Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

A pivotal time for privacy

2021-2022 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.

2021-2022 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

Table of Contents

Commissioner's message

This is a pivotal time for privacy. Digital technology, with its growing reliance on personal information, is part of every aspect of our lives. From the most complex – such as dealing with a global pandemic and preventing crime – to the most routine – buying coffee and using our phones to connect with each other.

Finding the right ways of protecting and promoting our fundamental right to privacy while harnessing these new technological opportunities will be a key challenge for Canada's institutions in the coming years. Indeed, Canada's federal public and private sector privacy laws will need to be modernized, both to respond and adapt to these societal and technological changes, and to keep pace with legislative developments in other jurisdictions domestically and internationally.

An important step towards meeting this challenge was taken by the government with the tabling of Bill C-27, the *Digital Charter Implementation Act* in June of this year. The Bill aims at modernizing the *Personal Information and Electronic Documents Act* and is a recognition by the government that Canadians need and expect modernized privacy laws. As Canada's new Privacy Commissioner, I look forward to providing my views on the proposed legislation to Parliament this fall.

As I indicated to parliamentarians during the review of my proposed appointment, as Commissioner, I will be promoting and implementing a vision of privacy that recognizes:

1. Privacy as a fundamental right;
2. Privacy in support of the public interest and Canada's innovation and competitiveness; and
3. Privacy as an accelerator of Canadians' trust in their institutions and a driver in their participation and contribution towards a robust digital economy.

This vision is based on the reality that Canadians want to be able to fully participate as active and informed digital citizens without having to choose between this participation and their fundamental privacy rights. Canadians should be able to benefit from the public interest and economic advances brought by the new technology with the reassurance that their laws and their institutions are there to appropriately safeguard and protect their personal information. In short, privacy is fundamental, it supports important public and private interests and it builds necessary trust.

Achieving this vision will require strong advocacy, enforcement, protection, promotion and education on an ongoing basis. This cannot be achieved by the Office of the Privacy Commissioner (OPC) alone and we look forward to building strong and effective relationships and to working with the privacy stakeholders and champions in the public and private sectors and with our counterparts in Canada and internationally.

This annual report provides an overview of the important work done by the OPC during 2021-2022, the last year of my predecessor's mandate.

I want to take this opportunity to thank Commissioner Daniel Therrien for his 8 years of outstanding service and leadership. He has been a superb champion for law reform and has raised the profile and the understanding of privacy rights in Canada and internationally.

During the last year, the OPC was involved in a number of important investigations, policy work, consultation and collaboration initiatives with the public and private sectors. It provided comprehensive submissions on law reform to the House of Commons and Senate, it prepared and commissioned ground-breaking policy work to deal with key files with inter-jurisdictional and international impacts.

Whether it was through our compliance processes, our leadership role in international privacy networks, our collaboration with global and domestic counterparts, or the provision of advice and interpretation guides to private and public sector organizations, the OPC was at the forefront of efforts to develop and promote a better understanding and implementation of privacy in Canada and around the world

The landscape of privacy issues investigated last year included pandemic-related measures, the use of facial recognition technology by law enforcement agencies, the location tracking of Tim Hortons customers and the 24-hour video and audio surveillance of employee drivers in the trucking industry. These enforcement matters demonstrated once more the many ways in which the privacy of Canadians can be affected by technology and highlighted the importance of putting in place early and effective mechanisms to identify and address privacy concerns at the outset.

The right to privacy and privacy issues affect everyone – younger persons, older persons, those who are fascinated by technology, and even those who are not.

It is certainly an important time for privacy in Canada, and for the OPC.

I am happy and humbled to be joining such an impressive team at such an exciting time. I look forward to continuing to serve Canadians, this time by helping to protect and promote their fundamental privacy rights that are essential to individual autonomy, dignity and the full enjoyment of rights and freedoms in Canada.

Philippe Dufresne

Privacy Commissioner of Canada

Legislative reform: New laws on the horizon

Legislative reform: New laws on the horizon

From the application of facial recognition technology by police to Tim Hortons' inadvertent tracking of customers through its mobile app, our recent work has further underscored the limits of existing privacy legislation and reinforced our call for overdue reform.

In June 2022, we welcomed the introduction by the Minister of Innovation, Science, and Industry, the Honourable François-Philippe Champagne, of Bill C-27, *The Digital Charter Implementation Act, 2022,* which replaces an earlier attempt at private-sector privacy law reform that died on the order paper when the last federal election was called. This much-anticipated development marks an important step toward a new law for the private sector and we have been carefully analyzing the bill so we may properly advise Parliament this fall.

We were also encouraged by remarks by the Minister of Justice, the Honourable David Lametti, following the tabling of Bill C-27 that public sector privacy reform is not far behind and that lawmakers are taking steps to harmonize the legislation to ensure both laws are grounded in the same privacy principles.

Effective privacy protection in the 21st century demands the adoption of public and private sector privacy laws that are interoperable, both nationally and internationally, and confer appropriate powers on the regulator to ensure compliance. Our federal laws must enable responsible innovation, but within a strong legal framework that recognizes, promotes, and protects the fundamental right to privacy.

Facial recognition technology

In May 2022, federal, provincial and territorial privacy protection authorities called on legislators to develop a legal framework that clearly and explicitly establishes the circumstances in which police use of facial recognition may be acceptable.

This followed a public consultation on police use of facial recognition technology during which we heard consistently that the current laws regulating its use did not offer sufficient protection against its associated risks.

When used responsibly, facial recognition technology can offer significant benefits such as helping solve serious crimes, locating missing persons and supporting national security objectives.

However, it can also be extremely intrusive, enable widespread surveillance, provide biased results and erode human rights, including the right to participate freely, without surveillance, in democratic life.

While we await new legislation, we issued joint guidance to assist police in ensuring any use of facial recognition technology complies with the current law, minimizes privacy risks, and respects privacy rights. Still, we remain hopeful the government will move forward with a legal framework that explicitly addresses the risks posed by this technology.

Rights-based reform

In our Parliamentary submission on Bill C-11, we recommended that any future law be entrenched within a rights-based framework that recognizes privacy as a human right, and as an essential element for the exercise of other fundamental rights.

Some have argued a rights-based approach to privacy protection is not possible under Canadian federal law, on the basis that the protection of personal information is a matter of "civil rights" that falls within provincial jurisdiction under the Constitution.

We hope a legal opinion by Addario Law LLP commissioned and released by the OPC in May lays this concern to rest. According to the opinion, certain amendments proposed by the OPC would "either strengthen" or "not affect" the constitutionality of the proposed law.

Preparing for new laws

The OPC has already begun work on a transition plan, based on Bill C-27's predecessor, to ensure we will be in a position to quickly implement new privacy laws once they are in place. This work has involved costing and growth modelling, as well as planning for and consulting on the eventual new responsibilities we could inherit, such as new order-making powers, adjudicatory functions and obligations to review applications for codes of practice and certification programs.

As discussed in our last annual report, the changes proposed in a Department of Justice discussion paper and consultation under the *Privacy Act* include new privacy impact assessment (PIA) obligations for departments, and new OPC responsibilities to offer guidance to federal institutions and undertake public education, among a host of other new functions.

We welcome many of these changes, but they mean the volume of PIAs and the demand for public sector guidance will increase significantly. We will need to be sufficiently resourced to provide this within reasonable timelines.

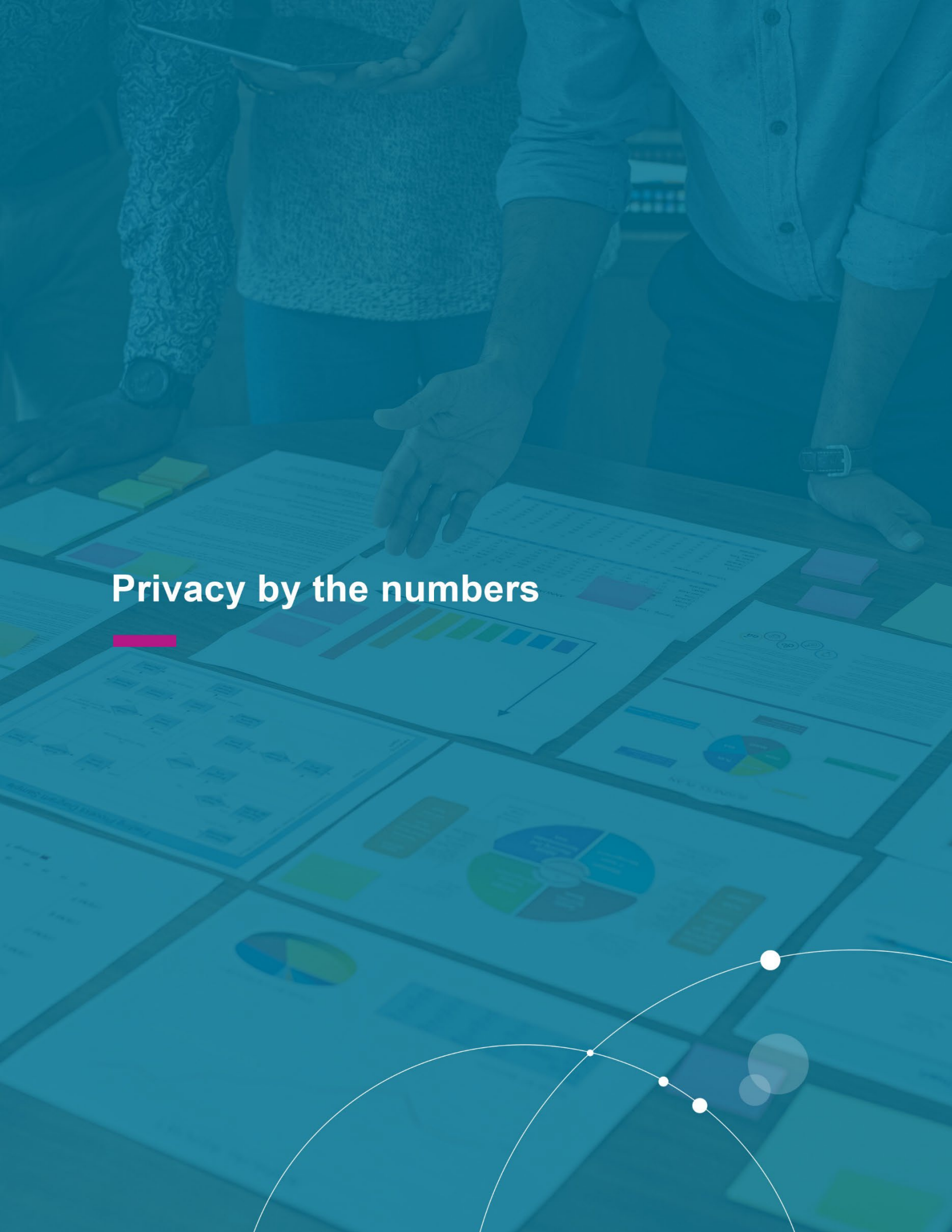
Conclusion

There is no doubt that the modern economy increasingly depends on the value of data extracted through digital technologies. But we have also seen the risks and the harms of technologies with inadequate privacy protections which have led us to the conclusion that the way forward is through reform of our privacy laws in a manner that recognizes and protects privacy as a fundamental right, while at the same time supporting the public interest, innovation, and accelerating Canadians' trust in their institutions and the digital economy.

We are optimistic that a new federal privacy regime is finally within reach.

Further Reading

- Summary of key recommendations for a new federal private sector privacy law in the OPC's C-11 submission (May 4, 2022)
- Backgrounder: Legal opinion on constitutional validity of OPC proposed amendments to former Bill C-11 (May 4, 2022)



Privacy by the numbers

Privacy by the numbers

Privacy Act complaints accepted	906
PIPEDA complaints accepted	427
Data breach reports received under PIPEDA	645
PIPEDA complaints closed through early resolution	303
Privacy Act complaints closed through early resolution	319
Advisory engagements with private-sector organizations	18
Privacy Act complaints closed through standard investigation	474
Well-founded complaints under the *Privacy Act*	81%
PIPEDA complaints closed through standard investigation	55
Well-founded complaints under PIPEDA	58%
Bills and parliamentary studies reviewed for privacy implications	36
Data breach reports received under the *Privacy Act*	463
Privacy impact assessments (PIAs) received	111
Advisory consultations with government departments	105
Advice provided to public-sector organizations following PIA review or consultation	119
Public interest disclosures by federal organizations	747
Parliamentary committee appearances on private-and-public sector matters	5
Information requests	7,494
News releases and announcements	39
Speeches and presentations	34
Tweets	863
Twitter followers	19,581
Visits to website	3,193,419
Blog visits	24,058
Publications distributed	19,923

The *Privacy Act*: A year in review

The *Privacy Act*: A year in review

Issues related to the COVID-19 pandemic were again at the forefront of our work under the *Privacy Act*.

At the time of writing this report, several investigations related to the public health crisis were ongoing, including those related to complaints about the government's policy on mandatory vaccination for federal employees, vaccination requirements for travellers and the government's collection and use of mobility data.

In addition to these formal investigations, over the last year our Government Advisory Directorate also continued to work closely with public sector stakeholders, including Health Canada, the Public Health Agency of Canada (PHAC) and the Canada Border Services Agency (CBSA) on privacy issues related to the COVID-19 pandemic. This work involved changes to border control measures, quarantine and tracking and tracing programs and activities. We also engaged with central agencies on vaccination mandate compliance programs and provided input into Health Canada's evaluation of the COVID Alert App, which was ultimately decommissioned in June 2022.

In non-COVID-19-related work, we issued our first joint review of information sharing related to national security under the *Security of Canada Information Disclosure Act* (SCIDA) with the National Security and Intelligence Review Agency (NSIRA), which is discussed later in this section.

We also concluded our stakeholder consultation on facial recognition technology, using the information gathered to finalize our privacy guidance for police agencies, issued jointly with our provincial and territorial counterparts. This work followed our June 2021 Special Report to Parliament (discussed in last year's annual report) that included the results of an investigation into the RCMP's use of facial recognition technology to conduct hundreds of searches of a database compiled illegally by a commercial enterprise. We concluded this was a violation of the *Privacy Act.*

The following section highlights key initiatives under the *Privacy Act* in 2021-22, including the pandemic-related work conducted by our Government Advisory Directorate.

Government Advisory work

The OPC continued to engage regularly with Health Canada and PHAC on COVID-19-related issues in an advisory role.

Early in the pandemic, we created a framework that encouraged the government to use data in a manner that would serve the public interest while also protecting privacy, a key point of which was to use de-identified or aggregated data wherever possible. As a general principle, we stated in our advisory work that the use of de-identified or aggregated data for public health purposes is consistent with our framework, provided appropriate technical standards are used to prevent re-identification.

