requirements.

FURTHER READING

Appearance before the Committee on Access to Information, Privacy and Ethics (ETHI) on their Study of the Collection and Use of Mobility Data by the Government of Canada

Statement from the Privacy Commissioner following release of ETHI report into the government's collection and use of mobility data

Collection and use of mobility data by the Government of Canada and related issues: Report of the Standing Committee on Access to Information, Privacy and Ethics

Appearance on RCMP investigative tools

Commissioner Dufresne appeared before ETHI on its study of the RCMP's use of on-device investigative tools, which can collect private communications, documents, audio and images sent or received from or stored on a device. The Commissioner recommended that all institutions, including the RCMP, make privacy a key consideration when contemplating the use of any technology that could have adverse impacts on privacy. The Commissioner recommended that a modernization of the *Privacy Act* would contain a binding requirement for government institutions to submit PIAs to the OPC in high-risk cases.

FURTHER READING

Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the Study of Device Investigation Tools Used by the RCMP

Letter to the Standing Committee on Access to Information, Privacy and Ethics on study of RCMP use of spyware

Device investigative tools used by the Royal Canadian Mounted Police and related issues – Report of the Standing Committee on Access to Information, Privacy and Ethics

Statement from the Privacy Commissioner following release of ETHI report on study into RCMP investigative tools

Privacy Commissioner Dufresne appearing before Parliamentary committee on the study into RCMP investigative tools / CPAC

Appearance on Bill S-7

OPC officials appeared before the Standing Senate Committee on National Security and Defence to discuss Bill S-7, An Act to amend the *Customs Act and Preclearance Act*, 2016, which seeks to clarify the circumstances in which border service officers may examine documents stored on personal digital devices. The OPC argued that the "novel" threshold of "reasonable general concern" proposed in S-7 for such a search creates the potential for ambiguity and proposed that the threshold be "reasonable grounds to believe," or "reasonable grounds to suspect," which is already established in the *Customs Act*. At Committee stage, the Senators amended the threshold to "reasonable grounds to suspect."

FURTHER READING

OPC officials appear before parliamentary committee examining Bill S-7

Appearance on Bill C-11

Commissioner Dufresne appeared before the Standing Senate Committee on Transport and Communications on Bill C-11, an *Act to amend the Broadcasting Act* (*Online Streaming Act*), which would give the Canadian Radio-television and Telecommunications Commission (CRTC) the power to impose conditions respecting the discoverability of Canadian programs and programming services. Given the potential impact for privacy, the Commissioner stressed the importance of assessing and mitigating privacy risks prior to imposing any such conditions. The Committee agreed and amended the Bill to include a requirement to consider "the right to privacy of individuals" and that the CRTC protect the privacy of individuals when it develops regulations for broadcasters.

FURTHER READING

Privacy Commissioner appears before Senate committee to offer comment on Bill C-11

Letter to the Standing Senate Committee on Transport and Communications on study of Bill C-11, *An Act to amend the Broadcasting Act (Online Streaming Act)*

Commissioner Dufresne with his G7 counterparts at the third rountable of the G7 Data Protection and Privacy Authorities in Tokyo, Japan.

Privacy Commissioner Dufresne at the third rountable of the G7 Data Protection and Privacy Authorities.

International and domestic cooperation

The OPC works closely with its domestic and international counterparts. Given the increase in international data flows, data protection authorities recognize the need to promote privacy as a fundamental right and to cooperate on common issues to achieve interoperability between rules in different jurisdictions.

Examples of this include 2 joint investigations launched with our counterparts in Quebec, British Columbia and Alberta: TikTok and ChatGPT.

The OPC also participates in a variety of domestic and international forums.

In September, Commissioner Dufresne and his provincial and territorial counterparts adopted 2 important resolutions. The first encouraged the implementation of a digital health communication infrastructure that would phase out the use of unencrypted email and fax communication. The second called on governments and relevant stakeholders to ensure that the rights to privacy and transparency are fully respected throughout the design, operation and ongoing evolution of a digital identity ecosystem.

Also with our domestic counterparts, the OPC published guidance on facial recognition for police agencies, and released a joint statement recommending that legislators develop a legal framework for the acceptable use by police of facial recognition technology.