A growing trend we have observed is the leveraging of private sector technologies and data by public sector institutions for policy development or to deliver digital government services.

The use of corporate expertise to assist the functioning of the state underscores the need for more consistency across our public and private sector laws. Both sectors should be held to similar standards.

COVID Alert App evaluation

Our office engaged in productive and in-depth discussions about the COVID Alert exposure notification app with the Government of Canada during its development and after its launch in July 2020.

At the time it was launched, our office supported the use of COVID Alert based on the understanding that using the app would be voluntary, that robust safeguards to protect the identity of users would be in place, and on the condition that it could be shown to be effective. We recommended that the COVID Alert app be closely monitored, and that it be decommissioned if new evidence indicated it was not effective in achieving its intended purpose. The OPC Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19 indicated that any privacy invasive measures that have been employed as a result of the pandemic should be time-limited, with obligations to end when they are no longer required.

Health Canada invited the OPC to participate in an evaluation of the app in 2021-22. The evaluation centered on whether the app adhered to the privacy principles outlined in the May 2020 statement “Supporting public health, building trust” issued by federal, provincial and territorial data protection and privacy commissioners on COVID-19 contact tracing and similar apps. It also looked at the app’s governance mechanisms and examined whether the app was effective in contributing to efforts to reduce the spread of COVID-19.

Published in June 2022, the evaluation found there were some indications that the app helped limit the spread of the virus. However, its impact was difficult to quantify given the absence of pre-determined indicators of effectiveness such as benchmarks, targets, and measurable public health impacts.

The evaluation also found steps should have been taken earlier in the app’s lifespan to determine effectiveness and that appropriate targets and goals should be set ahead of launch for any future similar app.

The app was decommissioned by Health Canada in June 2022. The department noted that with the evolution of provincial COVID-19-related public health measures and less PCR testing across Canada, fewer One Time Keys were being issued and fewer notifications were being generated by the app, leading to lower usage. We welcomed the conclusions, which are consistent with the necessity and effectiveness principles of the OPC Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19..

Further reading

- Privacy review of the COVID Alert exposure notification application (July 31, 2020)
- Health Canada Evaluation of the National COVID-19 Exposure Notification App (June 2022)

Border enhancements in response to the pandemic

Programs to prevent, control, track and contain COVID-19 infection at Canada's borders continued to be a high priority during the second year of the pandemic.

We engaged regularly with the CBSA, Immigration, Refugees and Citizenship Canada (IRCC), and PHAC on enhanced border control measures and the implementation of new technology and methodologies.

We were also consulted on the use of biometric technologies and advanced analytics by the CBSA and IRCC as they looked to adapt pandemic-related initiatives for the longer term.

For example, we have consulted with the CBSA as it seeks to leverage pandemic-related border practices limiting physical interactions to move toward an increasingly touchless border in the future. This includes the expansion of self-serve options and paperless processes at border crossings. For example:

CBSA Advance Declaration Initiative

This pilot project introduced in late 2021 enables travellers to provide customs declaration information through the ArriveCAN platform before arriving in Canada.

Our recommendations to the CBSA focused on potential risks related to limiting collection, accuracy and consent. The CBSA submitted a brief PIA annex assessing the pilot. We have recommended that the CBSA complete a PIA on the ArriveCAN platform as a whole, including the integration of Advanced Declaration information into the platform.

Chain of Trust customs clearance process

This initiative piloted a customs clearance process for air travellers entering Canada. It focused on streamlining traveller identification by using digital travel credentials and biometrics and eliminating person-to-person interactions at customs for low-risk travellers.

Pilot project participants used a mobile app to provide their information to CBSA electronically for risk assessment in advance of their arrival. They were then able to move through airport checkpoints without any intervention (unless necessary) by a border services officer.

While the pilot project has ended, CBSA has indicated it will use the lessons learned in the future to inform its larger-scale Traveller Modernization project. We recommended the CBSA carefully test biometric technologies and build internal accountability frameworks before implementing wider-scaled biometric-based border controls, and that the government communicate clearly to the public that its Traveller Modernization products and services are optional. This is vital to obtain meaningful consent.

Biometrics and border management

We also consulted with the CBSA during the fiscal year on the establishment and development of its Office of Biometrics and Identity Management (OBIM). The CBSA identified use of biometrics in border management as a significant priority. As the agency moves forward with increased use of biometrics across programs and activities, we will continue to offer guidance and advice on privacy risks, including risks related to accuracy and the potential risk of secondary uses. We anticipate providing the CBSA with feedback on its Biometric Privacy Framework and will continue to consult and review privacy assessments of various program components.

Immigration, Refugees and Citizenship Canada initiatives

Similarly, the impacts of COVID-19 have focused IRCC efforts on technological innovation and modernization of operations, and many changes instituted as a result of the pandemic will be leveraged for continuing programs. IRCC has consulted our office on its plans to move forward with expanded uses of digitization and advanced data analytics to reduce application processing times, improve service delivery, identify fraud, and improve program security.

We have consulted with IRCC and provided advice on initiatives such as the IRCC Digital Capture Pilot, which enables IRCC to pull information directly and automatically from passports using optical recognition technology, and the Passport Digital Service Project, which will allow individuals to use a cloud-based web application to renew their passports online. This initiative was partly propelled by the spike in the volume of passport renewals and applications in the post-COVID-19 travel boom.

Our advice on these projects has focused on ensuring the accuracy of personal information, avoiding over-collection and ensuring that the purposes for which the information is to be used are clearly indicated and understood as a basis for obtaining meaningful consent. We have also recommended that algorithms used in data analytics be assessed for fairness and accuracy, and that the effectiveness of their use be monitored and re-assessed an ongoing basis.

Other advice and outreach to government departments

As part of the OPC's Policy and Promotion Sector, the Government Advisory Directorate encourages compliance with the *Privacy Act* by providing government institutions with proactive guidance and practical advice on privacy risks associated with use of Canadians' personal information.

Our objective is to help ensure that institutions have the legal authority to use personal information for a clearly stated purpose, that privacy risks are eliminated or mitigated before

federal programs and activities are launched and that institutional transparency and accountability regarding government use of Canadians' personal information is increased. We provide advice and recommendations through our reviews of PIAs submitted to our office under the TBS Directive on Privacy Impact Assessment, through advisory consultations with institutions as initiatives are conceptualized and developed, and through our popular outreach program, which offers online sessions on a variety of privacy-related topics. Our outreach has been provided on an ad hoc basis to institutions requesting guidance. We are moving to a fixed outreach schedule in the new fiscal year, which we hope will broaden our audience even further and allow multiple institutions to attend simultaneously.

We review and provide advice on initiatives, programs and activities ranging in risk and complexity and covering diverse subject matter. In the past fiscal year, this included programs related to social benefit provisions, the use of facial recognition technology by law enforcement and border control, digital government services and digital identity verification and authentication credentials. We also receive and review information sharing agreements, other institutional documents that are part of departmental privacy management frameworks, and notifications of public interest disclosures.

We also consult regularly with the TBS and provide input during the development of central TBS policies, directives and standards pertaining to the use of personal information.

In keeping with a trend reported in our last annual report, the volume of PIAs received, consultations undertaken, and outreach provided by our office remains high, suggesting our input is necessary and valued by government departments. We received 111 PIAs and were consulted 105 times in 2021-22.

We also undertook 39 outreach sessions to government institutions on subjects ranging from how to develop a PIA, to how to comply with the *Privacy Act* when using biometrics, artificial intelligence (AI), or social media monitoring. We estimate that more than 700 federal employees from program development and policy areas, as well as from Access to Information and Privacy (ATIP) teams, attended these outreach sessions.

We also received 747 notifications of disclosures of personal information in the public interest, or in circumstances that benefited the individual. This is in keeping with the generally high volume of public interest disclosures made by government institutions received over the past several years (491 in 2020-21 and 611 in 2019-20).

Paragraph 8(2)(m) of the *Privacy Act* allows personal information to be disclosed when, in the opinion of the head of the institution, the public interest in disclosure would clearly outweigh any invasion of privacy that could result, or if the disclosure would clearly benefit the individual to whom the information relates. The head of the institution is responsible for determining whether the public interest, or the benefit to the individual, outweighs the right to privacy. Section 37 of the *Department of Employment and Social Development Act* has similar authorities.

As is usual, the vast majority of notifications we received were from Employment and Social Development Canada (ESDC). This included cases where Service Canada clients indicated they might harm themselves or have made threats against others – in these cases, police of local jurisdiction are given personal information to carry out wellness checks on the individuals involved and/or to ensure the safety of others. ESDC also assists police in locating missing persons and in notifying next of kin for deceased individuals.

As departments have the discretion to release this type of information under the law, the OPC's role is generally limited to helping ensure institutions have properly evaluated the merits in each case. As we are frequently notified of such disclosures after the fact, which is also permitted by the applicable legislation, we provide advice where we believe it will have the most impact and offer general guidance so that institutions have a clear understanding of appropriate use of the provision. In this regard, we updated our guidance on public interest disclosures under the *Privacy Act*.

Another trend we have observed over the last year is an increase in the number of institutions that have expressed interest in facial recognition technology. For example, the Canadian Air Transport Security Authority (CATSA) is deploying FaceStation to replace its legacy identity verification systems at restricted area points of entry in airports. CATSA employees and contractors present their faces to be authenticated using a facial recognition scanner. Similarly, when the trusted traveller program NEXUS kiosks that used iris scanning to authenticate identity reached their end of life, the CBSA replaced them with new kiosks that use facial biometrics.

We have consistently advised caution in the uptake of FR systems and have underlined the need for necessity and proportionality.

The pace of technological change in government has accelerated overall. For instance, we are seeing more and more digital services and applications being rolled out to the Canadian public every year. In the last number of years, we have engaged with government institutions on their expanded use of private sector and provincial digital identity credentials, their full digitization of institutional document repositories, their use of electronic storage systems, and their increasing use of apps to allow individuals to access government services. We have consistently stressed the need for full consideration of privacy and security concerns in tandem with ease-of-access objectives.

We've also continued to engage with federal institutions regarding social media monitoring and their collection of information from social media for program purposes. For example, we consulted with the CBSA on its collection and use of information about individuals from social media to assist in making admissibility decisions and provided outreach sessions to the Agency on social media monitoring and publicly available information. We also received and reviewed a PIA from Statistics Canada on its use of social media monitoring to assess public sentiment about its programs and activities.

While the CBSA indicated it limits collection to publicly available information, we noted that using open-source information may still have a negative impact on privacy, specifically around issues of accuracy, transparency, and how personal information is used. We advised the CBSA to conduct a comprehensive assessment of the privacy risks of undertaking this activity, and to develop clear procedural documents for employees who conduct searches. We look forward to continuing our discussion in this area.

We also consulted with Statistics Canada on its use of a media monitoring and social listening platform to search, monitor and analyze social media trends and conversations on issues relevant to its programs and activities. We recommended StatCan regularly assess the reports produced by the tool to ensure its use is effective and proportional in meeting the established objectives. We also commented on StatCan's view that prolific users of social media platforms, and in particular "influencers," have a lower expectation of privacy in posting their views. We

noted that while maintaining a public presence on social media may reduce an individual's expectations of privacy, this does not suggest that individuals therefore waive all privacy rights over their data. Information collected from the public domain is considered personal information if it meets the definition provided in section 3 of the *Privacy Act* and is therefore protected by legal requirements when collected by an institution subject to the Act.

RCMP body-worn cameras program

Our office has been engaging with the RCMP on pilot projects and other initiatives involving body-worn cameras for more than a decade.

In our view, body-worn cameras are an inherently privacy-invasive tool, as they collect identifiable images of individuals. As a law enforcement tool, their use is particularly sensitive. While body-worn cameras can be used to support transparency and police accountability, in our view federal institutions contemplating their use must take steps to ensure that any such use is lawfully authorized and that privacy risks are managed appropriately.

In June 2021, we consulted with the RCMP and provided comments on its draft Body-Worn Camera (BWC) Policy and Digital Evidence Management System for storing recordings from these cameras. We were pleased to note the RCMP integrated many of our recommendations into the program, resulting in design changes that included higher levels of privacy protection. For example, the RCMP policy now more clearly outlines the criteria for activating body-worn cameras prior to any interaction with the public or responding to a call for service.

The RCMP also clarified in the policy that members can obstruct the video (but not the audio) to protect the dignity of individuals in sensitive situations. Furthermore, our discussions helped ensure that the RCMP will include privacy clauses in its contracts with the vendor for both the body-worn cameras and the system that will store the video.

We will continue to consult with the RCMP in the future to ensure the national roll-out of body-worn cameras for front line officers is undertaken in as privacy protective a manner as possible. We note the RCMP is developing redaction processes to protect the identity of bystanders whose images are captured by these cameras, but who are not involved in the incident in question. We have not yet had the opportunity to review and offer comments on the redaction process. However, we have reminded the RCMP that its processes should be designed to protect the privacy of bystanders, non-targeted individuals and minors as much as possible. We look forward to continuing our work with the RCMP on this important issue as the program develops.

We anticipate receiving an updated PIA for the national rollout of the body-worn camera program and a new PIA on the Digital Evidence Management System for our review and recommendations. We are also aware that other federal institutions are interested in pursuing body-worn camera programs and we are consulting on these initiatives to ensure privacy risks are managed appropriately.

Compliance actions

Privacy Act enforcement

Compliance issues under *Privacy Act*

In 2021-22 we accepted a total of 906 complaints under the *Privacy Act*, a 10% increase from 2020-21, when we accepted 827 complaints.

As has been the case in the last few years, a great number of complaints concerned access to personal information (27%), and institutions failing to respond to access request within the time limit required under the Act (39%).

Correctional Service Canada (182) and the RCMP (179) continue to lead the list of federal institutions subject to complaints, followed by the CBSA (53), National Defence (53) and IRCC (49).

We received 463 reports of breaches, most of which concerned the loss (278) or unauthorized disclosure (132) of personal information.

The majority of the breach reports, 93%, were due to human error, which includes email and mailing errors, mishandling of data/records using an inappropriate shortcut or workaround and losing or misplacing information, suggesting that the institution may have had policies or security procedures in place that were not being followed or enforced.

These types of breaches underscore that it is not enough to have policies and protocols in place to protect information, but that they also need to be implemented and followed faithfully to be effective. It is key that personal information is properly managed throughout its lifecycle, from collection, to use, to disposal. To this end, employee awareness and engagement is crucial.

We continue to have concerns about under-reporting of cyber-attacks, including malware and phishing attacks, by public sector institutions. We received 5 reports in 2021-2022, down from 9 the previous year.

Complaint backlog

Between April 2019 and March 2021, we successfully leveraged a temporary budget increase and enhanced efficiencies to reduce our investigation files older than 12 months by more than 90% (from 324 cases in 2019 to 29 cases at the end of 2020-2021).

The backlog reduction and enhancements to our processes, including technological efficiencies, allowed us to significantly reduce our overall average treatment time for *Privacy Act* investigations to 6.17 months (down from 9.66 months in 2020-2021). The time it took to complete PIPEDA investigations fell to 7.8 months, compared to 12.2 months a year earlier.

However, with the expiration of the temporary funding this fiscal year, we have seen our backlog cases climb to 102 at the end of March 2022, representing 15% of all ongoing investigations that are under the *Privacy Act* or PIPEDA. While a backlog of approximately 15% is to be expected given our current resources, there is a risk it may continue to grow, therefore we are continuing to adopt new efficiencies in the absence of funding. This upward complaint pressure

is heightened by the introduction of *Privacy Act* Extension Order No. 3, which expanded the right of access to foreign nationals.

Time limits investigations

Our approach to addressing time-limit complaints for federal institutions' granting of access to personal information is an example of the investigative efficiencies that we have introduced. This approach has continued to significantly speed up our investigation processes.

We were able to reduce treatment times for time-limit complaints to just under 3 months.

Under our current approach, if a federal institution does not grant access within a set period of time, we consider that there is "deemed refusal" of access. The deemed refusal process has had the effect of encouraging institutions to respond to access requests in a more reasonable timeframe and empowering complainants with the right to pursue a matter in Federal Court when they do not.

Time limit investigations treatment times

Fiscal Year	Average treatment time in months
2021-22	2.91
2020-21	5.04
2019-20	7.50
2018-19	6.98
2017-18	6.28

Over the last year, we also prepared for *Privacy Act* Extension Order No. 3, which came into force on July 13, 2022. Before, only Canadian citizens and people physically in Canada had a right to request access to their personal information under the control of a federal government institution.

The Extension Order allows foreign nationals outside Canada to make requests, and as a consequence, lodge complaints to the OPC should those requests be unfulfilled. Ahead of the coming into force of the order, government institutions, primarily IRCC, expected to receive hundreds of thousands of new personal information requests, with an anticipated cascading impact on complaint volumes to our office. As a result, we have been seeking funding solutions, as well as developing new investigative approaches, to mitigate the effects of the increased complaint volumes.

Early resolution

Our Compliance, Intake and Resolution Directorate, of which the early resolution and intake teams are part, is responsible for ensuring that complaints of a non-systemic nature are resolved as efficiently and effectively as possible.

Early resolution – a negotiated or mediated investigative approach – is generally the optimal outcome for the parties involved. In such cases, our office does not issue a finding. Early resolution continues to be an integral part of our operations.

Percentage of complaints closed in early resolution

Fiscal year	Percentage of all complaints closed in early resolution
2021-22	40%
2020-21	52%
2019-20	25%
2018-19	32%
2017-18	37%

While down from last year's high-water mark (52%), we successfully concluded 40% of cases strictly through early resolution in 2021-22. It should be noted that the early resolution unit also issues summary investigation reports which are shortened investigations that conclude with the issuance of a brief report or letter of findings. Combining early resolution and summary investigations, the unit closed 88% of all complaints under the *Privacy Act* including time limit investigations.

Summaries of key reviews and investigations

Joint review with NSIRA of disclosures under SCIDA

In December 2021, the National Security and Intelligence Review Agency and the OPC concluded their first joint review of information sharing related to national security under the *Security of Canada Information Disclosure Act* (SCIDA). The review found 212 of the 215 disclosures by federal organizations were in compliance with the requirements of SCIDA.

The Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE) were the primary recipients of information under SCIDA in 2020, while the primary discloser was IRCC. Many of its 159 disclosures related to information contained in passport applications.

Three disclosures by the RCMP were cause for concern, including one that involved the personal information of thousands of people. In that case, the RCMP disclosed to the Department of National Defence (DND) and the Canadian Armed Forces (CAF) the biometric information of thousands of men, women and children detained by a foreign entity on suspicion of being members or supporters of a terrorist organization.

The review raised concerns about that instance which involved the RCMP disclosing highly sensitive information based on incomplete data. The missing information would have been necessary to properly assess both the effect on privacy and the reasonable necessity of the disclosure, as required by SCIDA. We were concerned that the RCMP rejected the key finding that it did not comply with SCIDA requirements in this case.

The joint review had recommended the RCMP provide additional information about this data set to the DND and the CAF. The federal government's response to our SCIDA Report did not clarify whether the RCMP had done so already, or would do so. Rather, the response reiterates the RCMP's defence of the initial disclosure, which was made based on incomplete data.

Overall, NSIRA and the OPC made 11 recommendations aimed at improving institutions' compliance with SCIDA. These related to, for example, record keeping, governance and measures to ensure SCIDA's disclosure test is met.

Why SCIDA reviews are important

SCIDA authorizes institutions to disclose information relevant to national security, including personal information, to a select group of federal government institutions with national security mandates.

SCIDA seeks to strike a reasonable balance between privacy and national security. An important concern in the development of SCIDA was the risk posed to law-abiding citizens that manifests when the personal information of "many" is shared to identify the "few" individuals actually involved in activities of concern to national security.

Further reading

- News release: Joint review of SCIDA disclosures finds general compliance but some areas of concern (February 22, 2022)

DND did not live up to confidentiality commitments to an employee who made a workplace violence complaint

The OPC received a complaint from a DND employee who alleged the department had breached a commitment to keep his identity confidential in connection with a workplace violence complaint he had made.

The department shared copies of the investigation report of his workplace violence complaint with individuals not listed on a related "consent form to disclose identity" he had signed. In signing the consent form, he expected that there was a clear commitment to confidentiality of the investigation into his own workplace violence complaint. The unexpected disclosures were made to individuals in labour relations and a second investigator involving in a related matter.

DND claimed that: the disclosures were necessary to address the allegations raised against the complainant; the disclosures were not prohibited by the consent form in question; and they constituted a "consistent use." The *Privacy Act* allows information to be disclosed without consent when it is for "the purpose for which the information was obtained … or for a use consistent with that purpose."

Our investigation found that the first disclosure, to labour relations, was a consistent use. In light of the important role that labour relations officers play as advisors in relation to workplace issues, it is reasonable to expect that a workplace violence report may be shared internally with them.

However, in consideration of the wording on the consent form, which created an expectation of confidentiality, we do not think that a complainant to a workplace violence process would reasonably expect a report into their complaint would in turn be used as evidence in separate disciplinary proceedings. We therefore determined that the disclosure to the investigator was not a consistent use, and this aspect of the complaint was well-founded.

For a disclosure to be a permissible "consistent use" under the *Privacy Act*, it must have a sufficiently direct connection to the original purpose for which the information was originally obtained such that an individual would reasonably expect it to be used in a particular manner. There must be clear alignment between how limits on confidentiality are explained to individuals and when and how disclosures are actually made to carry out valid purposes.

We recommended DND modify any products or tools used by staff, or provided to participants, in a workplace violence process, to ensure that any disclosures of personal information made on the basis of "consistent use" do not fall outside of a participant's reasonable expectations.

DND accepted our recommendations and committed to submit products or tools to the OPC for review prior to finalization, within nine months of the issuance of the report.

Further reading

- DND breached the *Privacy Act* in disclosing the identity of a workplace violence complainant who had an expectation of confidentiality

Compliance monitoring unit activities

Our investigative reports of finding often include recommendations to federal institutions. Our compliance monitoring unit is responsible for following up with institutions to verify recommendations have been successfully implemented. This helps us to ensure the success of institutions in meeting their commitments to our office as well as Canadians.

The compliance monitoring unit follows up on issues related to both the *Privacy Act* and PIPEDA.

In 2021-22, 7 public sector investigation reports were directed to the compliance monitoring unit and remain open. These included reports regarding IRCC, Correctional Service Canada, the RCMP, and the Canada School of Public Service. In such cases, the compliance monitoring unit actively engaged with the institution and provided feedback as appropriate.

RCMP implementing recommendations following investigation into use of facial recognition technology

In 2021, our office tabled a special report to Parliament on our investigation into the RCMP's use of Clearview AI's facial recognition technology.

The investigation found the RCMP had failed to properly assess the potential *Privacy Act* compliance risks that the use of Clearview's massive database and facial recognition technology clearly presented. Further, it did not have systems in place to track, identify, assess, and control such novel collection of personal information. We therefore recommended the RCMP institute systemic measures and pertinent training to ensure the collection of personal information is limited as required by the *Act*. These recommendations apply to any new technology involving the collection or use of personal information.

While the RCMP disagreed with certain of our findings that it contravened the Act, it nonetheless agreed to implement our recommendations.

With the creation of its National Technology Onboarding Program, the RCMP has made significant progress with its commitments. Since its initial launch, the program has received numerous requests to assess and evaluate various technologies; putting it in a position to satisfy the spirit of our recommendations.

At the time of writing, the RCMP advised us that budget and staffing challenges posed a risk to achieving a fully operational program.

That said, the RCMP worked closely with our compliance monitoring team. In addition to seeking advice and feedback on its plans, it has provided reports and details on the implementation of the recommendations to date. We will provide an update in the next annual report.

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 (June 10, 2021)
- Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta (February 2, 2021)

Privacy Act breaches

Breach reporting is mandatory in the public sector at the policy level, unlike in the private sector, where it is required by law. Public sector breach reporting practices remain a concern for our office.

Given the fluctuation in breach reporting over the last 5 years, the risk of under-reporting by federal government organizations continues to be a serious concern.

During the last fiscal year, we saw a 65% increase in breach reports received from public sector institutions (463 in 2021-22 compared to 280 in 2020-21).

However, the increase in breach reports is likely the result of new privacy awareness and breach reporting procedures at ESDC which accounted for a total of 349 of the breach reports submitted to our office in 2021-22 (an increase of 185 breach reports when compared to the 164 submitted in 2020-21). In total, ESDC accounted for 75% of the breach reports we received last year. The next largest reporting organization last year was CSC with 36 breach reports submitted to our office. We note that ESDC and Correctional Service Canada are large institutions which handle a significant volume of personal information.

As discussed in previous annual reports, we are concerned that several other large institutions have been conspicuously absent from the breach reports we receive. This includes many institutions that handle large amounts of personal information or highly sensitive information. Out of 288 government institutions subject to the *Privacy Act*, only 31 reported a breach to our office over the last fiscal year.

In other words, at least 257 organizations subject to the Act did not report any breaches last year.

If we remove the number of breaches reported by ESDC and CSC, our office only received 78 breach reports from institutions that are subject to the Act. This is a particular concern given the number of large government institutions handling vast amounts of personal information of both employees and the public.

Of further concern is that this is happening against a backdrop where 93% of the breach reports received by our office in 2021-22 involved human error. This further highlights the need for organizations to implement appropriate safeguards and to strengthen privacy awareness to ensure employees are aware of policies, procedures and legal responsibilities under the Act. This is an essential part of ensuring that organizations remain accountable for the personal information they collect, use and disclose.

Also, as we have noted in previous years, we continue to see very few breaches involving cyberattacks reported by government institutions, despite reports in the media that suggest they are happening with greater frequency and severity all around the world. In the past year we received a total of 5, compared with 9 in 2020-21. We remain concerned that overall reports of cyberattacks to our office remain low, especially when comparing the number of such breach reports under the *Privacy Act* to those under PIPEDA. Under PIPEDA, 45% of all breaches reported to our office related to cyberattacks.

In certain cases, we investigate privacy breaches, including those caused by cyberattacks. In addition to the CBSA investigation described in the next section, the OPC's investigation into

the cyberattack on the GCKey system used by approximately 30 government departments was ongoing at the time of writing.

In other cases, our Breach Response Unit reviews the breach report without a formal investigation. Reviews involve engaging with the institution and focus on analyzing the cause of the breach, understanding its impact and identifying measures to mitigate any resulting harm to individuals and prevent a breach recurrence.

We have noted certain trends through such reviews. For example, we increasingly see cyberattack breaches that bridge the private and public sectors. Three of the 5 cyberattack breaches reported to our office in 2021-22 involved private-sector service providers of federal institutions. Given we have also seen an increase in privacy matters involving private-public sector partnerships, security safeguard arrangements with service providers should warrant greater attention with government institutions in the future.

We have also observed that the involvement of IT and security specialists is often critical to ensuring a full assessment of any unauthorized access to or disclosure of information.

Either of these considerations could contribute to the under-reporting of breaches involving cyberattacks in the federal public sector, for example where accountability for breach reporting or breach impact are not properly understood.

To ensure more consistent reporting of breaches by federal government institutions, we reiterate our call for mandatory privacy breach reporting under the *Privacy Act* to help combat systemic under-reporting in the federal public sector.

Images of license plates at border crossings released on dark web after breach at CBSA contractor

The OPC initiated a complaint following media reports of a cyberattack targeting a U.S.-based third-party contractor used by both the CBSA and US Customs and Border Protection (CBP). The breach involved files transferred from the contractor's network and released on the dark web.

The CBSA advised our office in 2019 that the breach included approximately 9,000 photos of licence plates collected from travellers entering Canada at the Cornwall, Ont., border crossing.

Our investigation focused on determining the privacy impact of the breach on travellers entering Canada, and an assessment of the measures the CBSA took to ensure appropriate safeguards were in place.

The investigation revealed that the number of CBSA license plate images compromised in the breach was much higher than initially reported – as many as 1.4 million. Of those, approximately 11,000 were posted on the dark web.

Our investigation also found inconsistencies in the way the CBSA managed license plate information and a lack of security measures, including adequate contractual clauses to ensure the CBSA's private sector partner was properly protecting the information in its care.