Internationally, the OPC plays a leadership role in the Global Privacy Assembly (GPA). Our Office chairs or co-chairs several working groups, such as the Data Protection and Other Rights and Freedoms Working Group, the Digital Citizen and Consumer Working Group and the International Enforcement Cooperation Working Group.

In 2022 the Data Protection and Other Rights and Freedoms Working Group, which examines the relationship between privacy and other human rights, gave presentations focusing on its 2021 narrative report highlighting the role of privacy in upholding other fundamental human rights.

The Digital Citizen and Consumer Working Group, which explores the intersection between privacy and other regulatory spheres, held a workshop in February 2023 where regulators, civil society and other stakeholders met

to exchange perspectives on the nexus of privacy and competition in the digital economy. A main objective of the group is to facilitate cross-regulatory collaboration – an example of which is the newly formed Canadian Digital Regulators Forum, where the OPC, the Competition Bureau and the CRTC collaborate on matters relating to digital markets.

The International Enforcement Cooperation Working Group has organized sessions to discuss issues such as smart glasses and ad tech. In June 2022, the OPC and 5 other group members issued joint guidance for organizations and individuals to protect themselves against risks associated with credential stuffing. The group also organized a global capacity-building workshop to manage investigation backlogs.

The OPC is a member of the management committee of the Global Privacy Enforcement Network (GPEN), which supports information sharing, capacity building and collaboration on matters related to enforcement. Our Office hosts the GPEN website and, in the past year, shared information with other GPEN member authorities such as our investigative findings into Home Depot and Yahoo.

The OPC attended the GPA annual meeting in Türkiye in October, which brought together more than 120 data protection authorities. Discussions focused on topics such as facial recognition technology, artificial intelligence, big data, mass surveillance online, blockchain and the metaverse and cross-border data transfers. Resolutions adopted included one on improving cybersecurity regulation and another on the appropriate use of facial recognition technology.

Commissioner Dufresne joined his G7 counterparts at the 2022 Roundtable of G7 Data Protection and Privacy Authorities in Germany to discuss regulatory and technology issues in the context of "Data Free Flow with Trust" and shared knowledge about the prospects for "international data spaces." The Commissioner also led a discussion on de-identification standards.

Commissioner Dufresne also attended the Asia Pacific Privacy Authorities Forum in Singapore, where the OPC presented on anonymization, led a roundtable on privacy in the pandemic and participated in discussions on accountability in the regulation of artificial intelligence.

Additionally, our Office shares information on specific enforcement matters pursuant to various bilateral and multi-lateral arrangements. In 2022-23 the OPC widened its network by signing an information-sharing arrangement with Abu Dhabi.

FURTHER READING

- Securing Public Trust in Digital Healthcare: Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombudspersons with Responsibility for Privacy Oversight
- Ensuring the Right to Privacy and Transparency in the Digital Identity Ecosystem in Canada: Resolution of the Federal, Provincial and Territorial Privacy Commissioners and Ombuds with responsibility for privacy oversight
- Recommended legal framework for police agencies' use of facial recognition: Joint Statement by Federal, Provincial and Territorial Privacy Commissioners
- Privacy guidance on facial recognition for police agencies
- International privacy regulators endorse resolutions on cybersecurity and facial recognition
- G7 data protection and privacy authorities discuss data protection and the flow of data across borders
- Communiqué: Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces
- Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology
- Data protection authorities from Asia Pacific region discuss privacy issues, best practices
- OPC signs information-sharing agreement with the data protection authority of Abu Dhabi

Contributions Program

Each year the OPC funds a variety of independent privacy research and public education initiatives through its Contributions Program.

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

For 2023-24, the OPC called for proposals answering to the theme, "The future is now! Assessing and managing the privacy impacts of immersive and embeddable technologies."

Our Office received 44 proposals under this call.

FURTHER READING

The future is now! Contributions Program launches annual call for proposals for research and awareness projects

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

General information on the Contributions Program

Outreach to Canadians

Promoting awareness

The OPC protects and promotes the privacy rights of individuals through its education and outreach program. In particular, it seeks to promote greater awareness of the need for Canadians to ask questions when organizations seek to collect and use their personal information so that Canadians can know why this information is being sought.

Privacy Commissioner Dufresne speaking at the IAPP Canada Privacy Symposium 2023, in Toronto. / Anna Kobelak/IAPP

Children's privacy

The OPC takes a special interest in helping children and minors understand the importance of protecting their privacy. Activities to support these goals include social media campaigns, email campaigns directed at teachers and advertising in children's magazines.