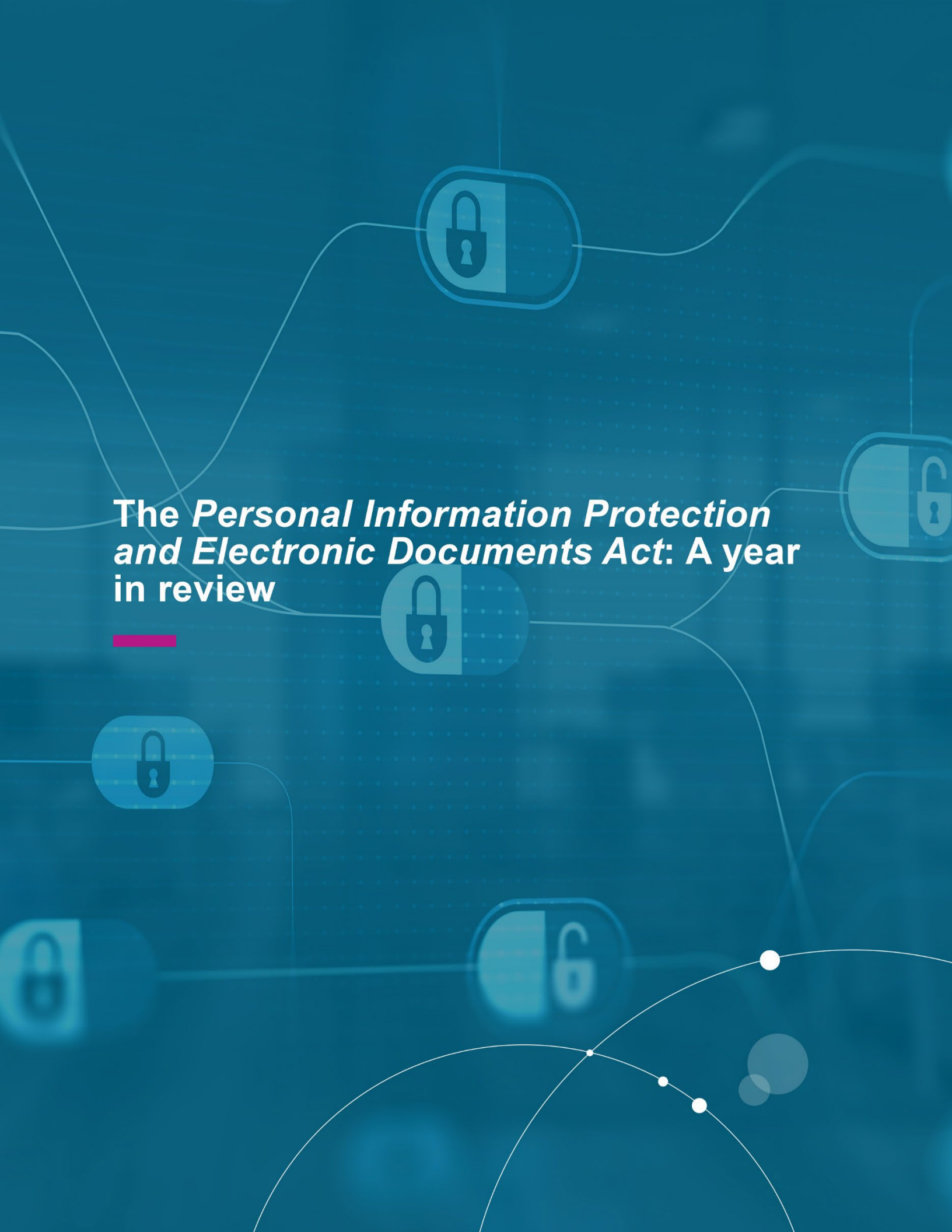
The OPC made a number of recommendations, including that the CBSA review its contract with its service provider to make it clear that licence plates constitute personal information and thus require appropriate protective measures related to storage, use, access and destruction.

Our investigation concluded that the complaint was well-founded and based on the CBSA's response to our investigation and acceptance of our recommendations, we considered the complaint to be resolved.

An important lesson learned in this case is that privacy obligations apply whether the data is processed by a government organization or a third-party contractor acting on its behalf – in such situations protecting privacy is a shared responsibility. It is also essential that institutions assess whether data being processed by external contractors constitutes personal information and to specify this in contracts.

Further reading

- Investigation into a privacy breach at a Canada Border Services Agency contractor



The *Personal Information Protection and Electronic Documents Act*: A year in review

The *Personal Information Protection and Electronic Documents Act*: A year in review

Over the year, our investigations work under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) included impactful collaborative enforcement initiatives with domestic and international counterparts to address privacy concerns related to emerging technologies.

For example, alongside our colleagues in Quebec, Alberta and BC, we completed a joint investigation into Tim Hortons' mobile app and the collection, use and disclosure of geolocation data. We found the company violated privacy laws in its collection of large amounts of sensitive location data through its app.

As discussed in other sections of this report, we also undertook significant work related to artificial intelligence and facial recognition technologies, including an initiative under the Global Privacy Assembly umbrella to develop principles and expectations related to the use of personal information in facial recognition technologies.

Some of the investigations highlighted in this section illustrate the importance of considering and addressing privacy issues before implementing new technologies. For example, we investigated a complaint related to a telecommunications company's voiceprint biometric authentication program. We also investigated complaints about surveillance technologies implemented by two transportation companies.

Our work under PIPEDA also included a significant focus on breaches resulting from cyber incidents involving compromised credentials. Some of the largest incidents cited in breach reports submitted to our office involved hacking, malware and phishing scams.

Notably, the overall number of breaches reported to our office has shown a marked decrease. In fact, this is the first year since November 2018 (when mandatory breach reporting came into effect) that the number of breach reports submitted to our office decreased as compared to the previous year. Moreover, this has occurred at a time when many organizations transitioned to remote work due to the pandemic. Given the privacy risks associated with telework and hybrid working arrangements, we would have expected to receive more breach reports, not fewer.

With the goal of continuing to increase efficiency, provide greater certainty for businesses and provide high quality service to Canadians, we used a variety of tools over the last year to conclude investigations as effectively as possible, resulting in more than 85% of PIPEDA files closed strictly through early resolution.

Greater use of early resolution and other efficiencies led to significantly shorter treatment times for complaint investigations – 7.8 months compared to 12.2 months the previous year.

As noted earlier, we saw the number of backlog cases begin to increase this year, following the end of temporary funding received in the 2019 federal budget. At the end of March 2021, there were 29 PIPEDA complaints older than 12 months, representing approximately 12% of our active investigations under PIPEDA. We will work to identify further efficiencies to prevent a significant backlog.

The following section highlights key outcomes under PIPEDA in 2021-22.

PIPEDA breaches

Last year, our office received 645 breach reports, affecting at least 1.9 million Canadian accounts. This represents a 17.5% decrease in reports received over the previous year. Although down substantially in 2021-22, breaches continue to be a significant area of concern for our office.

Of course, our office can only report on the breaches that we know about. Given the sheer volume of personal data that is collected, used and disclosed in the digital marketplace, many cases likely go unreported, or even undetected.

The drop in reported breaches comes at a time when more businesses have moved online due to the COVID-19 pandemic. As a result, we would have expected to see an increase in the number of breaches reported by sectors such as by the retail sector. However, reports from that sector were actually down year-over-year.

Top 5 sectors by percentage of total breaches reported

Industry sector	2018-19	2019-20	2020-21	2021-22
Financial	22%	19%	22%	20%
Telecommunications	17%	17%	14%	14%
Insurance	8%	11%	9%	14%
Professional services	4%	4%	8%	12%
Sales and retail	18%	14%	10%	8%
Manufacturing	4%	3%	6%	8%

That being said, we remain concerned about under-reporting from small- and medium-sized businesses, given they represent close to 90% of businesses in Canada. In the current digital economy, small organizations can often amass large amounts of sensitive personal information. A majority of the breach reports received by our office continue to come from large organizations.

Percentage of breaches reported by type

Breach Type	2018-19	2019-20	2020-21	2021-22
Unauthorized access	57%	59%	64%	65%
Unauthorized disclosure	26%	21%	28%	25%
Theft	9%	9%	5%	3%
Loss	9%	11%	3%*	7%*

* Figures may not add to 100 due to rounding

The leading cause of breaches involved unauthorized access, with 419 reported incidents (65%). These incidents often involved external actors gaining access to systems. It also

includes scenarios where employees viewed information without authorization and used the information for inappropriate purposes.

Among the unauthorized access reports, a total of 290 (69%) were cyber incidents involving malware, ransomware, hacking and phishing.

Meanwhile, a quarter of breaches were caused by unauthorized disclosures, including employee errors involving misdirected communications and disclosures resulting from a failure of technical safeguards and system vulnerabilities.

Bringing efficiencies to breach processes

Our office has worked to implement a number of measures to streamline our breach reporting and review processes to help us provide more timely feedback to organizations.

In the 2019-20 fiscal year we launched a secure portal for reporting breaches that allows businesses to easily submit their breach reports and instantly receive a file number, which facilitates future communication regarding the breach.

As noted above, organizations subject to PIPEDA are required to report to our office all breaches of security safeguards involving personal information that pose a real risk of significant harm (RROSH) to individuals.

To assist with our assessment of compliance with this reporting requirement, our office has developed and implemented an innovative new tool, based on risk science, to assess harm in breaches. The tool considers factors such as the sensitivity of personal information involved, and the probability that the information has been, is being, or will be misused. We are using the tool in-house and a version of the tool is scheduled for public launch by the end of the 2022 calendar year. The goal is to more quickly and consistently identify breaches where there is a likelihood of RROSH, triggering mandatory reporting, and offer guidance to help reporting organizations subject to PIPEDA better assess risks, manage incidents and mitigate harms to affected Canadians.

Law reform and breach reporting

Given its positive impact in protecting Canadians' privacy, it is our view that any future private sector privacy law should continue to require mandatory reporting of breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals. However, given the lag we see in reporting of breaches to the OPC, we have recommended organizations be required to report a breach to the OPC no more than 7 days after they become aware of it. While C-27 retains mandatory obligations for organizations related to privacy breaches, it preserves the current terms found in PIPEDA where reports are to be provided to the OPC "as soon as feasible after the organization determines that the breach has occurred."

Breach investigations

MGM Resorts breach affected 1.9 million Canadians

The OPC engaged with MGM Resorts International Inc. in 2020 after becoming aware of media reports of a data breach that had occurred 7 months earlier, affecting more than 10 million people. Having not received a breach report about the incident, the OPC wanted to find out more about it, including whether it involved the personal information of any Canadians.

After the OPC contacted MGM in February 2020, MGM analyzed the breach and confirmed that nearly 2 million Canadians had been affected; including 5,635 whose government identifier (e.g., passport number, Nexus number, health card number, or military identification number) had been compromised. In June 2020, MGM submitted a breach report to the OPC and began notifying affected Canadians.

Given the potential impact of the breach and considering the significant passage of time between MGM's confirmation of the breach and its assessment of its impact on Canadians, the Commissioner initiated a complaint to investigate whether MGM had adequately complied with its mandatory breach reporting obligations under PIPEDA. Specifically, we looked at whether the breach met the RROSH threshold under the law, and if it did, whether MGM had notified the OPC as soon as feasible, as required by PIPEDA.

When it assessed the risk of the breach to affected individuals, MGM did not conclude that the breach created a real risk of significant harm, given "the poor and disorganized state, the possibility of the relevant information being expired or invalid, and the non-sensitive nature" of the affected data.

The OPC believes that government-issued identifiers constitute sensitive information, as do other data involved in the breach when combined with other personal information. Based on our technical analysis, we found it would be possible, without significant time or effort, for a malicious actor to piece the personal data together in such a way as to identify the personal information in the breached data.

As a result, we found that the breach created a RROSH to affected individuals, and that as MGM had not commenced a RROSH analysis until 7 months after the breach (as it first focused its efforts on affected U.S. customers, who were notified of the breach 2 months after its occurrence, in September 2019), it had not notified our office or affected individuals as soon as feasible.

MGM commenced notifying affected Canadians in June 2020, which was almost 11 months after MGM had first become aware of the breach. This delayed notification left affected Canadians unable, for almost a year, to take steps to mitigate any further harm that may have resulted from their personal information being breached.

MGM committed to amending its privacy breach response framework to ensure that when it learns of a breach that may affect Canadian residents, it will:

- Promptly assess whether the breach constitutes a real risk of significant harm, consistent with guidance published by the OPC; and

- Provide a breach report as soon as possible to the OPC and notify affected individuals as soon as feasible if it is determined such a risk exists.

We considered the matter to be well-founded and conditionally resolved.

Further reading

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

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

Marriott International, Inc. experienced a data security breach involving unauthorized access to a hotel database which it had acquired as a result of its purchase of Starwood Hotels in 2016. Marriott advised that an attacker obtained access to the personal information contained in approximately 339 million records, including up to 12.8 million records in which Canada was listed as the country of residence.

The breach involved Starwood guest profile and contact details, as well as Starwood Preferred Guest account and reservation information. For a subset of individuals, passport details (passport numbers, passport country code, or the country of the guest's passport) and/or encrypted payment card details were also affected.

In response to the breach, Marriott engaged with an outside law firm and a third-party forensic firm, deployed enhanced monitoring and forensic tools on the Starwood network, installed additional monitoring tools in Starwood's data centres to alert for suspicious behaviour, and began notifying affected individuals. Marriott also updated its security plan.

Through our investigation, we learned that the attacker had introduced malware into the Starwood system prior to Marriott's acquisition of that system. We found that certain allegations in the complaints were well-founded because at the time of the breach, Marriott's safeguard and accountability measures were inadequate. These inadequacies highlight key lessons to all organizations for avoiding or mitigating the damages of a breach. This includes the importance of organizations to:

- maintain anti-virus testing and access controls by promptly identifying and resolving deficiencies in these safeguard measures;
- use appropriate encryption methods to protect personal information;
- delete personal information in a timely way through adequate processes and procedures;
- identify threats by establishing and implementing comprehensive logging and monitoring; and
- continually assess and review security safeguards, which is particularly important when organizations acquire new assets (as Marriott had in this case).

Since the breach, Marriott has made a number of enhancements, such as conducting regular vulnerability scans of corporate servers; ensuring better authentication before employees are able to log into certain accounts (including human resources and payroll systems); and updating its incident and crisis management policies.

Additionally, Marriott agreed to engage an experienced and independent accredited external assessor to evaluate the enhancements it has undertaken towards preventing a similar privacy breach from re-occurring on its systems.

As a result, our office considers these complaints well-founded and conditionally resolved.

Further reading

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

PIPEDA enforcement

General complaint and investigations statistics and trends

In 2021-22, our office accepted 427 complaints under PIPEDA, a 38% increase from the previous year. We accepted 309 complaints in 2020-21.

We received the greatest proportion of complaints against businesses in the financial (24%), telecommunications (12%), Internet (10%) and accommodations (10%) industries. Use and disclosure of personal information (36%) was the top complaint category from individuals, followed by access (28%), collection of personal information (13%) and retention of personal information (8%).

As noted earlier, our online complaint form has continued to help us find efficiencies by allowing us to better direct complainants and request necessary documentation and information at the outset of a process, reducing the back-and-forth with complainants and respondents.

Our office closed 358 complaints in 2021-22, a 21% increase from the previous year (2020-21) in which we closed 296 complaints.

Investigations

Tim Hortons violated privacy laws by collecting vast amounts of personal data through its app

A joint investigation by our office and provincial counterparts in Quebec, Alberta and BC found Tim Hortons' mobile app tracked and recorded its customers' movements every few minutes of every day, even when the app was not open. It used that information to infer the app user's home and place of work, and when they were visiting a competitor or travelling.

We concluded that Tim Hortons' continual collection of vast amounts of location information was not proportional to the benefits the company may have hoped to gain from better targeted promotion of its coffee and other products, such that the practice was "inappropriate" and in violation of Canadian privacy laws.

The investigation further found that Tim Hortons had attempted to obtain consent via unclear, and in certain circumstances, misleading statements that did not allow individuals to understand the consequences of agreeing to be tracked by the app.

While Tim Hortons stopped continually tracking users' location in 2020 after the investigation was launched, that decision did not eliminate the risk of surveillance. The investigation identified that Tim Hortons' contract with an American third-party location services supplier contained language so vague and permissive that it would have allowed the company to sell "de-identified" (but potentially re-identifiable) location data for its own purposes.

The investigation also revealed that Tim Hortons lacked a robust privacy management program for the app, which would have allowed the company to proactively identify and address many if not all of the privacy contraventions the investigation found.

The four privacy authorities made a number of recommendations, including that Tim Hortons delete any remaining location data and direct third-party service providers to do the same.

Tim Hortons agreed to implement the recommendations. As a result, our office concluded this matter to be well-founded and conditionally resolved.

Further reading

- Joint investigation into location tracking by the Tim Hortons App (June 1, 2022)

Telecommunications firm failed to obtain appropriate consent for voiceprint authentication program

In a complaint against Rogers, a customer alleged the company enrolled her in its voiceprint biometric authentication program, Voice ID, despite her refusal to be part of the initiative. After discovering she had been enrolled, she called Rogers and once again opted out of the program. In a subsequent call, she discovered she was again enrolled without her knowledge or consent.

Rogers told investigators the Voice ID program was designed to be an authentication and anti-fraud solution for securing customer accounts. The program uses algorithmic voiceprints, which are created when individuals contact call centres. On subsequent calls, the voiceprint can be matched to help authenticate a caller's identity.

Upon investigation, we determined that Rogers failed to obtain valid and meaningful consent for its Voice ID program.

Given the sensitivity of biometric voiceprints, we concluded that express consent was required before collection. However, Rogers collected voiceprints in the background of calls before seeking consent.

While Rogers ostensibly required its customer service agents to obtain express consent before associating the voiceprint to an account, we found that Rogers' customer service representatives failed to obtain express consent from the complainant in this case.

We further found that it was easy for customer service agents to bypass the consent requirement, and that there were deficiencies in processes, training and monitoring to ensure agents' compliance with Rogers' consent protocols. Given these factors, we determined that Rogers did not obtain valid consent for its Voice ID program.

We also found Rogers had retained voiceprints improperly in cases where individuals had opted-out for no actual purpose. It had intended to continue using the voiceprints for fraud detection but never did.

In response to our investigation, Rogers agreed to make a number of significant changes to its Voice ID program. It committed to obtaining express consent from individuals; more clearly informing customers of their ability to opt out; and deleting voiceprints upon opt-out. Rogers will also delete the voiceprints of individuals who previously opted out of Voice ID, implement significant changes to documents and agent training that outline the initiative, and implement monitoring to ensure agent compliance with Voice ID consent protocols. Finally, it will reconfirm consent for previously enrolled individuals as they call in to call centres. As a result, our office concluded this matter to be well-founded and conditionally resolved.

Further reading

- Telecommunications firm failed to obtain appropriate consent for voiceprint authentication program

Transportation company using cameras with audio in truck cabs to monitor drivers

A truck driver complained to our office that his employer, Trimac Transportation Services Inc., had installed a dash camera in his vehicle that continuously recorded audio and video without his consent. He was particularly concerned about the audio recording functionality.

Trimac, one of the largest transportation service companies in North America, explained it deployed dash camera systems in truck cabins in 2017 to protect its assets and ensure the safe operation of company trucks. The system, which consists of a small device installed on the truck's interior windshield, captures forward facing video and audio within a Trimac truck's cabin. In the event of one of a predetermined set of risky driving behaviours, the system records clips, which are reviewed and categorized by a third-party processor before they are transferred to Trimac. At the time of the complaint, the system was continuously active when the truck was on (including when idling), even when the driver was off-duty and not driving.

We found drivers were subjected to up to 24/7 surveillance in that the system had to be continuously active to capture the clips. We also found that clips transferred to Trimac were available, with limited safeguards against unauthorized access, to more Trimac employees than necessary.

While we understand the importance of road safety and recognize the system could be effective in encouraging safe driving behaviours, our investigation found that continuous recording, particularly when drivers were off duty and not driving, was not necessary to meet Trimac's purposes and that the loss of privacy resulting from the implementation of the system was disproportionate to the benefits Trimac hoped to gain.

Our office recommended, and the organization agreed to employ, a less privacy-intrusive approach where, at a minimum, the audio recording functionality is active only when a driver is on-duty, or driving, and where access to clips transferred to Trimac is limited to those who need to know. Our office concluded this matter to be well-founded and conditionally resolved.

Further reading

- Investigation into Trimac's use of an audio and video surveillance device in its truck cabins

Transportation company's constant surveillance of drivers more intrusive than necessary

In a similar case, a truck driver complained that his employer, Oculus Transport Ltd., an interprovincial trucking company, was collecting audio recordings of all conversations that occurred in the cab of his truck, even while he was off-duty.

Oculus introduced surveillance devices in the cabs of its trucks, primarily to aid incident investigations and to ensure compliance with provincial regulations and private road

requirements. The devices were able to record audio within the cab, video out the front window of the truck, and real-time location information.

The audio collected had the potential to be sensitive as it would include conversations employees had in their trucks, such as private conversations with friends, family, doctors or other third parties.

Oculus explained that the audio recordings were safeguarded against unauthorized access and were only to be accessed in limited identified circumstances.

While we accepted that the audio surveillance in question was collected to address a legitimate need and that it may have been effective in achieving the company's purposes, we felt 24-hour-a-day collection, including when drivers were off-duty or asleep in the cab of the truck, was more intrusive than necessary, and that the impact on drivers' privacy was disproportionate to any benefits the company may have gained from the surveillance.

The company confirmed to our office that it is no longer using audio surveillance. We therefore consider the complaint to be well-founded and resolved. Should Oculus decide to implement in-cab audio surveillance in the future, we would expect the company to limit the collection of audio to what is necessary to achieve its purposes.

Further reading

- Transportation company's constant surveillance of drivers is more intrusive than necessary

Early resolution

As illustrated in its application with the public sector law, early resolution continues to be an invaluable tool to resolve complaints of a non-systemic nature. Complainants typically see an outcome in a few months, compared to other forms of investigation, which are much lengthier. We appreciate that many organizations work with our office to resolve matters up front, to the mutual satisfaction of all involved parties, without the need for a full investigation.

We closed 85% (or 303) of all PIPEDA complaints using early resolution in 2021-22, the highest proportion ever.

Percentage of all complaints closed in early resolution

Fiscal Year	Percentage of all complaints closed in early resolution
2021-22	85%
2020-21	71%
2019-20	69%
2018-19	63%
2017-18	66%

In addition to maximizing our use of early resolution, we continue to use summary investigations to conclude complaints, primarily where the facts can be readily ascertained, but a consensual resolution cannot be reached.

In 2021-22, our office's Early Resolution Unit initiated Advisory Letters, a new tool that will further streamline the most common complaints and allow our office to resolve matters more quickly. Advisory Letters set out the details of the complaint and remind organizations of their obligations under PIPEDA and our Office's expectations, without the need to make a finding. In time, the use of this new tool should enhance our ability to provide expeditious service to Canadians.

Early resolution success stories

COVID-19 testing company stops sending marketing emails

A company authorized by the federal government to administer mandatory COVID-19 tests at the Montreal-Trudeau airport became the subject of a complaint after a traveller who was required to submit to testing received an email promoting the company's other services, even though he had not consented to receiving marketing emails.

Our office launched an investigation, during which Biron Groupe Santé Inc., indicated that it initially felt it had established a business relationship with arriving passengers and thus relied on implied consent to send email ads.

After receiving several direct complaints from travellers and further engaging with our Office, the company stopped sending such marketing emails and deleted the email addresses of more than 147,000 arriving travellers who were not already clients from its marketing database.

The matter was deemed settled during the course of investigation and no findings were issued.

Our office and the Commission d'accès à l'information du Québec cooperated during the investigation by sharing information relevant to the OPC's review of the complaint.

Companies offering online accounts update authentication procedures

Several individuals complained to our office about authentication requirements to reactivate blocked accounts on various online platforms. The organizations were requiring copies of photo ID, such as drivers' licences, in order to authenticate accounts.

During our discussions, we learned that frontline staff receiving the account reactivation requests from complainants did not communicate that certain information on the ID – deemed unnecessary for authentication – could be redacted prior to submission.

In the end, we facilitated an improved communication strategy for the respondent companies, and the complainants became more comfortable with the account retrieval process, resulting in the early resolution of their complaint.

Compliance monitoring unit activities

When organizations sign compliance agreements, they agree to take binding actions to ensure their practices conform to the law. In other cases, organizations agree to implement our recommendations following an investigation.

When such agreements are made, it is important that we follow up. Our compliance monitoring unit is responsible for doing just that to verify whether commitments made are being addressed according to any timelines laid out.

Desjardins addressing issues that led to massive breach

In 2019, Desjardins notified our office of a breach that ultimately affected close to 9.7 million individuals in Canada and abroad – the largest-ever data breach in the Canadian financial services sector. We found that, due to gaps in administrative and technological safeguards, a Desjardins employee was able to access and exfiltrate clients' personal information including names, birthdates, social insurance numbers, addresses, email addresses and transaction histories.

Our investigation, conducted in collaboration with la Commission d'accès à l'information (CAI) du Québec, concluded that Desjardins violated PIPEDA with regard to accountability, data retention periods, and security safeguard measures.

Desjardins agreed to implement our recommendations to improve its information security and protection of personal information, including its data destruction practices. It also agreed to engage external auditors to assess and certify its programs and to submit an assessment report to our office.

Desjardins has been cooperative, reporting on its implementation of a comprehensive action plan addressing those issues every six months. It is making good progress on its implementation of our recommendations and its action plan. An audit of its governance/accountability and security improvement measures is due to the OPC in December 2022.

We will continue to monitor Desjardins' progress until it has demonstrated that it has met the terms of the recommendations outlined in our final report.

Further reading

- Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019 (December 14, 2020)
- Combination of weaknesses led to massive data breach at Desjardins (December 14, 2020)

Advice and outreach to businesses

The OPC's Business Advisory Directorate engages with businesses subject to PIPEDA to help them proactively assess and address any privacy risks associated with their initiatives and practices. The aim is to support them in complying with the law as they adopt new technologies and innovative business models.

Our office carried out a range of compliance promotion activities to provide specific and practical advice to businesses so that they are properly informed and guided in terms of their obligations under PIPEDA. In all, we initiated 14 new advisory activities this fiscal year and conducted 25 outreach activities in various industry sectors. There were 18 consultations ongoing at year-end.

The following are examples of our Business Advisory work:

Apple continues consultation on Apple Maps image collection project

Apple Inc. voluntarily requested its first advisory consultation for its Apple Maps Image Collection Project in Canada in 2019. Our Business Advisory team has since provided PIPEDA compliance advice and privacy recommendations to Apple on progressive phases of the Apple Maps street cartography and mapping project. Given the scope of this project, we have sought input from our provincial counterparts with privacy laws substantially similar to PIPEDA. Our recent recommendations built on earlier PIPEDA compliance advice and were well received by the organization.

SME seeks advice on online marketplace for artistic talent

A company engaged with our office after attending one of our virtual Privacy Clinics to request an advisory consultation on its online marketplace for creative talent. Specifically, the company sought comprehensive advice on its personal information management practices. The organization appreciated the advice and was receptive to specific recommendations.

Contributions Program

Each year the OPC furthers privacy policy development and promotes the protection of personal information in the private sector through its Contributions Program. Since its inception in 2004, the program has allocated approximately $8 million to some 180 projects.

For the 2022-23 funding cycle, we asked for proposals for research projects that dealt with the topic: “Who is impacted and how: Assessing and mitigating privacy risks, barriers and inequalities.” We wanted to explore the range of privacy-related experiences, barriers and inequalities diverse groups of people face, and how that impact might be mitigated.

We received 33 proposals, which we evaluated based on merit, and selected 11 projects for funding. We awarded up to $50,000 per project, out of a total budget of $500,000, to a variety of non-profit organizations, including academic institutions and advocacy groups. This year’s projects range from an examination of the impact of PIPEDA on First Nations data sovereignty, to public perspectives on facial recognition technology, to privacy in virtual classrooms.

For 2021-22 the OPC enhanced its efforts to attract a broader range of applications and was pleased to receive proposals from across Canada, including a successful application from Nunavut. That project will look at privacy, artificial intelligence and machine learning through a “rural, remote and Indigenous lens.”

Further reading

- OPC announces new funding recipients for independent research: Assessing and mitigating privacy risks, barriers and inequalities (June 20, 2022)
- Contributions Program projects underway (June 20, 2022)

Highlights of other OPC work

Highlights of other OPC work

Advice to Parliament

2021-22 was another unusual year in terms of parliamentary activity, with COVID-19 and the federal election disrupting routine parliamentary business.

The OPC continued to proactively work with Parliament, appearing a number of times before various parliamentary committees in response to bills and studies on topics such as the use and impact of facial recognition technology, the use and collection of mobility data by the Government of Canada, and restricting young persons' online access to sexually explicit material.

Study on the use and impact on facial recognition technology

The OPC shared its views on the use of facial recognition technology during an appearance before the Committee on Access to Information, Privacy and Ethics (ETHI) in early May 2022. The committee had undertaken a study on the use and impact of this emerging technology.

We highlighted our work in this area, including our investigations of Clearview AI and the RCMP's use of Clearview's technology as well as a national public consultation on police use of facial recognition technology, which led to a joint statement by federal, provincial and territorial privacy guardians on the need for a legislative framework to establish protections against the risks associated with the technology. (This is discussed in greater detail in the section on law reform above.)

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 (May 2, 2022)

Collection and use of mobility data for COVID-19 tracking

The OPC appeared in February before ETHI as part of its study of the collection and use of mobility data by the Government of Canada.

During the appearance, we noted that the case illustrates the urgent need for law reform – in this case, to authorize the use of personal data for socially beneficial purposes and legitimate commercial interests within a rights-based law that acknowledges the nature and value of privacy as a human right. We said this movement of data between the private and public sectors demonstrated the need for both to be governed by common principles and rules, and held to similar standards.

Our office had received complaints about the use of such data by the Public Health Agency of Canada in its efforts to track the spread of COVID-19. Given an investigation was ongoing at the time of the appearance, we were not in a position to respond directly to issue of whether the information had been properly de-identified.