Exhibiting events

With events starting up again post-pandemic, in-person activities this year included exhibiting at conferences and events for key groups such as librarians, teachers and students.

A member of OPC's Outreach team at a library association exhibit.

Sharing advice

The OPC developed radio campaigns offering tips about protecting privacy, and also shared advice on issues such as the Internet of Things and privacy settings on book check-out slips in libraries across the country.

Before the Courts

Privacy Commissioner of Canada v Facebook, Inc. **(T-190-20 & A-129-23) (Federal Court and Federal Court of Appeal), *Facebook, Inc. v Privacy Commissioner of Canada* (T-473-20) (Federal Court)**

There are 2 different legal proceedings related to the OPC's 2019 investigation into Facebook which 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.

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

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

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

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

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

FURTHER READING

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

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

Privacy Commissioner appeals Federal Court decision related to Facebook investigation

Google Reference (A-250-21) (Federal Court of Appeal)

In 2018, the OPC sought clarification from the Federal Court on whether Google's search engine is subject to federal privacy law when it indexes web pages and presents search results in response to searches of a person's name.

The OPC asked the Court to consider the issue in the context of a complaint involving an individual who alleged that Google was contravening PIPEDA by prominently displaying links to online news articles about the complainant when their name was searched.

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

In July 2021, the Federal Court released its decision, which agreed with the OPC's position that PIPEDA applies to Google's search engine.

Google appealed that decision in September 2021. The appeal was heard in October 2022 and a decision from the Federal Court of Appeal is pending.

Cain v Canada (Minister of Health) (T-645-20 and T-641-20) and *Hayes v Canada* (Minister of Health) (T-637-20)

Health Canada received requests for information about medical cannabis producer registrations under the *Access to Information Act*, including the postal codes of registered personal producers. Health Canada's position was that releasing more than the first digit of a postal code would unacceptably increase the risk of disclosing information about identifiable individuals.

The Information Commissioner of Canada did not agree with Health Canada's position and brought the matter before the Federal Court. The OPC intervened to recommend a framework for operationalizing the test for determining whether there is a serious possibility that an individual could be identified.

On January 25, 2023, the Federal Court issued its decision, finding that releasing more than the first digit of postal codes raised a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information. In its decision, the Court reiterated its recognition of the fundamental and quasi-constitutional nature of privacy rights.

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

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
Our office 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 office 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 *Privacy Act*

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

Respondent	Discontinued	Not well-founded	Resolved	Settled	Well-founded	Well-founded Conditionally resolved	Well-founded Resolved	Withdrawn	Total
Administrative Tribunals Support Service of Canada	1		4				1		**6**
Canada Border Services Agency			14		1	1	2		**18**
Canada Energy Regulator			1						**1**
Canada Lands Company Limited	1								**1**
Canada Post Corporation			8				2		**10**
Canada Revenue Agency		3	13				3	1	**20**
Canada School of Public Service							1		**1**
Canadian Air Transport Security Authority			1				1		**2**
Canadian Broadcasting Corporation			1	1					**2**
Canadian Human Rights Commission		3	1				1		**5**
Canadian Security Intelligence Service		4	7						**11**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police			2						**2**
Communications Security Establishment Canada		2	2						**4**
Correctional Service Canada		12	48	2	1	1	2		**66**
Crown-Indigenous Relations and Northern Affairs Canada			9						**9**
Department of Justice Canada		1	3	1					**5**
Department of National Defence	2	5	10	2		1			**20**

APPENDIX 2

Respondent	Discontinued	Not well-founded	Resolved	Settled	Well-founded	Well-founded Conditionally resolved	Well-founded Resolved	Withdrawn	Total
Elections Canada / Office of the Chief Electoral Officer			1						**1**
Employment and Social Development Canada	1		14				2		**17**
Fisheries and Oceans Canada			8						**8**
Global Affairs Canada		1	2						**3**
Health Canada		1	10						**11**
Immigration and Refugee Board of Canada					1				**1**
Immigration, Refugees and Citizenship Canada		1	34			1			**36**
Indigenous Services Canada			3	1		1	1		**6**
Innovation, Science and Economic Development Canada			2						**2**
International Development Research Centre	1								**1**
Library and Archives Canada			4						**4**
Military Grievances External Review Committee	1								**1**
Military Police Complaints Commission	1								**1**
National Research Council Canada						1			**1**
Natural Resources Canada			2						**2**
Office of the Auditor General of Canada,	2								**2**
Office of the Information Commissioner of Canada	2								**2**
Office of the Ombudsman National Defence and Canadian Forces			1						**1**
Privy Council Office	1	1	1						**3**
Public Health Agency of Canada			3						**3**
Public Prosecution Service of Canada		1							**1**

APPENDIX 2

Respondent	Discontinued	Not well-founded	Resolved	Settled	Well-founded	Well-founded Conditionally resolved	Well-founded Resolved	Withdrawn	Total
Public Safety Canada	1		1						**2**
Public Service Commission of Canada	1		1						**2**
Public Services and Procurement Canada	1		9	2			1		**13**
Royal Canadian Mounted Police	3	5	43	1	1		1		**54**
Service Canada			4						**4**
Shared Services Canada		1				1			**2**
Statistics Canada			2						**2**
Telefilm Canada			1						**1**
Transport Canada			3			1			**4**
Treasury Board of Canada Secretariat	2		20	1		2			**25**
Veterans Affairs Canada			8	1					**9**
Veterans Review and Appeal Board			1						**1**
Total	**21**	**41**	**302**	**12**	**4**	**10**	**18**	**1**	**409**

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	**146**	**8.9**	**60**	**15.8**	**206**	**10.9**
Access	144	8.9	58	15.8	202	10.9
Correction - Notation	2	10.1	1	22.8	3	14.4
Index			1	11.5	1	11.5
Privacy	**152**	**6.8**	**51**	**18.8**	**203**	**9.8**
Accuracy	3	5.0			3	5.0
Collection	18	7.9	15	25.7	33	16.0
Retention and disposal	4	5.4	2	17.6	6	9.5
Use and disclosure	127	6.7	34	15.9	161	8.6
Time limits	**171**	**1.3**	**419**	**2.4**	**590**	**2.1**
Correction - Time limits	1	6.6			1	6.6
Extension notice			3	0.9	3	0.9
Time limits	170	1.3	416	2.4	586	2.1
Total	**469**	**5.4**	**530**	**5.5**	**999**	**5.5**

Table 3 - *Privacy Act* treatment times - all closed files by disposition

Complaint type	Count	Average treatment time (Months)
Early resolved	**469**	**5.4**
All other investigations	**530**	**5.5**
Discontinued	37	6.9
Not well-founded	41	17.0
Resolved	5	11.4
Settled	12	20.9
Well-founded	4	18.4
Well-founded - Conditionally resolved	182	2.9
Well-founded - Deemed refusal	58	4.3
Well-founded - Resolved	190	4.0
Withdrawn	1	21.4
Total	**999**	**5.5**

Table 4 - *Privacy Act* breaches by institution

Respondent	Number of incidents
Canada Energy Regulator	1
Canada Post Corporation	2
Canada Revenue Agency	30
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police	1
Communications Security Establishment Canada	2
Correctional Service Canada	14
Defence Construction Canada	1
Department of National Defence	1
Employment and Social Development Canada	196
Farm Credit Canada	1
Fisheries and Oceans Canada	4
Global Affairs Canada	6
Health Canada	1
Immigration and Refugee Board of Canada	1
Immigration, Refugees and Citizenship Canada	7
Library and Archives Canada	2
Natural Resources Canada	3
Office of the Auditor General	1
Office of the Secretary to the Governor General	1
Public Prosecution Service of Canada	3
Public Service Commission of Canada	10
Royal Canadian Mounted Police	6
Shared Services Canada	1
Transport Canada	1
Treasury Board of Canada Secretariat	1
Veterans Affairs Canada	1
Total	**298**

Table 5 - *Privacy Act* complaints and breaches

Category	Total
Accepted	
Access	332
Privacy	252
Time limits	657
Total complaints accepted	**1241**
Closed through early resolution	
Access	146
Privacy	152
Time limits	171
Total	**469**
Closed through all other investigations	
Access	60
Privacy	51
Time limits	419
Total	**530**
Total complaints closed	**999**
Breaches received	
Unauthorized disclosure	99
Loss	132
Theft	2
Unauthorized access	65
Total breaches received	**298**