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 (February 7, 2022)
- Statement from the Privacy Commissioner following release of ETHI report into the government's collection and use of mobility data (May 4, 2022)

Appearance on bill to restrict young persons' access to sexually explicit material online

The OPC appeared before the Senate Standing Committee on Legal and Constitutional Affairs to discuss Bill S-203, *An Act to restrict young persons' online access to sexually explicit material*. During the appearance, we noted that while the OPC supports efforts to incorporate special consideration for children's rights in the digital environment, the bill raised a number of privacy-related issues related to the requirement to collect personal information to facilitate the age-verification scheme.

Further reading

- Appearance before the Senate Standing Committee on Legal and Constitutional Affairs on Bill S-203, *An Act to restrict young persons' online access to sexually explicit material* (June 2, 2021)

OPC responds to Senator's *Competition Act* consultation

The OPC was invited to participate in a consultation by Senator Howard Wetston examining the *Competition Act* in the digital age. The OPC was able to draw from its leadership experience in this area as co-chair of the Global Privacy Assembly's Digital Citizen and Consumer Working Group (DCCWG), which has examined issues related to the intersection between privacy and competition law.

The nature of the digital economy has created an increasing cross-regulatory intersection between privacy, competition and consumer protection, the OPC opined in the submission. Data and privacy considerations will play an increasingly important role in competition policy, and as such, the need for cross-regulatory collaboration will continue to grow as well.

Further reading

- Examining the Canadian *Competition Act* in the Digital Era (December 21, 2021)

International and domestic cooperation

Domestic and international enforcement cooperation in the area of privacy law, and across regulatory spheres, is increasingly critical in a digitized world where data flows transcend borders. Cross-jurisdictional and cross-regulatory collaboration helps to ensure better protection of the rights of citizens. Enforcement collaboration expands our capacity to take actions and amplifies the compliance impact of those actions. It can also benefit organizations by streamlining investigative processes and promoting greater harmonization in the application of laws.

Cooperation with other data protection authorities in Canada and beyond has become an increasingly important focus of our work over the years, while cooperation with authorities outside of the realm of privacy, including in the areas of competition, is beginning to gain momentum. The following summarizes some key initiatives in 2021-22.

International cooperation

Protecting the personal information of Canadians increasingly involves enforcing Canada's laws against companies located, and carrying out business, in other countries.

Our office tracks international developments in legal, technological and business realms that may ultimately affect Canada. We are involved in a number of global, regional and linguistic forums where privacy authorities participate to share experiences and coordinate efforts at setting policies and establishing best practices. These types of activities present significant opportunities and provide substantial benefits in terms of operational efficiencies and overall improved privacy protections for Canadians.

Some examples of our international collaboration work in 2021-22 include:

Global Privacy Assembly

The OPC is an active member of the Global Privacy Assembly (GPA), which connects more than 130 data protection and privacy authorities from around the world and plays a central role in fostering international collaboration. Our office chairs or participates in a variety of GPA working groups and is involved in collaborative work on globally relevant topics such as AI and facial recognition technology, digital education and data sharing. We also work to draft and sponsor resolutions on these and other topics of global concern.

International Privacy and Human Rights Working Group

In our role as chair of this GPA working group, our office oversaw the adoption of a report – Privacy and data protection as fundamental rights: A narrative – that examines the relationship of privacy to other fundamental rights.

2021 conference and resolutions

Key themes of the 43rd GPA conference, held virtually in October 2021, included the promotion of a human-centric approach to privacy protection as well as working toward a global regulatory environment with high standards of data protection. Among the resolutions adopted:

- a resolution advocating for respect of key privacy principles when governments access personal information held by the private sector for national security and public safety purposes;
- a resolution on children's digital rights, which aims to strengthen the protection of children's rights in the digital environment; and
- a resolution to establish a GPA working group that will focus on identifying approaches to sharing data for the public good.

International Enforcement Working Group

Our office continues to serve as co-chair of the GPA's International Enforcement Working Group (IEWG). Given the foundational importance of enforcement cooperation, the IEWG is a permanent working group of the GPA. The group's mandate is to foster proactive and practical enforcement cooperation on critical issues of interest to the international privacy enforcement community.

The working group, with 34 members, serves as a forum for enforcement cooperation. The group held several virtual sessions to share perspectives on global privacy risks such as adtech and data scraping. These discussions led to the creation of topic-specific subgroups to advance compliance initiatives. Our office contributed to several of these subgroups, namely the:

- Credential stuffing subgroup to develop guidance for organizations and the general public;
- Data scraping sub-group to draft a joint statement to raise awareness of the risks and mitigating strategies related to data scraping;
- AdTech sub-group to help promote greater understanding of issues related to the AdTech ecosystem; and
- Facial recognition technology sub-group, a joint sub-group of the IEWG and AI working group, to develop principles and expectations related to the use of personal information in facial recognition technologies.

Digital Citizen and Consumer Working Group

Our office is a co-chair to the Digital Citizen and Consumer Working Group (DCCWG), which since 2017, has been focusing on the growing intersection between privacy, competition and consumer protection, and promoting cross-regulatory cooperation between those spheres. Given the importance of this work in ensuring a privacy-protective global digital economy, the DCCWG has been recently made a permanent working group of the GPA.

The group produced a survey report entitled "Privacy and Data Protection as Factors in Competition Regulation: Surveying Competition Regulators to Improve Cross-Regulatory Collaboration," which was launched at the 2021 GPA conference. The OPC was the lead author of the report, which aimed to identify opportunities for better cooperation between privacy authorities and authorities working to regulate competition.

The DCCWG also commissioned a complementary academic report, which provides an in-depth analysis of the intersection of privacy and competition regulation, exploring the two regulatory spheres' complements and tensions, along with outlining benefits of cross-regulatory collaboration.

Finally, the DCCWG has been advocating for greater recognition of privacy in competition regulatory instruments, and this year authored a submission to the US Federal Trade Commission and US Department of Justice's joint consultation aimed at modernizing American merger guidelines to better detect and prevent anticompetitive deals.

Our office has played a leading role in promoting and advocating for cross-regulatory cooperation among regulators and key stakeholders through public speaking engagements and media interviews and will continue to lead this priority global discussion with our privacy authority counterparts in other jurisdictions.

Further reading

- Digital Citizen and Consumer Working Group, 2021 Annual Report (August 2021)

Global Privacy Enforcement Network

The Global Privacy Enforcement Network (GPEN) is an informal network which empowers privacy enforcement authorities to share knowledge, experience and best practices on privacy enforcement and co-operation. It also coordinates joint enforcement initiatives, such as the Global Privacy Sweep (now in its 8th year), to foster greater compliance with global privacy laws. Our office is a member of the GPEN executive committee along with counterparts from the United Kingdom, Hong Kong, Israel and the United States. GPEN focuses on establishing strong relations at the enforcement practitioner level and has held Investigative workshops to share strategies and techniques.

GPEN marks its 10-year anniversary in 2022. In February, the executive committee hosted an event to begin discussions on renewing an action plan for the informal network's next decade.

G7 Data Protection and Privacy Authorities

In September 2021, our office participated in a roundtable of data protection and privacy authorities from G7 countries. Discussions underlined the need for data protection and privacy authorities to work together to develop strategies to oversee global data flows.

The meeting took place in the context of the Roadmap for Cooperation on Data Free Flow with Trust, announced by G7 Digital and Technology Ministers in April 2021.

The growing global, data-driven economy as well as the changes being driven by the ongoing pandemic made the meeting even more timely.

As the data protection and privacy regulators of the world's most advanced digital economies, the G7 authorities agreed to strengthen collaboration, play a leadership role in discussions pertaining to digital issues and help influence the adoption of higher standards for data protection around the world.

G7 authorities agreed to meet on an annual basis to discuss issues of mutual interest. This would also help the group forge a stronger relationship, voice and influence with international organizations and other key international stakeholders, with the aim of promoting shared values and objectives.

Further reading

- Communiqué from September Roundtable of G7 data protection and privacy authorities (September 7-8, 2021)

New memorandums of understanding

The OPC renewed and updated a Memorandum of Understanding (MOU) with Autoriteit Persoonsgegevens, the data protection authority for the Netherlands, to facilitate information sharing between the two organizations.

The OPC also signed an MOU with the Commissioner of Data Protection of the Abu Dhabi Global Market to facilitate information sharing between the two organizations.

Federal, provincial and territorial collaboration

Federal, provincial and territorial information and privacy commissioners meet annually to coordinate on matters of public policy and public education including calling for action that will encourage consistent privacy protections for individuals across the country. The next Annual Meeting is scheduled to take place in September 2022, in St. John's, Newfoundland and Labrador. The Commissioners also meet virtually on a monthly basis to discuss issues of mutual interest and advance joint projects.

We often also work with our provincial and territorial colleagues on key initiatives, including our joint call to legislators to develop a legal framework that clearly and explicitly establishes the circumstances in which police use of facial recognition may be acceptable, as discussed earlier in this report.

As well, building on the success of last year's joint investigation into Clearview AI and Cadillac Fairview, we collaborated with four provincial counterparts on an important investigation into Tim Hortons' mobile app, also discussed earlier in this report. This fiscal year represented a historical high-water mark for domestic enforcement collaboration, with our office, along with counterparts in B.C., Alberta and Quebec, receiving the Global Privacy Assembly's award for dispute resolution in recognition of joint enforcement actions related to facial recognition.

Memorandum of understanding

Our office also renewed a longstanding memorandum of understanding with the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for British Columbia to include the Commission d'accès à l'information of Quebec.

The MOU sets out a framework to better support federal/provincial collaboration and coordination in order to leverage the resources of the offices to maximize capacity and the impact of oversight activities, while at the same time reducing inefficiencies and any duplication of effort. It will also help to increase knowledge sharing and enhance relationships between the offices in order to ensure consistent, coordinated, efficient and harmonized oversight of private sector privacy in Canada, while carrying out joint instructions of the various Privacy Commissioners involved.

The primary vehicles for achieving the objectives set out in the MOU are the Private Sector Privacy Forum and the Domestic Enforcement Cooperation Forum. The Private Sector Privacy Forum, which includes representatives of the OPC along with provincial counterparts with oversight of private sector privacy laws (B.C., Alberta and Quebec), meets on a quarterly basis to identify opportunities for collaborative policy and public education, as well as to advise and update each other on proposed and ongoing initiatives.

The Domestic Enforcement Cooperation Forum facilitates discussions amongst participating authorities with a view to more effectively protect the privacy rights of Canadians, including by identifying opportunities for information sharing and collaboration on joint or parallel investigations and sharing enforcement challenges as well as practical solutions developed to address them.

Our office also signed an MOU with the Office of the Information and Privacy Commissioner of Nunavut to facilitate information sharing between the two organizations.

Further reading

- Privacy guardians sign collaboration agreement (May 10, 2022)
- OPC signs information-sharing agreement with Nunavut counterpart (December 7, 2021)

Before the Courts

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)

The OPC's Facebook litigation continued this year.

Facebook 1 is a Federal Court application brought by the OPC in February 2020, under paragraph 15(a) of PIPEDA, following an investigation and issuance of a report of findings regarding a complaint concerning the personal information-handling practices of the respondent, Facebook Inc.

The 2019 joint investigation by the OPC and the Office of the Information and Privacy Commissioner for British Columbia found major shortcomings in the social media giant's privacy practices. Facebook disputed the findings and refused to implement recommendations to address the deficiencies identified.

The OPC then filed a Notice of Application in the Federal Court seeking a declaration that Facebook had contravened PIPEDA, and various other remedies. Among other powers, the Federal Court can impose binding orders requiring an organization to correct or change its practices and comply with the law.

The OPC's 2018-2019 Annual Report provides details of the investigation and the April 2019 Report of Findings.

The OPC's 2019-2020 Annual Report summarizes its Notice of Application and the relief that it is seeking.

In March 2020, our office served Facebook with our affidavit evidence in support of the s.15 application. In response, Facebook brought a motion to strike portions of our affidavit.

In April 2020, Facebook also brought an application for judicial review under s. 18.1 of the *Federal Courts Act* of our Report of Findings (Facebook 2). In this matter, Facebook is seeking judicial review of our decision to investigate and continue to investigate, and the investigation process, and seeks to quash the resulting report of findings.

In response, our office brought a motion to strike Facebook's application for judicial review on the basis that Facebook is out of time to bring such a challenge and has an adequate alternative remedy in its legal right to respond to our office's ongoing application under section 15 of PIPEDA (Facebook 1).

The motions were heard on January 19 and 21, 2021. On June 15, 2021, the Federal Court released its decision on these motions. With respect to Facebook's motion to strike large portions of the OPC's affidavit, the Court was largely unpersuaded that the OPC's affidavit evidence was inadmissible and held that only a certain limited number of paragraphs and exhibits to the affidavit should be struck. The Court also dismissed our application to strike Facebook's application for judicial review, finding that there was at least a debatable issue as to whether there is an adequate alternative remedy for Facebook in the PIPEDA application, such

that Facebook's arguments were not so bereft of any chance of success to justify striking out its application at this stage.

In February 2022, the parties completed cross examination of witnesses on affidavits filed in both the s. 15 PIPEDA application and the judicial review proceeding. On April 11, 2022, Facebook filed its submissions in the judicial review proceedings with the Court. The OPC filed its submissions in response with the Court by April 28, 2022.

In the s. 15 PIPEDA proceeding, the OPC brought a motion to file supplemental affidavit evidence in May 2022. The motion sought further, or in the alternative, that the Court require Facebook's affiant to answer the more than 70 questions refused during cross-examination. The hearing took place in Toronto over two days – May 30, 2022 and June 10, 2022. The Court ordered Facebook's affiant to make herself available to be re-examined by the OPC on certain questions raised in the initial cross examination, and ruled on the propriety of the OPC's questions and Facebook's refusals. The Court dismissed the OPC's motion to file additional affidavit evidence; with leave to reapply following the completion of the cross-examination on July 26, 2022.

The OPC filed its application record in the s.15 proceeding on the merits of the case on August 19, 2022.

The Court ordered that the judicial review application and the s.15 application be heard consecutively, before the same judge. Hearing dates have not yet been set.

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

The reference proceeding concerning whether PIPEDA applies to Google's search engine service continued this year. In 2018, pursuant to section 18.3 of the *Federal Courts Act*, the OPC referred two questions of law and jurisdiction for hearing and determination. The questions arose in the context of a complaint from an individual alleging that Google is contravening PIPEDA by continuing to prominently display links to online news articles concerning him in results when his name is searched using Google's search engine service. The complainant requested that Google remove the articles in question from results for searches of his name.

The questions were as follows:

Does Google LLC in the operation of its search engine service, collect, use or disclose personal information in the course of commercial activities within the meaning of paragraph 4(1)(a) of PIPEDA when it indexes web pages and presents search results in response to searches of an individual's name?

Is the operation of Google's search engine service excluded from the application of Part I of PIPEDA by virtue of paragraph 4(2)(c) of PIPEDA because it involves the collection, use or disclosure of personal information for journalistic, artistic or literary purposes and for no other purpose?

The Federal Court issued its decision on the merits of the Reference questions in July 2021. The Court agreed with the OPC's position that PIPEDA applies to Google's search engine service. The Court's answer to the first question was "Yes" – Google is collecting, using, and

disclosing personal information in the course of commercial activities when operating its search engine service. The Court's answer to the second question was "No" – Google's search engine service is not exempt from the application of PIPEDA by virtue of the journalistic exemption found in paragraph 4(2)(c) of the Act, because it does not operate for a journalistic purpose, and certainly not for an exclusively journalistic purpose.

On September 28, 2021, Google filed a Notice of Appeal, seeking an Order striking or declining to answer the reference questions on the basis that the questions should not or could not be answered without also addressing the issue of whether a potential requirement to remove links from search results would violate section 2(b) of the *Canadian Charter of Rights and Freedoms*, or alternatively, an Order answering the second reference question in the affirmative.

The OPC, the Attorney General of Canada, and the complainant are participating as respondents to the appeal. The Federal Court of Appeal also granted leave for both the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic and a coalition of Canadian media entities to participate as interveners in the proceeding.

A hearing of the appeal is expected to take place in October 2022.

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

Provided certain conditions are met and upon registering with Health Canada, medical users may grow their own cannabis, or designate someone to grow it for them. Health Canada received requests for information about these registrations under the *Access to Information Act*, including requests for information such as the first 3 digits of postal codes of registered personal producers. Health Canada's position is that it should only release the first digit of a postal code as including more would unacceptably increase the risk of disclosing information about identifiable individuals.

Personal information cannot be released unless certain exceptions apply. Information is personal information where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information (*Gordon v Minister of Health*, 2008 FC 258 at para 34).

The Information Commissioner of Canada did not agree with Health Canada's position and brought applications on behalf of the complainants in Federal Court requesting the release of the first 3 digits of the postal codes of registered personal and designated producers where there is no serious possibility of identification.

Our office intervened in this case to recommend a framework for operationalizing the test for determining whether there is a serious possibility that an individual could be identified. We await the Court's decision.

Clearview AI – Court challenges

On February 2, 2021, our office, along with the *Commission d'accès à l'information du Québec*, the Information and Privacy Commissioner for British Columbia and the Information and Privacy

Commissioner of Alberta, found that Clearview AI violated federal and provincial private-sector privacy laws by scraping images from the internet without permission.

U.S.-based Clearview created and maintains a database of more than 20 billion images – up from 3 billion at the time of our investigation – scraped from the internet without people's consent. Clearview clients, which previously included the RCMP, are able to match photographs of people against the images in the databank using facial recognition technology.

In July 2020, Clearview advised Canadian privacy protection authorities that, in response to their joint investigation, it would cease offering its facial recognition services in Canada. This data was primarily used in Canada for policing purposes without the knowledge or consent of those involved. The result was that billions of people essentially found themselves in a police line-up. We concluded this represented mass surveillance and was a clear violation of PIPEDA.

Clearview put forward a series of arguments based on PIPEDA's approach that privacy rights and commercial interests must be balanced against one another. It claimed that individuals who placed or permitted their images to be placed on the Internet lacked a reasonable expectation of privacy in their images, that the information was publicly available, and that the company's appropriate business interests and freedom of expression should prevail.

In December 2021, our provincial counterparts ordered Clearview to comply with recommendations flowing from our joint investigation. The OPC supported the provincial orders, but under PIPEDA lacks its own order-making powers.

The legally binding provincial orders require Clearview to:

- Stop offering facial recognition services that have been the subject of the investigation in the 3 provinces
- Stop collecting, using and disclosing images of people in the three provinces without consent, and
- Delete images and biometric facial arrays collected without consent from individuals in the three provinces.

Clearview is challenging those provincial orders[1] in court (via judicial review) arguing, among other things, that:
(1) provincial privacy laws do not apply to it;
(2) the personal information in question was publicly available and collected, used, and disclosed reasonably;
(3) certain sections of the provincial private sector privacy acts violate s.2(b) of the *Charter*; and
(4) the provincial orders, as worded, cannot be complied with (i.e., unreasonable and unenforceable).

At this time, our joint report of findings is not being contested in court.

On September 16, 2021, a Notice of Application[2] for a proposed class proceeding under s.14(1) of PIPEDA was filed before the Federal Court for the following proposed class: "[a]ll natural

[1] In the Supreme Court of British Columbia (January 14, 2022): No. S-220204; before the Court of Queen's Bench of Alberta (January 21, 2022): No 2201 01019; before the Court of Quebec [Administrative and Appeal Division] (January 14, 2022): No. 500-80-042393-224.
[2] In the Federal Court of Canada (September 15, 2021): Court File No. T-1410-21.

persons, who are either residents or citizens of Canada, whose faces appear in the photographs collected by Clearview." Amongst other things, this class action seeks to obtain:

- a declaration from the Court that Clearview illegally collected, copied, stored, used, and disclosed personal information of class members in violation of their privacy rights
- an order enjoining Clearview to destroy all personal information of class members and to not market or provide its services in Canada
- various forms of damages for breaches and invasions of privacy

On November 30, 2021, Clearview followed up by filing a "notice of constitutional question" in this matter and is challenging the constitutional validity of *Part I* of PIPEDA. Clearview AI is also challenging the constitutionality of paragraphs 7(1)(d), (2)(c.1), (3)(h.1) of the Act, and paragraph 1(e) of the *Regulations Specifying Publicly Available Information,* SOR/2001-7. In short, Clearview appears to be arguing that PIPEDA is invalid as per s.94(1) of the *Constitution Act* and ought to be declared unconstitutional pursuant to s.52 of that same Act. This class proceeding has yet to be certified and the constitutional questions have not yet been confirmed by the Federal Court. The OPC is closely monitoring this matter as it develops.

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.

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 the *Privacy Act*

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

Respondents	Discontinued	No jurisdiction	Not well-founded	Resolved	Settled	Well-founded	Well-founded - Conditionally resolved	Well-founded - Resolved	Total
Administrative Tribunals Support Service of Canada			1	2		2			5
Agriculture and Agri-food Canada				2					2
Atomic Energy of Canada Limited				1					1
Bank of Canada	1								1
Canada Border Services Agency	2		8	10				5	25
Canada Employment Insurance Commission				1					1
Canada Industrial Relations Board				1					1
Canada Post Corporation			1	11		1		1	14
Canada Revenue Agency	2		5	16		1		3	27
Canada School of Public Service							1	2	3
Canada-Newfoundland and Labrador Offshore Petroleum Board				1					1
Canadian Broadcasting Corporation				1					1
Canadian Food Inspection Agency				1	1				2
Canadian Human Rights Commission				3					3
Canadian Nuclear Safety Commission				1					1
Canadian Radio-Television and Telecommunications Commission				1					1
Canadian Security Intelligence Service			4	6					10
Canadian Transportation Agency								1	1

Civilian Review and Complaints Commission for the Royal Canadian Mounted Police			1	1					2
Communications Security Establishment Canada				2					2
Correctional Service Canada	1		15	29		12	1	3	61
Crown-Indigenous Relations and Northern Affairs Canada			1						1
Department of Justice Canada	2		4	2					8
Elections Canada	1								1
Elections Canada / Office of the Chief Electoral Officer	1		1						2
Employment and Social Development Canada	2	1	4	14		1			22
Environment and Climate Change Canada			1						1
Export Development Canada				1					1
Federal Government of Canada	1								1
Federal Public Service Labour Relations and Employment Board					1				1
Fisheries and Oceans Canada		1	1	2				1	5
Global Affairs Canada				2				1	3
Health Canada	1			4					5
Immigration and Refugee Board of Canada				2					2
Immigration, Refugees and Citizenship Canada			3	18					21
Indigenous Services Canada				2					2
Innovation, Science and Economic Development Canada				1	1				2
Library and Archives Canada				1					1
National Defence			1	18			1		20
National Security and Intelligence Review Agency				1					1
Natural Resources Canada				1					1
Office of the Information Commissioner of Canada		2							2
Office of the Public Sector Integrity Commissioner of Canada		1							1
Parks Canada Agency			2						2

Parole Board of Canada			1	7				1	9
Privy Council Office				2					2
Public Health Agency of Canada				1					1
Public Services and Procurement Canada	1		1	18					20
Royal Canadian Mounted Police	7		18	46		3	3	1	78
Shared Services Canada				4					4
Statistics Canada			2	3	1				6
Telefilm Canada				1					1
Transport Canada			1	3					4
Treasury Board of Canada Secretariat				1					1
Veterans Affairs Canada			1	1			1		3
Total	**22**	**5**	**77**	**246**	**4**	**20**	**7**	**19**	**400**

Table 2 - *Privacy Act* treatment times – Early resolution cases by complaint type

Complaint Type	Count	Average treatment time (months)
Privacy	**121**	**5.17**
Accuracy	1	6.13
Collection	18	4.58
Retention and disposal	7	4.21
Use and disclosure	95	5.34
Access	**117**	**6.31**
Access	114	6.39
Correction – Notation	3	3.23
Time Limits	**81**	**0.99**
Correction – Time limits	1	4,49
Time limits	80	0.95
Total	**319**	**4.53**

Table 3 - *Privacy Act* treatment times – All other investigations by complaint type

Complaint Type	Count	Average treatment time (months)
Privacy	**63**	**15.90**
Collection	11	17.54
Retention and disposal	2	24.79
Use and disclosure	50	15.19
Access	**99**	**15.54**
Access	97	15.78
Correction – Notation	2	3.58
Time Limits	**312**	**2.91**
Extension notice	1	1.54
Time limits	311	2.91
Total	**474**	**7.27**

Table 4 - *Privacy Act* treatment times – All closed files by disposition

Complaint type	Count	Average treatment time (months)
Early resolved	**319**	**4.53**
All other investigations	**474**	**7.28**
Discontinued	28	16.76
No jurisdiction	5	27.63
Not well-founded	81	11.38
Resolved	8	11.39
Settled	4	55.51
Well-founded	20	11.80
Well-founded - Conditionally resolved	108	3.86
Well-founded - Deemed refusal	54	3.70
Well-founded - Resolved	166	4.54
Total	**793**	**6.17**

Table 5 - *Privacy Act* breaches by institution

Respondent	Incident
Canada Border Services Agency	1
Canada Energy Regulator	3
Canada Post Corporation	2
Canada Revenue Agency	7
Canadian Food Inspection Agency	1
Canadian Human Rights Commission	1
Correctional Service Canada	36
Employment and Social Development Canada	349
Fisheries and Oceans Canada	1
Global Affairs Canada	6
Government of Canada RCMP	1
Health Canada	1
Immigration and Refugee Board of Canada	1
Immigration, Refugees and Citizenship Canada	6
National Capital Commission	1
National Defence	1
National Research Council Canada	2
National Security and Intelligence Review Agency	1
Office of the Commissioner of Official Languages	2
Public Health Agency of Canada	2
Public Service Commission of Canada	8
Public Services and Procurement Canada	2
Royal Canadian Mounted Police	13
Service Canada	1
Shared Services Canada	1
Statistics Canada	3
Telefilm Canada	2
Transport Canada	2
Veterans Affairs Canada	3
Windsor-Detroit Bridge Authority	2
Office of the Auditor General of Canada	1
Total	**463**

Table 6 - *Privacy Act* complaints and breaches

Category	Total
Accepted	
Privacy	306
Access	247
Time limits	353
Total Accepted	**906**
Closed through early resolution	
Privacy	121
Access	117
Time limits	81
Total	**319**
Closed through all other investigation	
Privacy	63
Access	99
Time limits	312
Total	**474**
Total closed	**793**
Breaches received	
Unauthorized disclosure*	132
Loss	279
Theft	11
Unauthorized access	41
Total received	**463**

* In previous years, “Accidental disclosure” was used by this office to reflect instances where personal information was disclosed outside of the provisions of the *Privacy Act*. This term has been changed to “Unauthorized disclosure” to reflect the wording in TBS Guidelines for Privacy Breaches, but the meaning remains unchanged.

Table 7 - *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	194	43%	17	6%	31	19%	242	27%
Correction – Notation	4	1%	1	0%	1	1%	6	1%
Time Limits								
Correction – Time limits	1	0%					1	0%
Extension notice			1	0%			1	0%
Time limits	82	18%	269	93%			351	39%
Privacy								
Accuracy	3	1%					3	0%
Collection	34	7%	1	0%	58	36%	93	10%
Retention and disposal	6	1%			1	1%	7	1%
Use and disclosure	131	29%	1	0%	70	43%	202	22%
Total	**455**	**100%**	**290**	**100%**	**161**	**100%**	**906**	**100%**

* Figures may not sum to total due to rounding.
** Summary investigations are shorter investigations that conclude with the issuance of a brief report or letter of findings.

Table 8 - *Privacy Act* top 10 institutions by complaints accepted

Respondent	Privacy			Access			Time Limits			Total
	Early Resolution	Summary Investigation	Investigation	Early Resolution	Summary Investigation	Investigation	Early Resolution	Summary Investigation	Investigation	
Correctional Service Canada	33	1	4	43	4	1	3	93		182
Royal Canadian Mounted Police	20		3	34	4	2	38	78		179
Canada Border Services Agency	8		8	12	1		6	18		53
National Defence	5		6	12			10	20		53
Immigration, Refugees and Citizenship Canada	17		4	7		2	5	14		49
Canada Revenue Agency	7		4	22	1	5	5	4		48
Canada Post Corporation	5		33	2		2	1	2		45
Employment and Social Development Canada	13		3	4		2		4		26
Public Services and Procurement Canada	6		2	6		2	1	2		19
Canadian Security Intelligence Service	1		1	7	4	1				14
Total	**115**	**1**	**68**	**149**	**14**	**17**	**69**	**235**	**0**	**668**

Table 9 - *Privacy Act* top 10 institutions by complaints accepted and fiscal year

Respondent	2017-18	2018-19	2019-20	2020-21	2021-22
Correctional Service Canada	440	426	155	130	182
Royal Canadian Mounted Police	232	273	176	186	179
Canada Border Services Agency	76	109	42	48	53
National Defence	93	121	33	51	53
Immigration, Refugees and Citizenship Canada	29	59	44	47	49
Canada Revenue Agency	63	79	63	40	48
Canada Post Corporation	33	29	4	22	45
Employment and Social Development Canada	24	39	25	41	26
Public Services and Procurement Canada	49	27	70	42	19
Canadian Security Intelligence Service	26	24	15	16	14
Total	**1065**	**1186**	**627**	**623**	**668**

Table 10 - *Privacy Act* complaints accepted by institution

Respondent	Early Resolution	Summary investigation*	Investigation	Total
Administrative Tribunals Support Service of Canada	5		2	7
Agriculture and Agri-food Canada	1			1
Business Development Bank of Canada			1	1
Canada Border Services Agency	26	19	8	53
Canada Industrial Relations Board	1			1
Canada Lands Company Limited			1	1
Canada Post Corporation	8	2	35	45
Canada Revenue Agency	34	5	9	48
Canada School of Public Service		2		2
Canada-Newfoundland and Labrador Offshore Petroleum Board	1			1
Canadian Air Transport Security Authority	1		1	2
Canadian Broadcasting Corporation	2		1	3
Canadian Food Inspection Agency	1		2	3
Canadian Heritage	1	1		2

Canadian Human Rights Commission	6	1		7
Canadian Museum of Nature		1		1
Canadian Nuclear Safety Commission			1	1
Canadian Radio-Television and Telecommunications Commission	1			1
Canadian Security Intelligence Service	8	4	2	14
Canadian Space Agency			1	1
Canadian Transportation Agency			2	2
Civilian Review and Complaints Commission for the Royal Canadian Mounted Police	1			1
Communications Security Establishment Canada	1	5	2	8
Correctional Service Canada	79	98	5	182
Crown-Indigenous Relations and Northern Affairs Canada	9	1		10
Department of Finance Canada			2	2
Department of Justice Canada	4	2	4	10
Elections Canada / Office of the Chief Electoral Officer	4			4
Employment and Social Development Canada	17	4	5	26
Environment and Climate Change Canada	1	1		2
Export Development Canada	1			1
Federal Government of Canada			4	4
Financial Transaction and Reports Analysis Centre of Canada			1	1
Fisheries and Oceans Canada	6	1	5	12
Global Affairs Canada	5	5	1	11
Health Canada	6	1	6	13
Immigration and Refugee Board of Canada	1	1	1	3
Immigration, Refugees and Citizenship Canada	29	14	6	49
Impact Assessment Agency of Canada	3			3
Indigenous Services Canada	3		4	7
Innovation, Science and Economic Development Canada	3	1	1	5

Library and Archives Canada	3	1		4
National Defence	27	20	6	53
National Research Council Canada			1	1
National Security and Intelligence Review Agency	1		1	2
Natural Resources Canada	2			2
Natural Sciences and Engineering Research Council of Canada	1	3		4
Office of the Auditor General of Canada			2	2
Office of the Commissioner of Official Languages	2			2
Office of the Correctional Investigator	1	1		2
Office of the Information Commissioner of Canada			1	1
Parks Canada Agency	1		1	2
Parole Board of Canada	5	1	1	7
Privy Council Office	4	1	1	6
Public Health Agency of Canada	3	2	7	12
Public Prosecution Service of Canada		1		1
Public Safety Canada	2		3	5
Public Service Commission of Canada	2		1	3
Public Services and Procurement Canada	13	2	4	19
Royal Canadian Mounted Police	92	82	5	179
Shared Services Canada	2		3	5
Social Sciences and Humanities Research Council of Canada	1			1
Statistics Canada	5	3	1	9
Telefilm Canada	1			1
Trans Mountain Corporation	2			2
Transport Canada	4	2	4	10
Treasury Board of Canada Secretariat	1		4	5
Veterans Affairs Canada	10	2	1	13
Veterans Review and Appeal Board	1			1
VIA Rail Canada			1	1
Total	**455**	**290**	**161**	**906**

Table 11 - *Privacy Act* complaints accepted by province, territory or other

Province/territory	Early Resolution		Summary investigation		Investigation		Total	
	Number	Percentage*	Number	Percentage*	Count	Percentage*	Number	Percentage*
Alberta	51	11.21%	37	12.76%	11	6.83%	99	10.93%
British Columbia	110	24.18%	67	23.10%	20	12.42%	197	21.74%
Manitoba	8	1.76%	4	1.38%	2	1.24%	14	1.55%
New Brunswick	18	3.96%	9	3.10%	4	2.48%	31	3.42%
Newfoundland and Labrador	6	1.32%	3	1.03%	2	1.24%	11	1.21%
Nova Scotia	12	2.64%	8	2.76%	4	2.48%	24	2.65%
Ontario	155	34.07%	104	35.86%	74	45.96%	333	36.75%
Prince Edward Island	1	0.22%		0.00%		0.00%	1	0.11%
Quebec	84	18.46%	43	14.83%	36	22.36%	163	17.99%
Saskatchewan	2	0.44%	11	3.79%	5	3.11%	18	1.99%
United States	1	0.22%	1	0.34%		0.00%	2	0.22%
Other (Not US)	6	1.32%	3	1.03%	1	0.62%	10	1.10%
Not specified	1	0.22%		0.00%	2	1.24%	3	0.33%
Total	**455**	**100.00%**	**290**	**100.00%**	**161**	**100.00%**	**906**	**100.00%**

* Figures may not sum to total due to rounding.

Table 12 - *Privacy Act* dispositions by complaint type

Complaint type	Discontinued	No jurisdiction	Not well-Founded	Resolved	Settled	Well-founded	Well-founded - Conditionally resolved	Well-founded - Deemed refusal	Well-founded - Resolved	Total
Privacy										
Accuracy				1						1
Collection	2		5	18	1	1	2			29
Retention and disposal	2			7						9
Use and disclosure	9	1	15	98	3	14	5			145
Access										
Access	9	4	55	119		5			19	211
Correction – Notation			2	3						5
Time Limits										
Correction – Time limits				1						1
Extension notice			1							1
Time limits	6		3	80			101	54	147	391
Total	**28**	**5**	**81**	**327**	**4**	**20**	**108**	**54**	**166**	**793**

Table 13 - *Privacy Act* dispositions of time limits by institution

Respondent	Discontinued	Not well-founded	Resolved	Well-founded - Conditionally resolved	Well-founded - Deemed refusal	Well-founded - Resolved	Total
Canada Border Services Agency			6	6	8	7	27
Canada Post Corporation		1	1				2
Canada Revenue Agency			3			4	7
Canada School of Public Service				1		1	2
Canadian Heritage						1	1
Canadian Human Rights Commission			1			1	2
Canadian Museum of Nature						1	1
Communications Security Establishment Canada				1	2	1	4
Correctional Service Canada	1		3	55	14	42	115
Department of Justice Canada						1	1
Employment and Social Development Canada		1		2	2	1	6
Environment and Climate Change Canada			1	1		2	4
Federal Economic Development Agency for Southern Ontario						1	1
Fisheries and Oceans Canada		1	1				2
Global Affairs Canada			1	1	3	2	7
Health Canada			1			1	2
Immigration and Refugee Board of Canada		1					1
Immigration, Refugees and Citizenship Canada	1		5	1	1	11	19
Impact Assessment Agency of Canada			1				1
Indigenous Services Canada			1				1
Innovation, Science and Economic Development Canada			1		1	2	4
Library and Archives Canada			1			1	2
National Defence			10	11	3	8	32

Natural Sciences and Engineering Research Council of Canada				3			3
Office of the Correctional Investigator			1			1	2
Privy Council Office						1	1
Public Health Agency of Canada				1	1	1	3
Public Prosecution Service of Canada						1	1
Public Safety Canada			1	1			2
Public Services and Procurement Canada			1			4	5
Royal Canadian Mounted Police	3		37	11	16	50	117
Statistics Canada					1		1
Trans Mountain Corporation						1	1
Transport Canada	1			1			2
Transportation Safety Board of Canada				1			1
Treasury Board of Canada Secretariat				1	2		3
Veterans Affairs Canada			4	3			7
Total	**6**	**4**	**81**	**101**	**54**	**147**	**393**

Statistical tables related to PIPEDA

Table 1 - PIPEDA complaints accepted* by industry sector

Industry sector	Number	Proportion of all complaints accepted *
Accommodations	41	10%
Agriculture, Forestry, Fishing and Hunting	2	0%
Construction	1	0%
Entertainment	6	1%
Financial	102	24%
Food and Beverage	6	1%
Government	4	1%
Health	11	3%
Individual	2	0%
Insurance	25	6%
Internet	44	10%
Manufacturing	8	2%
Not for profit organizations	2	0%
Professionals	22	5%
Publishers (except Internet)	6	1%
Rental	3	1%
Sales/Retail	28	7%
Services	32	7%
Telecommunications	53	12%
Transportation	28	7%
Utilities	1	0%
Total	**427**	**100%**

* Figures may not sum to total due to rounding.

Table 2 - PIPEDA complaints accepted* by complaint type

Complaint type	Number	Proportion of all complaints accepted*
Access	121	28%
Accountability	1	0%
Accuracy	2	0%
Collection	57	13%
Consent	19	4%
Correction - Notation	4	1%
Openness	1	0%
Retention	36	8%
Safeguards	19	4%
Use and disclosure	154	36%
Time limits	13	3%
Total	**427**	**100%**
* Figures may not sum to total due to rounding.		

Table 3 - PIPEDA investigations closed by industry sector and disposition

Sector category	Early resolved	Declined	Discontinued (under 12.2)	No jurisdiction	Not well-founded	Settled	Well-founded	Well-founded - Conditionally resolved	Well-founded - Resolved	Withdrawn	Total
Accommodations	19				1						20
Agriculture, Forestry, Fishing and Hunting	1										1
Construction	1										1
Entertainment	3	1									4
Financial	68		3		3		5		3	2	84
Food and Beverage	1										1
Government	3										3
Health	3			1				1			5
Individual	2										2
Insurance	23		3		1						27
Internet	34									1	35
Manufacturing	9									1	10
Not for profit organizations			1								1
Not Specified	1										1
Professionals	12		1			1			1		15
Publishers (except Internet)	11		2			1					14
Sales/Retail	29		2		1						32
Services	31		5		2			1	1	2	42
Telecommunications	33		3		2			1			39
Transportation	18		1					1			20
Utilities	1										1
Total	**303**	**1**	**21**	**1**	**10**	**2**	**5**	**4**	**5**	**6**	**358**

Table 4 - PIPEDA investigations closed by complaint type and disposition

Complaint type	Early resolved	Declined	Discontinued (under 12.2)	No jurisdiction	Not well-founded	Settled	Well-founded	Well-founded - Conditionally resolved	Well-founded - Resolved	Withdrawn	Total
Access	94		4		2		1		3	1	105
Accuracy	2									1	3
Appropriate purposes									1		1
Collection	29		3		2	1					35
Consent	23	1	3	1	2		1	1		3	35
Correction - Notation	1										1
Retention	28										28
Safeguards	16		5		1		1	1	1		25
Use and disclosure	105		6		3	1	2	1			118
Time limits	5							1		1	7
Total	**303**	**1**	**21**	**1**	**10**	**2**	**5**	**4**	**5**	**6**	**358**

Table 5 - PIPEDA investigations – Average treatment time by disposition

Disposition	Number	Average treatment time in months
Early resolved	303	6.3
Declined	1	14.0
Discontinued (under 12.2)	21	9.9
No jurisdiction	1	13.8
Not well-founded	10	13.0
Settled	2	5.1
Well-founded	5	21.1
Well-founded - Conditionally resolved	4	32.7
Well-founded - Resolved	5	32.0
Withdrawn	6	16.9
Total	**358**	
Overall weighted average		**7.8**

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

Complaint type	Early resolved		Dispositions not early resolved		All dispositions	
	Number of cases	Average treatment time in month	Number of cases	Average treatment time in month	Number of cases	Average treatment time in month
Access	94	6.7	11	12.8	105	7.4
Accuracy	2	4.1	1	46.4	3	18.2
Appropriate purposes			1	69.0	1	69.0
Collection	29	7.4	6	11.8	35	8.2
Consent	23	8.7	12	16.6	35	11.4
Correction - Notation	1	6.7			1	6.7
Retention	28	5.9			28	5.9
Safeguards	16	7.8	9	18.8	25	11.7
Time limits	5	0.8	2	2.2	7	1.2
Use and disclosure	105	5.3	13	13.4	118	6.2
Total	**303**	**6.3**	**55**	**15.9**	**358**	**7.8**

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*		
Accommodations		1	2		3	0%
Agriculture, Forestry, Fishing and Hunting			2		2	0%
Construction			4		4	1%
Entertainment			5	1	6	1%
Financial	14	11	71	35	131	20%
Food and Beverage			4		4	1%
Government			10	4	14	2%
Health	4		12	6	22	3%
Insurance	15	3	36	35	89	14%
Internet			6	3	9	1%
Manufacturing	1	1	48	3	53	8%
Mining and Oil and Gas Extraction			5	1	6	1%
Not for profit organizations	1	1	18	6	26	4%
Professionals	4	2	53	21	80	12%
Publishers (except Internet)			6	1	7	1%
Rental			1		1	0%
Sales/Retail	2		44	6	52	8%
Services	1		17	12	30	5%
Telecommunications	1	2	61	27	91	14%
Transportation			12		12	2%
Utilities			2	1	3	0%
Total	**43**	**21**	**419**	**162**	**645**	**100%**

* In previous years, “Accidental disclosure” was used by this 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.
** Figures may not sum to total due to rounding.

Table 8 - Number of Canadians accounts affected by incident type

Incident type	Number of Canadians accounts affected
Loss	2,869
Theft	5,077
Unauthorized access	1,916,557
Unauthorized disclosure*	21,605
Total	**1,946,108**

* In previous years, “Accidental disclosure” was used by this 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 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 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; and

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 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 that have been declared substantially similar to PIPEDA:

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

Appendix 4: Report of the Privacy Commissioner, Ad Hoc

During the past year I received few matters for review, and all of which were cases that I could not accept as complaints as the subject matter did not fall within my area of review.

These individuals were seeking assistance nonetheless, and I was able to discern their concerns, direct them to the appropriate channels to pursue their complaints, and in some cases, I informed the Office of the Privacy Commissioner (OPC) directly as the OPC was already involved in their case.

In one case, I could not identify the true nature of the issues the individual was genuinely seeking to appeal, and this individual had referenced several files that were active, on-going, or closed. I therefore requested that the OPC clarify those files for me and, armed with the information provided by the OPC, I was then able to assist the individual in pursuing the right course of action. While I was not able to review these matters, I was nonetheless able to provide a useful service to this individual as well as to the others who wrote to me last year.

My authority as Ad Hoc Privacy Commissioner is to investigate any complaints that may be lodged against the OPC under the *Privacy Act*. For instance, where a request for access to personal information has been submitted to the OPC and the OPC's decision was to refuse access, this will trigger the right to file a complaint with the Ad Hoc Commissioner. Another form of complaint lies in where it is alleged the OPC mishandled the personal information of an individual contrary to the *Privacy Act*, to which the OPC is subject. There were no such complaints filed with me this past year.

We begin a new year and I look forward to continuing to be of service to those who seek my assistance.

Respectfully submitted,

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