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	267	40%	12	3%	50	45%	329	27%
Correction - Notation	3	0%					3	0%
Privacy								
Accuracy	2	0%			2	2%	4	0%
Collection	23	3%			12	11%	35	3%
Retention and disposal	6	1%					6	0%
Use and disclosure	158	24%	1	0%	48	43%	207	17%
Time limits								
Extension notice			8	2%			8	1%
Time limits	213	32%	436	95%			649	52%
Total	**672**	**100%**	**457**	**100%**	**112**	**100%**	**1241**	**100%**

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

Table 7 - *Privacy Act* top 10 institutions by complaints accepted and fiscal year

Respondent	2017-18	2018-19	2019-20	2020-21	2021-22	2022-23
Royal Canadian Mounted Police	232	273	176	186	179	262
Correctional Service Canada	440	426	155	130	182	199
Immigration, Refugees and Citizenship Canada	29	59	44	47	49	131
Canada Revenue Agency	63	79	63	40	48	79
Canada Border Services Agency	76	109	42	48	53	78
Department of National Defence	93	121	33	51	53	74
Employment and Social Development Canada	24	39	25	41	26	54
Public Services and Procurement Canada	49	27	70	42	19	36
Global Affairs Canada	2	20	19	18	11	26
Canada Post Corporation	33	29	4	22	45	23
Total	**1041**	**1182**	**631**	**625**	**665**	**962**

Table 8 - *Privacy Act* complaints accepted by institution

Respondent	Early resolution	Summary investigation	Investigation	Total
Administrative Tribunals Support Service of Canada	2			**2**
Canada Border Services Agency	37	33	8	**78**
Canada Energy Regulator	1			**1**
Canada Post Corporation	21	2		**23**
Canada Revenue Agency	51	20	8	**79**
Canadian Air Transport Security Authority	1		1	**2**
Canadian Broadcasting Corporation	1			**1**
Canadian Centre for Occupational Health and Safety	1			**1**
Canadian Food Inspection Agency	2	1	1	**4**
Canadian Forces Morale and Welfare Services / Non-Public Property and Staff of the Non-Public Funds, Canadian Forces	1			**1**
Canadian Human Rights Commission	1		2	**3**
Canadian Institutes of Health Research		2		**2**
Canadian Museum for Human Rights	1			**1**
Canadian Security Intelligence Service	7	3	3	**13**
Canadian Transportation Agency	1	1		**2**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police	3			**3**
Communications Security Establishment Canada	4	2		**6**
Correctional Service Canada	94	99	6	**199**
Crown-Indigenous Relations and Northern Affairs Canada	5	2		**7**
Defence Construction Canada	1			**1**

APPENDIX 2

Respondent	Early resolution	Summary investigation	Investigation	Total
Department of Justice Canada	5	6		**11**
Department of National Defence	41	30	3	**74**
Elections Canada / Office of the Chief Electoral Officer	1			**1**
Employment and Social Development Canada	41	8	5	**54**
Environment and Climate Change Canada	5			**5**
Federal Government of Canada	1			**1**
Financial Transaction and Reports Analysis Centre of Canada			1	**1**
Fisheries and Oceans Canada	16	2	2	**20**
Global Affairs Canada	16	4	6	**26**
Halifax Port Authority	1			**1**
Health Canada	14	1	1	**16**
Immigration and Refugee Board of Canada	3	3	4	**10**
Immigration, Refugees and Citizenship Canada	72	53	6	**131**
Impact Assessment Agency of Canada	3			**3**
Indigenous Services Canada	7	2		**9**
Innovation, Science and Economic Development Canada	4		1	**5**
International Development Research Centre			1	**1**
Library and Archives Canada	8	2		**10**
Military Grievances External Review Committee			1	**1**
Military Police Complaints Commission	1		1	**2**
National Research Council Canada	2		1	**3**
National Security and Intelligence Review Agency		1	8	**9**

APPENDIX 2

Respondent	Early resolution	Summary investigation	Investigation	Total
Natural Resources Canada	1		1	**2**
Office of the Information Commissioner of Canada			3	**3**
Office of the Correctional Investigator of Canada	1			**1**
Office of the Ombudsman National Defence and Canadian Forces	1			**1**
Office of the Public Sector Integrity Commissioner of Canada			1	**1**
Office of the Superintendent of Financial Institutions Canada		1	1	**2**
Pacific Economic Development Canada			3	**3**
Parks Canada Agency	1			**1**
Parole Board of Canada	3			**3**
Passport Canada	2		1	**3**
Prairies Economic Development Canada		1		**1**
Privy Council Office	1	3		**4**
Public Health Agency of Canada	12	2	5	**19**
Public Prosecution Service of Canada	1			**1**
Public Safety Canada			1	**1**
Public Service Commission of Canada	1	3	1	**5**
Public Services and Procurement Canada	24	10	2	**36**
Royal Canadian Mounted Police	99	151	12	**262**
Service Canada	5			**5**
Shared Services Canada	1	2	2	**5**
Social Sciences and Humanities Research Council of Canada	1			**1**
Statistics Canada	5	2	2	**9**

Respondent	Early resolution	Summary investigation	Investigation	Total
Trans Mountain Corporation			1	**1**
Transport Canada	7	5		**12**
Treasury Board of Canada Secretariat	19		3	**22**
Veterans Affairs Canada	10		3	**13**
VIA Rail Canada	1			**1**
Total	**672**	**457**	**112**	**1241**

Table 9 - *Privacy Act* dispositions by complaint type

Complaint type	Discontinued	Not well-founded	Resolved	Settled	Well-founded	Well-founded Conditionally resolved	Well-founded Deemed refusal	Well-founded Resolved	Withdrawn	Total
Access	**8**	**31**	**148**	**7**		**1**		**11**		**206**
Access	7	31	146	7				11		**202**
Correction – Notation	1		2							**3**
Index						1				**1**
Privacy	**13**	**10**	**154**	**5**	**4**	**9**		**7**	**1**	**203**
Accuracy			3							**3**
Collection	3	8	19			1		2		**33**
Retention and disposal	1		4	1						**6**
Use and disclosure	9	2	128	4	4	8		5	1	**161**
Time limits	**16**		**172**			**172**	**58**	**172**		**590**
Correction – Time limits			1							**1**
Extension notice								3		**3**
Time limits	16		171			172	58	169		**586**
Total	**37**	**41**	**474**	**12**	**4**	**182**	**58**	**190**	**1**	**999**

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

Respondent	Discontinued	Resolved	Well-founded Conditionally resolved	Well-founded Deemed refusal	Well-founded Resolved	Total
Canada Border Services Agency	2	13	10	6	10	**41**
Canada Post Corporation		1		1	2	**4**
Canada Revenue Agency		13	8		8	**29**
Canadian Air Transport Security Authority		1				**1**
Canadian Forces Morale and Welfare Services / Non-Public Property and Staff of the Non-Public Funds, Canadian Forces		1				**1**
Canadian Human Rights Commission		1				**1**
Canadian Institutes of Health Research			1			**1**
Canadian Museum for Human Rights		1				**1**
Canadian Transportation Agency					1	**1**
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police		1				**1**
Communications Security Establishment Canada	2					**2**
Correctional Service Canada	1	19	76	6	15	**117**
Crown-Indigenous Relations and Northern Affairs Canada					1	**1**
Department of Justice Canada		1	2	3	1	**7**
Department of National Defence	1	15	16	3	9	**44**
Employment and Social Development Canada		5	4		1	**10**
Environment and Climate Change Canada		1				**1**
Fisheries and Oceans Canada		1	1		1	**3**
Global Affairs Canada		8	1	3	1	**13**

Respondent	Discontinued	Resolved	Well-founded Conditionally resolved	Well-founded Deemed refusal	Well-founded Resolved	Total
Health Canada		1				**1**
Immigration, Refugees and Citizenship Canada	7	35	2	3	40	**87**
Indigenous Services Canada			1			**1**
Library and Archives Canada		4			2	**6**
Office of The Correctional Investigator of Canada		1				**1**
Privy Council Office					2	**2**
Public Health Agency of Canada		2		1	1	**4**
Public Services and Procurement Canada		7			10	**17**
Royal Canadian Mounted Police	2	38	47	31	64	**182**
Shared Services Canada				1	1	**2**
Statistics Canada					1	**1**
Transport Canada	1	2	3		1	**7**
Total	**16**	**172**	**172**	**58**	**172**	**590**

Statistical tables related to PIPEDA

Table 1 - PIPEDA complaints accepted by industry sector

Industry sector	Number	Proportion of all complaints accepted
Accommodations	19	4%
Construction	1	0%
Entertainment	12	3%
Financial sector	116	26%
Food and beverage	5	1%
Government	4	1%
Health	24	5%
Insurance	22	5%
Internet	55	12%
Manufacturing	10	2%
Mining and Oil and gas extraction	1	0%
Not for profit organizations	2	0%
Not specified	14	3%
Professionals	26	6%
Publishers (except Internet)	9	2%
Rental	2	0%
Sales/retail	36	8%
Services	36	8%
Telecommunications	38	8%
Transportation	22	5%
Total	**454**	**100%**

Table 2 - PIPEDA complaints accepted by complaint type

Complaint type	Number	Proportion of all complaints accepted
Access	120	26%
Accountability	4	1%
Accuracy	4	1%
Collection	39	9%
Consent	63	14%
Correction/Notation	9	2%
Openness	2	0%
Retention	43	9%
Safeguards	11	2%
Use and disclosure	92	20%
Time limits	67	15%
Total	**454**	**100%**

Table 3 - PIPEDA investigations closed by industry sector and disposition

Sector Category	Early resolved	Discontinued (under 12.2)	No jurisdiction	Not well-founded	Settled	Well-founded	Well-ounded Conditionally resolved	Well-founded Resolved	Withdrawn	Total
Accommodations	21	2			6		2			**31**
Construction	1									**1**
Entertainment	5				1					**6**
Financial sector	71	7	1	5	10	1	3	2	1	**101**
Food And beverage	3			1			1		1	**6**
Government	3							1		**4**
Health	3	1		1	1				9	**15**
Insurance	15	3		2				1	1	**22**
Internet	28								3	**31**
Manufacturing	1									**1**
Mining and Oil and gas extraction	1									**1**
Not for profit organizations	1									**1**
Not specified	2									**2**
Professionals	19	2		2		1				**24**
Publishers (except Internet)	2	2				2				**6**
Rental		1		1						**2**
Sales/retail	22	2		2	1	1		2	1	**31**
Services	24	2		1					2	**29**
Telecommunications	39	2			1			1	1	**44**
Transportation	21	1		1	1		1		1	**26**
Total	**282**	**25**	**1**	**16**	**21**	**5**	**7**	**7**	**20**	**384**

Table 4 - PIPEDA investigations closed by complaint type and disposition

Complaint type	Early resolved	Discontinued (under 12.2)	No jurisdiction	Not well-founded	Settled	Well-founded	Well-founded Conditionally resolved	Well-founded Resolved	Withdrawn	Total
Access	67	10	1	6	1	1	2	3	2	**93**
Accountability	1	1								**2**
Accuracy	2								1	**3**
Appropriate purposes									1	**1**
Collection	34	2		4			1		1	**42**
Consent	26	3		1	9		2	1	2	**44**
Correction/Notation	6				1					**7**
Openness	1									**1**
Retention	21	1			2					**24**
Safeguards	13				7	1	2	1	1	**25**
Time limits	45			1					9	**55**
Use and disclosure	66	8		4	1	3		2	3	**87**
Total	**282**	**25**	**1**	**16**	**21**	**5**	**7**	**7**	**20**	**384**

Table 5 - PIPEDA investigations - Average treatment times by disposition

Disposition	**Number**	**Average treatment time** (Months)
Early resolved	282	7.8
Discontinued (under 12.2)	25	10.9
No jurisdiction	1	6.7
Not well-founded	16	12.6
Settled	21	11.2
Well-founded	5	13.5
Well-founded - Conditionally resolved	7	36.2
Well-founded - Resolved	7	16.1
Withdrawn	20	8.9
Total	**384**	
Overall weighted average		9.2

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	67	8.4	26	11.9	93	9.4
Accuracy	2	8.4	1	48.4	3	21.7
Accountability	1	10.1	1	9.4	2	9.8
Appropriate purposes			1	17.6	1	17.6
Collection	34	8.8	8	13.0	42	9.6
Consent	26	8.5	18	17.2	44	12.0
Correction/Notation	6	9.8	1	10.2	7	9.9
Openness	1	9.6			1	9.6
Retention	21	7.7	3	9.6	24	8.0
Safeguards	13	9.3	12	19.4	25	14.1
Time limits	45	5.2	10	4.8	55	5.1
Use and disclosure	66	7.8	21	10.1	87	8.4
Total	**282**	**7.8**	**102**	**13.0**	**384**	**9.2**

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

Sector	Incident type				Total incidents per sector	Percentage of total incidents*
	Loss	Theft	Unauthorized access	Unauthorized disclosure		
Accommodation			7	1	**8**	**1%**
Agriculture, forestry, fishing and hunting			1		**1**	**0%**
Construction	1	1	6		**8**	**1%**
Entertainment			8		**8**	**1%**
Financial sector	12	12	105	56	**185**	**27%**
Food and beverage			9		**9**	**1%**
Government		1	5	1	**7**	**1%**
Health	2		11	10	**23**	**3%**
Insurance	5	3	10	28	**46**	**7%**
Internet		1	9	3	**13**	**2%**
Manufacturing			26	1	**27**	**4%**
Mining and Oil and gas extraction			4	1	**5**	**1%**
Not for profit organizations	1	4	23	8	**36**	**5%**
Professionals	2	4	37	25	**68**	**10%**
Publisher (except Internet)			15	2	**17**	**2%**
Sales/retail	6	3	37	12	**58**	**9%**
Services		1	22	7	**30**	**4%**
Telecommunications			101	14	**115**	**17%**
Transportation			15	2	**17**	**2%**
Total	**29**	**30**	**451**	**171**	**681**	

* Figures may not sum to total due to rounding.

Table 8 - Number of Canadian accounts affected by incident type

Incident type	Number of Canadian accounts affected
Loss	867
Theft	3,630
Unauthorized access	10,222,970
Unauthorized disclosure*	2,047,639
Total	**12,275,106**

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

Appendix 3: Substantially similar legislation

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

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

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

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

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

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

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

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

Appendix 4: Report of the Privacy Commissioner, Ad Hoc

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

In the reporting year of April 1, 2022, to March 31, 2023, I received 10 new matters, most of which involved questions regarding the handling of privacy complaint investigations by the OPC. Those complaints cannot be accepted by the Ad Hoc Commissioner as their subject matter does not fall within my statutory delegated area of review. The correct recourse to challenge an investigative decision of the OPC is with the Federal Court, via an application for judicial review.

Despite not being able to accept those complaints, I still provided explanations and directed the individuals to the appropriate channels to permit them to pursue their concerns. In doing so, I intend to render a useful public service in helping people distinguish between the review processes which are understandably difficult to keep separate.

There was 1 complaint matter that fell within my area of investigation. In that case, an individual had filed a prior privacy breach complaint with the OPC regarding the handling of the individual's personal information by a federal government institution.

The OPC, via its Compliance Directorate, concluded its investigation and found that the privacy breach complaint was not well founded. In seeking more answers, the individual sought access to the very information found in the complaint investigation file through an access request submitted to the OPC. Access requests at the OPC are filed with the Director of Access to Information and Privacy. In the Director's response, information was withheld from the individual, including some of the individual's own personal information, and as a result, a complaint was filed with me.

My review centred on whether section 22.1(1) of the *Privacy Act* was applied properly. That statutory provision bars access to some of the information found in the OPC's complaint investigation file involving another federal government institution, the rationale being that the OPC is prohibited from disclosing information obtained during its privacy complaint investigations.

The rule in section 22.1(1) is very strict and will extend to barring access to personal information obtained by the OPC, even where it concerns the individual, and even where the information is already known to the requester. This was the conclusion in that case and I found the response to be lawful. Yet, my findings were able to address the individual's concerns and provide clarity as to why access to some of the requested information could not take place.

More generally, findings of this nature raise awareness of the process, again often difficult to understand, as to how access requests for complaint investigation files at the OPC are handled, especially as it related to the delicate subject matter of accessing one's own personal information.

It goes without saying that all cases filed with me are noteworthy and interesting, and while I cannot accept some that are filed with me, the service I provide to each individual is intended to be worthwhile and helpful.

And so, I look forward to continuing my work for all who seek my assistance in the coming year.

Respectfully submitted,

Anne E. Bertrand, K.C./c.r.
Ad Hoc Privacy Commissioner / Commissaire spéciale à la protection de la vie privée

Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada