Office of the Information and Privacy Commissioner for British Columbia

Annual Report and Service Plan

2025/26

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

WHO WE ARE

Established in 1993, the Office of the Information and Privacy Commissioner provides independent oversight and enforcement of BC's access and privacy laws, including:

•The *Freedom of Information and Protection of Privacy Act* (FIPPA), which applies to over 2,900 public bodies, including ministries, local governments, schools, crown corporations, hospitals, municipal police forces, and more; and

•The *Personal Information Protection Act* (PIPA), which applies to any private sector organization (including businesses, charities, non-profits, and political parties) that collects, uses, and discloses the personal information of individuals in BC. PIPA also applies to any organization operating in BC that collects, uses, or discloses personal information of any individual inside or outside of BC.

Michael Harvey is BC's Information and Privacy Commissioner.

The Office of the Information and Privacy Commissioner for BC respectfully acknowledges that its offices are located on the traditional territory of the lək̓ʷəŋən People, the Songhees and xʷsepsəm (Esquimalt) First Nations.

As an Officer of the Legislature, the work of the Commissioner spans across British Columbia, and the OIPC acknowledges the territories of First Nations around BC and is grateful to carry out our work on these lands.

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

June 2026

The Honourable Raj Chouhan
Speaker of the Legislative Assembly
Room 207, Parliament Buildings
Victoria, BC V8V 1X4

Dear Honourable Speaker,

In accordance with s. 51 of the *Freedom of Information and Protection of Privacy Act* and s. 44 of the *Personal Information Protection Act,* I have the honour of presenting the office's Annual Report to the Legislative Assembly.

This report covers the period from April 1, 2025 to March 31, 2026.

Yours sincerely,

Michael Harvey
Information and Privacy Commissioner
and Registrar of Lobbyists for British Columbia

OUR CORE VALUES

Impartiality	We are independent and impartial regulators of British Columbia's access to information and privacy laws.
Expertise	We use our expertise to enforce and advance rights, resolve disputes, and encourage best practices.
Dedication	We are dedicated to protecting privacy and promoting transparency.
Respect	We respect people, organizations, public bodies, and the law.
Innovation	We are innovators and recognized in the global community.

TABLE OF CONTENTS

Commissioner's message 6

Mandate and Vision 10

Our team 12

Year in review 14

A win for children's privacy 16

Lessons learned 18

Trust in the age of information 20

Watching out for us, or watching us? 22

AI scribes guidance puts patients first 24

Trust after tragedy 26

Legal updates 28

Highlights 30

Year in numbers 34

Adjudication 48

Service Plan 50

Financial reporting 60

Resources 62

COMMISSIONER'S MESSAGE

I am pleased to present the Annual Report and Service Plan of the Office of the Information and Privacy Commissioner for British Columbia for the fiscal year 2025/26.

Last spring, as part of our strategic planning process, I had the privilege of travelling the province to speak with people in British Columbia. From Prince George and Smithers to Abbotsford and Vancouver, what struck me was not only the tremendous diversity of this province, but also how the same concerns resonated across such different communities.

One of the most common was, "How do we rebuild trust?"

People were worried about institutions keeping information from them, about technology moving faster than the laws and what this means for their children.

Underlying all of this was the feeling that trust between people and organizations and institutions was broken, perhaps beyond repair.

Those conversations shaped our *Strategic Plan 2025-2028: Trust in the Age of Information*, which we released in October, and our three strategic priorities of trust and transparency, trusted innovation, and enhancing rights equity. That document is our commitment to doing what is within our mandate to address today's trust crisis. Our work over the period covered in this report also advanced that goal.

Transparency is a right, not an option

Trust is earned through reciprocal obligations between institutions and the people they serve. Likewise, when those obligations go unmet – when people are left waiting for months on end for a reply to a freedom of information request – that trust suffers.

Our audit of the University of British Columbia's (UBC) FOI processes reflected a mindset that is damaging to transparency across many public bodies: the belief that access requests are secondary to a public body's "real work."

We found that UBC took an average of 100 business days to respond to requests, the

lowest compliance rate of any public body in 10 years of audits by our office. UBC committed to positive changes; however, the report remains a call for all public bodies to build a culture of transparency.

Protecting who we are, and who we aspire to be

During this period, the need to find new ways to safeguard people's privacy in the Information Age became critically important. Our personal information is often treated as a resource to be exploited, when, instead, it is who we are, how we express ourselves, and what gives us autonomy and dignity.

For children, especially, technology can empower and enrich, but it can also be used to manipulate their behaviour, their relationships, and their developing sense of themselves and the world.

Our joint investigation with federal and provincial privacy commissioners into the information practices of TikTok found that hundreds of thousands of underage

COMMISSIONER'S MESSAGE

Canadian children were accessing the social media platform, which was feeding their information into algorithms and using their data without valid, meaningful consent. TikTok had the tools to keep children off the platform – they were using them for ad targeting rather than age-gating.

TikTok committed to improvements; however, until we hold organizations to account and mandate privacy by design principles in our laws, we will be left addressing damages after the fact.

Two other investigation reports released during this period spoke to our expectations of privacy in public spaces in very different contexts.

The growth of a surveillance society

Surveillance has become, in many respects, the default response to a host of social issues, often with the implicit belief that once you're out in "public," you lose all expectations of privacy. The courts have been clear privacy is context dependent – what is reasonable depends on the specific facts.

The idea that privacy rights disappear altogether in public spaces is antithetical to the principles of a free democratic society. Whether in our homes, on the sidewalk, or online, public and private organizations alike can only collect our personal information if it is authorized by law.

As I noted in our report into the City of Richmond's use of surveillance cameras at a key intersection in the city, there are appropriate uses for surveillance; however, those uses need to be limited, proportional, and authorized. I found that Richmond did not have the mandate to use cameras to assist in law enforcement, and I ordered them to stop the surveillance.

An egregious breach of public trust

The second pertained to a breach of public

trust that compounded a tragedy. Our investigation into privacy breaches following the tragic events at the 2025 Lapu Lapu Day festival found 71 incidents of snooping by 36 workers across three health authorities, breaching the privacy of 16 individuals, including those who lost their lives in the tragedy. This was illegal, unethical, and a profound betrayal of public trust. While health authorities took corrective measures to address the breaches, the report was a stark reminder of how, as our health system becomes more digitized, the importance of a strong privacy foundation will grow.

Towards trust

How do we rebuild trust?

No one person or even sector can do it alone. We do it by repairing what's broken – by public bodies meeting their transparency obligations; by organizations making privacy by design the default; and by government reforming our laws to make the latter mandatory. In the age of artificial intelligence, we cannot afford to rely on laws written for a different era. We need a comprehensive reform of our privacy laws that addresses today's challenges and today's trust crisis. To do that in a way that reflects our values as British Columbians and Canadians, we need to talk to each other about these issues. That conversation needs to start now.

It is my privilege to work alongside a team that is dedicated to building trust in the work they do every day, and I look forward to carrying out our strategic priorities – *your* priorities – in the year ahead.

Michael Harvey
Information and Privacy Commissioner
for British Columbia

MANDATE

Under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA), the mandate of the Office of the Information and Privacy Commissioner (OIPC) is to:

- Independently review decisions and practices of public bodies and private sector organizations concerning access to information and protection of privacy;
- Comment on the implications for access to information or protection of privacy of proposed legislative schemes, automated information systems, record linkages, and programs of public bodies and organizations;
- Educate and inform the public about access and privacy rights; and
- Promote research into access and privacy issues.

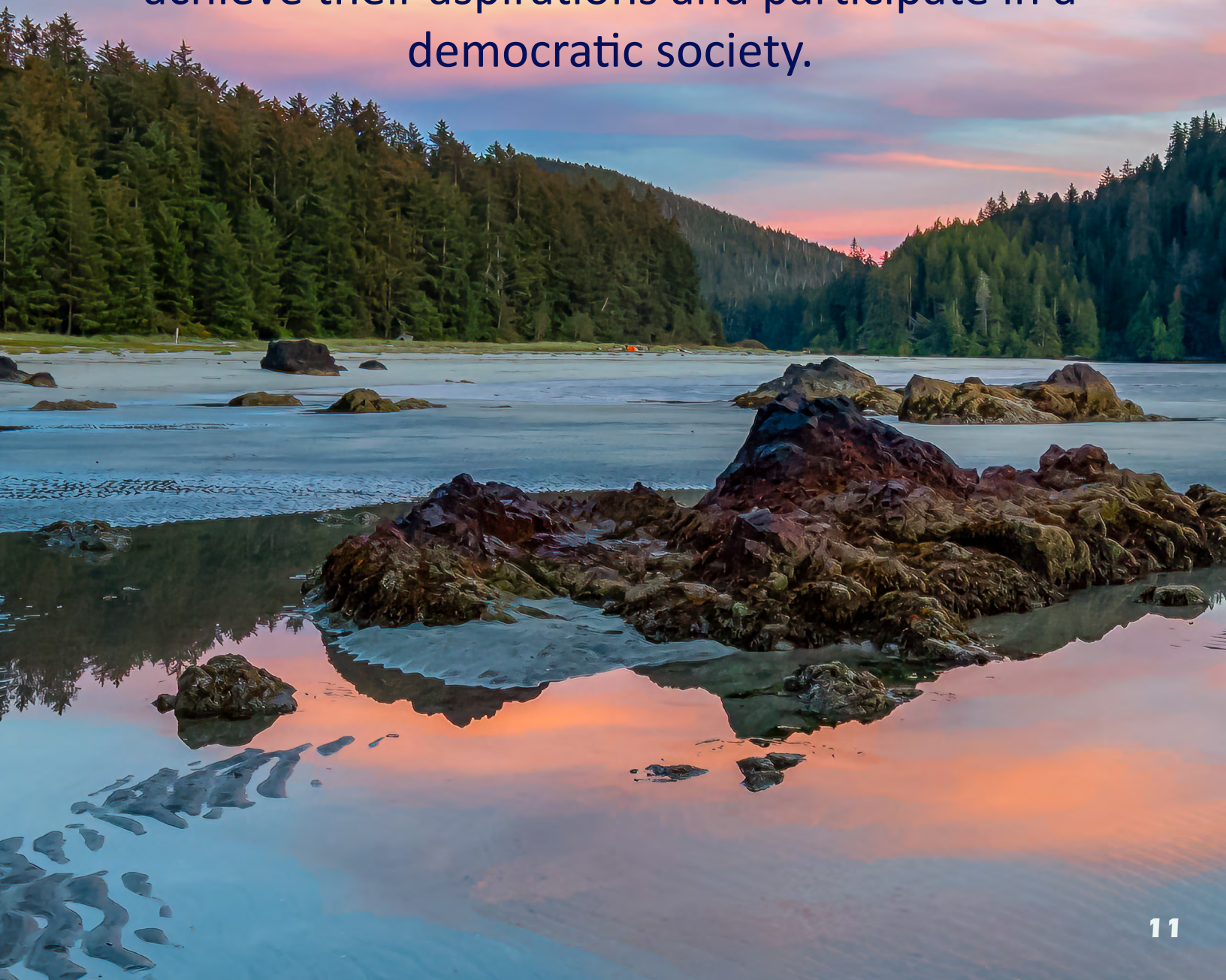
A dedicated staff, committed to service

Sixty-four people worked at the Office of the Information and Privacy Commissioner in 2025/26. They were supported by the Corporate Shared Services team responsible for providing finance, HR, IT, and facilities management to the office and to the three other Officers of the Legislature: the Office of the Merit Commissioner, the Office of the Police Complaint Commissioner, and the Office of the Ombudsperson.

OIPC staff recognize they are part of a wider community. They take pride in, and have long supported, community causes. This includes the Provincial Employees Community Services Fund, as well as other local causes. OIPC staff were recognized for their contributions to the 2025 PECSF campaign with the Highest Participation Award - an award won, and held, by the OIPC since 2013, highlighting the OIPC's commitment to community support and engagement.

VISION

A province where people in BC have protection of their rights to access to information, privacy, and transparency and that those protections enable them to achieve their aspirations and participate in a democratic society.



OUR TEAM

Staff at the OIPC are delegated to carry out the responsibilities and powers of the Commissioner under the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act*.

Commissioner

The Information and Privacy Commissioner for British Columbia, an independent Officer of the Legislature, oversees the information and privacy practices of public bodies and private organizations. The Commissioner has the legal authority to investigate programs, policies, or information systems in order to enforce compliance with BC's access and privacy laws. The Commissioner also reviews appeals of access to information responses; investigates access and privacy complaints; comments on the implications of new programs, policies, and technologies on access and privacy rights; issues binding orders; collaborates with national and international regulators; and engages in public education and outreach activities.

Senior leadership team

The Deputy Commissioners help oversee the team that carries out the Commissioner's authorities to deliver education and conduct enforcement. The Deputy Commissioners provide strategic advice to the Commissioner and administer finance and human resource functions as delegated by the Commissioner. The senior leadership team consists of team leads from departments across the office and provides strategic direction for the work of the office.

Legal

The legal team delivers comprehensive legal advice and guidance to the Commissioner and other teams on current and emerging matters relating to access, privacy, and lobbying, as well as on matters relating to administrative law, common law, and constitutional law.

Executive support

The executive support team assists the Commissioner, Deputy Commissioners, and OIPC and ORL staff with scheduling, coordinating cross-program projects, organizing and maintaining office facilities, and other administrative tasks as required. This team also responds to general enquiries from the public.

Communications

The communications team publicizes the work of the office, including public education and outreach to inform and empower individuals to exercise their information and privacy rights. They manage the office's website, social media presence, media relations, annual report, and open data/proactive disclosure. The team also supports the work of the Office of the Registrar of Lobbyists.

Case review

The case review team assesses all incoming complaints and requests for reviews to determine admissibility based on OIPC BC jurisdiction and scope. The team also does early resolution of select complaints and breach notifications where appropriate. They provide guidance to individuals, organizations, and public bodies seeking information on OIPC processes and statutory functions and respond to general questions regarding the application of PIPA and FIPPA.

Additionally, they exercise delegated decision-making authority on all time extension requests.

Investigation & mediation

The investigations team conducts investigations and mediations on access and privacy complaints, reviews access to information requests, makes decisions on complaint files, and processes privacy breach notifications. They review any records at issue or investigate relevant facts and evidence, and work with public bodies, organizations, complainants, and applicants to reach resolutions.

Some investigators also support the work of the Office of the Registrar of Lobbyists by determining potential matters of non-compliance.

Adjudication

When a complaint or request for review cannot be resolved at investigation, the Commissioner or their delegate may conduct an inquiry. Adjudicators assess evidence and arguments and issue final and legally binding decisions. Orders are subject to review by the Supreme Court of British Columbia.

Policy

The policy team researches and analyzes current and emerging access and privacy issues, reviews and comments on privacy management programs and privacy impact assessments, and consults with public bodies and private organizations to provide guidance and make educational presentations.

They also review and analyze proposed legislation for implications to the access and privacy rights of people in British Columbia and review all public Independent Investigations Office reports (as legislated by the *Police Act*).

Audit & systemic review

The audit and systemic review (AnSR) team performs audits, systemic reviews and investigations of information access and privacy compliance within public bodies and private sector organizations in relation to legislation, guidelines, and best practices. AnSR projects may be conducted jointly with other access and privacy regulators, and often comprise high-profile, complex investigations.

Office of the Registrar of Lobbyists

The *Lobbyists Transparency Act* (LTA) designates the Information and Privacy Commissioner as Registrar of Lobbyists for British Columbia. See the Office of the Registrar of Lobbyists' Annual Report and Service Plan for more information about how OIPC legal, communications, and investigations teams, and a Deputy Commissioner, support the work of that office.

YEAR IN REVIEW

Select publications, speaking engagements, and events

APRIL

3 Commissioner announces seven-city public consultation tour to inform strategic plan

28 Commissioner files order with BC Supreme Court after Northern Health Authority fails to respond to applicant despite agreeing to a consent order to do so

MAY

5 Privacy Awareness Week kicks off with the theme of "Privacy is everyone's business"

28 Commissioner delivers speech to Fraser Valley Regional Library on FIPPA and the importance of privacy protection to libraries

JUNE

24 Commissioner participates in panel on environmental law at the International Conference of Information Commissioners (ICIC) in Berlin

JULY

23 Deputy Commissioner oline Twiss participates in a Genvis justice and privacy round-table on balancing privacy, legal accountability, and survivor autonomy

SEPTEMBER

15 Commissioner participates in joint OECD/GPA panel on health data sharing and moderated a panel on children's privacy at the 47th Global Privacy Assembly in Seoul

19 OIPC co-sponsors Global Privacy Assembly (GPA) Resolutions on Meaningful Human Oversight of Decisions involving AI Systems and Digital Education, Privacy and Personal Data Protection for Responsible Inclusive Digital Citizenship

22 Right to Know Week highlights information rights' essential role in a democracy

OCTOBER

6 OIPC releases three-year strategic plan, Trust in the Age of Transparency

10 Canadian information and privacy regulators meet in Banff, Alberta, to discuss new technologies, AI, cybersecurity, and protection of online data

23 OIPC raises concerns over children's privacy in joint investigation report with federal and provincial counterparts into TikTok

25 OIPC audit finds UBC failed to meet FOI response timelines in 90% of requests

NOVEMBER

3 OIPC takes part in 2025 Global Privacy Enforcement Network sweep, focusing on children's privacy on websites and apps

5 Canada's information regulators issue joint resolution calling for more robust access to information laws and practices

18 Commissioner addresses OECD panel on the secondary use of health data for public interest purposes

20 Canada's privacy regulators issue joint resolution calling for strong protection of children's privacy in educational technologies

20 Commissioner joins a panel on responsible AI at the Prompt AI conference in Victoria

DECEMBER

2 Commissioner shares how embedding privacy principles from the outset of initiatives helps earn public trust at Public Sector Network: Government Innovation Showcase

4 Commissioner interviewed by BC FIPA for a podcast about misinformation

JANUARY

14 OIPC releases investigation report into the City of Richmond's field test of its Public Safety Camera System and Order to stop surveillance

26 In Privacy Data Day statement, Commissioner calls on private and public sector organizations to innovate to enhance privacy rights

FEBRUARY

28 OIPC publishes guidance for healthcare organizations when using AI scribes to transcribe patient records

12 Commissioner testifies before the Senate of Canada on proposed changes to the *Canada Elections Act* and implications for privacy oversight of political parties in BC

18 OIPC releases a report following the Lapu Lapu tragedy with nine recommendations to curtail snooping incidents by healthcare workers

MARCH

4 Deputy Commissioner Jeannette Van Den Bulk presents to legislative committee on Bill M217 – Dashboard Cameras in Commercial Vehicles Act

4 Deputy Commissioner oline Twiss discusses agentic AI on a panel at the Victoria International Privacy & Security Summit.

18 Deputy Commissioner Van Den Bulk and Director of Investigations Trevor Presley present OIPC processes, procedures, and priorities to group of BC crown corporations

23 OIPC BC and international data protection authorities release statement on privacy risks of AI-generated imagery

25 Results of 2025 GPEN privacy sweep on children's websites released as report and infographic

26 Commissioner releases statement regarding proposed amendments to the *Freedom of Information and Protection of Privacy Act*

A WIN FOR CHILDREN'S PRIVACY

Joint investigation with federal, Alberta, and Quebec privacy commissioners results in TikTok committing to advanced privacy safeguards for young people

TikTok, one of the world's most popular social media platforms, committed to introducing "industry-leading" privacy protections for children and youth following an investigation by the Office of the Information and Privacy Commissioner for British Columbia and Canadian counterparts.

The investigation, conducted by the OIPC BC, counterparts in Alberta and Quebec, and the federal privacy commissioner, found that over 500,000 Canadian children were being banned from the platform annually – roughly the equivalent of one child every minute – from a platform that they should not have been able to access. Considering the gaps observed in TikTok's underage user detection mechanisms, the Commissioners found it likely that many more children continued using it undetected.

TikTok's core commercial business is delivering ads to users based on the information it collects about them. For children on the platform, that meant exposure to targeted advertising and content that put their wellbeing at risk. This included the marketing of games that can lead to the normalization of gambling; increased risk of identity theft and fraud; and hindering their normal development and identity exploration, including through negative body image perception and early sexualization. While the investigation focused on children, investigators also found that TikTok failed to provide adequate information about or obtain consent for its collection and use of data of all users on the platform.

Improved protections for children

TikTok's initial "age gate" asked users to enter their birthdate. Users could easily bypass this by entering false information. Once on the platform, based on their engagement with the platform, users were subject to more sophisticated age estimation technology that targeted them with ads and recommended content.

However, investigators noted disparity in that the company did not use such tools to keep underage users *off* the platform.

In response to the investigation, TikTok committed to using its existing technology for more effective age-assurance methods and to implementing technology that can identify underage users even when they don't actively engage with the platform. This passive user detection model would monitor behaviour patterns rather than rely on user-generated content. This would be more effective in identifying and removing underage users from TikTok, given that 73.5% of users do not post videos, and 59.2% don't comment. TikTok told investigators that this would be the first use of such technology in the industry to their knowledge.

The company also agreed to strengthen its privacy communications to ensure that users understand how their data could be used, including for targeted advertising and content personalization, and provide more information in French.

"The offices involved in the investigation are monitoring TikTok's progress on its commitments", said Commissioner Harvey.

"This investigation points to a path forward for us in the information age – one where we can benefit from technologies, without having our rights trampled by them, and, critically, where children can flourish online and enjoy the benefits of these platforms, without being exposed to harms that they – and the people who care for them – could not and should not be expected to understand. It's about taking control back – of our information and our lives – as we move forward in this new age."

Download

Joint investigation of TikTok Pte Ltd
News release, video on the report, and overview fact sheet

LESSONS LEARNED

UBC failed to meet response time limits in 90% of FOI request, audit finds

The audit found concerns over applicant anonymity after records searches were completed, and identified three primary areas where delays occurred:

- UBC took 18 days on average to initiate a search for requested records;
- an additional 28 days to retrieve records; and
- 59 days to process and respond to applicants.

Universities and our freedom of information laws are both founded on the principle that society benefits when information and ideas are released to the public arena and open to scrutiny and debate. When universities don't comply with the *Freedom of Information and Protection of Privacy Act* (FIPPA), they undermine the fundamental principles of transparency and accountability that empower people with information, for the benefit of society.

The OIPC launched an audit of the University of British Columbia (UBC) following analysis of complaints filed with the office over the previous three fiscal years. OIPC auditors found that UBC failed to comply with FIPPA's maximum time limits in 90% of FOI requests – the highest rate of non-compliance the OIPC has seen in 10 years. Additionally, UBC responded to only 8% of requests within FIPPA's benchmark of 30 days, taking an average of 100 business days to respond to requests – over three times the benchmark.

"This was concerning not only because of UBC's important role in education and advancing knowledge in this province, but also because of the size of the university's operations," said Commissioner Harvey. "UBC is the largest university in this province and operates on the scale of a municipality."

OIPC auditors made nine recommendations for UBC to improve its FOI processes, including addressing process issues identified in the report, eliminating its FOI request backlog within one year, and providing proper training to staff so the university can meet its duty to assist applicants under FIPPA. At the time the report was published, UBC had begun implementing the recommendations and making improvements to their processes.

"The lessons learned from this report provide all public bodies with an opportunity to assess and improve their own FOI processes – to train staff, improve systems, and foster a culture of openness that serves FIPPA's core purpose of building trust through transparent and accountable public institutions," said Commissioner Harvey. "Doing so benefits not only the individual public body and the people they serve – it strengthens the fabric of our institutions, and our democracy."

Download

The University of British Columbia's duty to assist
News release, video on the report, and overview fact sheet

TRUST IN THE AGE OF INFORMATION

OIPC strategic plan focuses on advancing transparency, trusted innovation, and equitable rights access over next three years

How can we build the future we want amid rapid technological change, eroding trust in public institutions, and inequitable access to fundamental information and privacy rights? These were the recurring themes that Commissioner Harvey heard during a months-long consultation process that shaped the OIPC's three-year strategic plan. The consultation process included eight in-person consultation sessions led by Commissioner Harvey across seven regions in BC, written submissions, and internal engagement with OIPC staff.

The resulting plan, *Trust in the Age of Information*, was released in October 2025. It includes three priority areas based on feedback from the consultations: trust and transparency, trusted innovation, and enhancing rights equity.

Trust and transparency

A healthy democracy requires that people trust public institutions. As Commissioner Harvey noted: "This trust is fostered when people feel like they can know how their public bodies are working in their interests, that their concerns are heard, they can make a difference, and that there is accountability." However, many public bodies are failing to meet basic obligations under the *Freedom of Information and Protection of Privacy Act* (FIPPA), which aims to provide

transparency about how public bodies operate and use personal information.

To address this, the OIPC will focus on promoting timely FOI management by public bodies, fostering resilient and trusted institutions, and improving the office's own internal processes.

Trusted innovation
In our Information Age, the ability to control our personal information is related to the ability to control our lives – how we maintain autonomy and express ourselves as individuals as part of wider society. During consultations, Commissioner Harvey heard how people felt that control was slipping and their privacy rights were being eroded amid the rapid advances of technologies that directly challenge them, including artificial intelligence and surveillance systems. The risk is that people may lose trust in these technologies, and leave their potential benefit to society unrealized.

The strategic plan aims to support a privacy rights-first approach to innovation in BC by developing the office's strategic expertise in the priority areas of artificial intelligence, surveillance, and digital health.

Enhancing rights equity
While all individuals have equal rights before the law, their ability to exercise those rights can differ widely. To address this, the OIPC will take several measures, including a focus on protecting the privacy rights of children and youth in digital environments, where deceptive designs are often the norm. The office also committed to advancing Truth and Reconciliation with Indigenous peoples by supporting Indigenous data sovereignty.

Finally, the office will focus on making access and privacy rights more accessible to seniors, newcomers, people with disabilities, and other communities facing barriers.

A path forward
Commissioner Harvey concluded his introduction to the strategic plan by reflecting on the wider aims of the report and the OIPC's work.

"We should together be striving for a society that has a strong level of trust built on a foundation of democratic accountability and individual, equitable autonomy," he wrote. "The OIPC is committed to do its part. This three-year plan is intended to take us down that path. We are privileged to be walking it with British Columbians."

Download

Trust in the Age of Information
News release and overview fact sheet

WATCHING OUT FOR US, OR WATCHING US?

The City of Richmond's use of ultra-high surveillance cameras at intersections not authorized, says Commissioner

Surveillance in BC communities is on the rise, with advancing technologies offering ever-increasing levels of resolution and functionality, such as the ability to collect biometric information like faceprints, heat signatures, gait patterns, and more. The trend is driven by concerns about crime and social disorder in communities across the province. However, under the *Freedom of Information and Protection of Privacy Act* (FIPPA), public bodies can only collect, use, or disclose personal information under certain circumstances listed in the Act.

While some situations may justify the use of surveillance, it should be limited, proportional, and must be authorized by law, said Commissioner Harvey. These comments followed an investigation into the City of Richmond's (the City) field testing of ultra-high resolution surveillance cameras at a major intersection.

The City originally submitted a privacy impact assessment (PIA) to the OIPC in July 2024 for a field test of its Public Safety Camera System (PSCS). The system used multiple ultra-high-definition video cameras to collect video footage of individuals, licence plates, and vehicle features that would be disclosed to the Royal Canadian Mounted Police (RCMP) to assist the RCMP in identifying criminal suspects.

The OIPC advised the City in 2024 that it was not apparent that FIPPA provided legal authority to collect personal information through the PSCS for their intended purpose. The City disagreed and began implementing the PSCS in February 2025.

The OIPC then initiated its investigation, which confirmed that FIPPA does not authorize the City to collect, use, or disclose personal information via the PSCS to assist the RCMP in identifying criminal suspects. Public bodies must have a statutory mandate to enforce criminal laws, not merely an interest in their enforcement. As the RCMP provides policing services to the City, independently, it is the RCMP that has general responsibility for criminal law enforcement in Richmond – not the City.

"I would encourage other public bodies exploring options for similar high-tech video surveillance to read this report and consider whether they have the authority to collect personal information, whether that collection is necessary and proportional to the issue at hand, and whether the project actually serves the public. Privacy is a core democratic value, and upholding its protection is paramount to a free and healthy society," said Commissioner Harvey.

The report recommended that the City stop collecting personal information through the PSCS, delete all recordings to date, and disband the equipment used to collect personal information. After the City advised the OIPC it did not intend to follow the recommendations, Commissioner Harvey issued Order F26-01, which ordered the City to immediately comply.

The City decided to stop recording and delete the data, but challenged the Commissioner's ruling. The matter will proceed to the Supreme Court of BC.

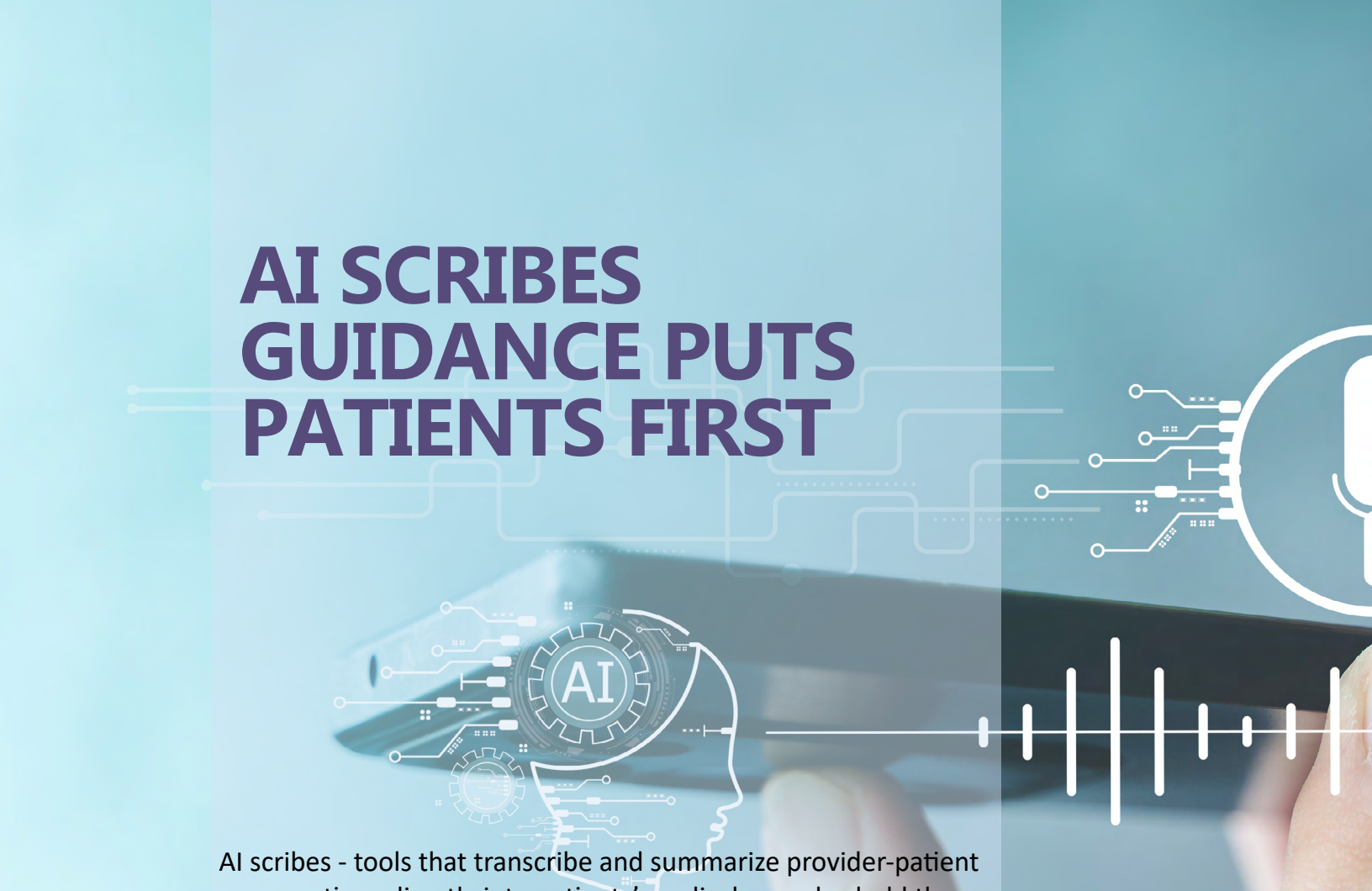
The report also includes a recommendation to the BC Government to regulate technologies that capture biometric information. In a letter to Minister of Citizens' Services, Diana Gibson, Commissioner Harvey noted:

"The lack of regulation partnered with the ease and availability of advanced technologies has created an untenable situation in BC where private organizations and public bodies are employing highly invasive tools without the necessary control and oversight."

Download

Investigation into City of Richmond's Public Safety Camera System Field Test
Order F26-01: City of Richmond
Public sector surveillance guidelines
Letter to Minister of Citizens' Services
News release, video overview and overview fact sheet

AI SCRIBES GUIDANCE PUTS PATIENTS FIRST



AI scribes - tools that transcribe and summarize provider-patient conversations directly into patients' medical records - hold the promise of improving healthcare efficiency by allowing providers to spend more time on patient care and less on note-taking and administrative tasks. However, certain privacy risks, if not properly managed, could damage people's trust in the health system.

On Data Privacy Day, January 28, 2026, the OIPC released guidance to help healthcare organizations understand those risks and comply with the law. *PIPA and AI scribes: best practices for healthcare organizations in BC* offers privacy considerations for healthcare organizations under BC's *Personal Information Protection Act* (PIPA), including independent health practitioners, most primary care clinics, and a variety of other health-related organizations operating outside of the public system.

Unlike traditional note-taking, AI scribes may collect people's biometric data, such as voice recordings. Patients may not know what happens with their information once it's collected, including how AI vendors may be using it. Errors introduced into patients' medical records through AI hallucinations, omissions and misspellings could also have catastrophic consequences in healthcare settings.

The guidance provides a framework for the privacy-protective use of AI scribes in clinical settings. It emphasizes that patients have the right to decline or withdraw their consent for the use of AI scribes, and that healthcare organizations remain responsible for PIPA compliance when using AI tools. This includes making sure that all collections, uses and disclosures of people's personal information are reasonable, and that security obligations under PIPA are met. The guidance includes a self-assessment tool that healthcare organizations can use to evaluate PIPA compliance when considering these tools.

Commissioner Harvey said that the release of the guidance, the first AI-specific resource published by the office, on Data Privacy Day reflected how important trustworthy innovation is in the health sector.

"Patients share some of their most intimate and sensitive personal information in conversations with their healthcare providers. As healthcare organizations incorporate AI scribes into their practices, patients' trust depends on this sensitive information being properly protected. This guidance document provides a roadmap so people can benefit from these technologies while trusting that their rights are protected."

Download

PIPA and AI scribes: best practices for healthcare organizations in BC

TRUST AFTER TRAGEDY

Investigation into privacy breaches linked to Lapu Lapu Day festival underscores urgency of protecting patient privacy in times of crisis

Following the tragedy at the 2025 Lapu Lapu Day festival in Vancouver, 32 people were sent to hospital throughout the Lower Mainland. An OIPC investigation found that in the days and weeks that followed, half of those people would have their privacy breached by healthcare workers.

The OIPC put the wellbeing of those affected first by taking a trauma-informed approach to all aspects of the investigation, which included engaging an expert clinician for advice on how to provide transparency without re-traumatizing those affected.

The investigation found 71 incidents in which 36 healthcare workers accessed the private medical records of those affected without authorization. These incidents took place at Vancouver Coastal Health (VCH), Fraser Health Authority (FHA), Providence Health Care (PHC) and the Provincial Health Services Authority (PHSA). All but one of these incidents were employee violations of section 25.1 of the *Freedom of Information and Protection of Privacy Act* (FIPPA), which prohibits people working for public bodies from collecting, using, or disclosing personal information, except as authorized by FIPPA (the other involved a healthcare worker in private practice who inappropriately accessed a public healthcare database).

Commissioner Michael Harvey expressed his sympathy and condolences for those who experienced the tragedy and spoke to the threat that breaches like this pose to people's trust in the healthcare system.

"Snooping is illegal, unethical, and an egregious and intentional invasion of our privacy, and it breaks trust with those in healthcare that are serving us in a time of need," he said. "As we move deeper into digitization of healthcare services, where more information is collected and accessible through the use of multiple information systems, it is essential for public bodies,

and those that work for them, to uphold their obligations to protect personal information. Only by doing so can the public's trust in their healthcare system be maintained."

The investigation found that the three health authorities had reasonable safeguards in place – including mandatory privacy training, confidentiality agreements, role-based access controls and audit logging – and that they moved quickly to issue staff reminders about privacy and confidentiality, flagged patient records for additional protections and monitoring, audited access to those records, commenced investigations into suspected unauthorized access, and imposed disciplinary measures.

Commissioner Harvey also stressed the importance of notifying individuals whose personal information was breached without delay. VCH and PHSA initially did not notify affected individuals, reasoning that it was not required and doing so could cause them unnecessary stress.

The Commissioner noted that while this decision was not made lightly, the response did not meet their legal obligation under FIPPA to notify without unreasonable delay and individuals have a right to know when their healthcare information has been compromised. The expert consultant engaged by the OIPC advised on how notification could be carried out in a trauma-informed manner.

The report includes nine recommendations, including a call for stronger automated auditing tools, reviewing role-based access controls, and applying disciplinary measures for snooping that are strong enough to effectively sanction and deter it.

All 36 healthcare workers caught snooping were disciplined, with consequences ranging from letters of expectation to termination, with most receiving suspensions. As nearly half of them were regulated health professionals, the Commissioner wrote to the Minister of Health recommending that it be mandatory for employers to report snooping-related offences that result in suspensions or terminations to regulatory colleges.

Commissioner Harvey acknowledged the cooperation and work of the health authorities throughout the investigation.

While the stakes are especially high in the health sector given the sensitivity of the information involved and the trust patients place in care providers, the Commissioner said the report's findings were relevant to every public body entrusted with the personal information of people in this province.

"I call on all public bodies to review the recommendations in this report, and their own protocols, to prevent snooping and reinforce that it cannot be tolerated," said Commissioner Harvey.

Download

Investigation Report 26-02: Privacy breaches following the Lapu Lapu Day Festival
News release, video overview and overview fact sheet

LEGAL UPDATES

One court ruling upheld the OIPC's authority to call organizations to account to protect people's fundamental right to privacy, especially as new technologies test jurisdictional boundaries. Another court ruling, headed for the Supreme Court of Canada, centred around questions of how BC's privacy laws apply when they come into conflict with religious beliefs.

Clearview AI

In February 2026, the BC Court of Appeal rejected US-based facial recognition company Clearview AI's claim that provincial privacy laws didn't apply to it.

Clearview AI had scraped billions of images from the internet – many from people's social media accounts – to train its facial recognition tool. Millions of these were from Canadians, many of them children. Following a 2021 joint investigation with the privacy commissioners of Canada, Alberta, and Quebec, the OIPC ordered Clearview AI to comply with the recommendations in the investigation report and prohibited the company from offering its facial recognition services to BC clients. The OIPC also ordered the company to cease its collection, use, and disclosure of personal information from individuals in the province without their consent, and to delete data already collected.

Clearview AI launched a petition for judicial review of the OIPC's Order with the BC Supreme Court, which was dismissed. The company then appealed to the BC Court of Appeal, claiming that provincial laws didn't apply to it and the OIPC's decision was incorrect.

The Court of Appeal upheld the OIPC's decision and confirmed that Clearview AI's collection of online facial data from people in BC constitutes a real and substantial connection between it and the province, and the OIPC had jurisdiction over such activities. The Court of Appeal also found the OIPC's order was reasonable and enforceable.

Clearview AI has filed for leave to appeal to the Supreme Court of Canada.

OIPC Order 21-08, Clearview AI, Inc.
Clearview AI Inc. v. British Columbia (Information and Privacy Commissioner), 2026 BCCA 67 (CanLII)

Vabuolas v British Columbia (Information and Privacy Commissioner)

The Supreme Court of Canada will be hearing a case involving a religious organization and the application of the *Personal Information Protection Act* (PIPA) to its activities.

Two former members of Jehovah's Witnesses requested their personal information from the Grand Forks and Coldstream Congregations under PIPA. The congregations refused to disclose certain records, stating they contained privileged and confidential religious communications.

The requesters asked the OIPC to review those decisions. The congregations declined to produce the disputed records, arguing that disclosure to anyone, including the Commissioner, would violate their religious beliefs. After considering the *Canadian Charter* of *Rights and Freedoms*, the adjudicator ordered production of the records under s. 38(1)(b) of PIPA, so they could determine what information, if any, should be provided to the requesters.

The BC Supreme Court dismissed a petition for judicial review. The Court of Appeal also dismissed the appeal, though on different grounds, holding that PIPA itself does not infringe the *Charter.* Rather, the statute empowers the Commissioner to consider *Charter* rights when exercising discretion, and the production order in this case reflected a proportionate balancing of religious freedom against PIPA's statutory objectives.

The Supreme Court of Canada granted the congregations' leave to appeal on November 20, 2025, and is expected to hear the appeal some time within the next year. Numerous interveners have filed motions to participate.

OIPC Order P22-03, Grand Forks Congregation of Jehovah's Witnesses and Coldstream Congregation of Jehovah's Witnesses

2024 BCSC 27 (CanLII) | Vabuolas v British Columbia (Information and Privacy Commissioner) | CanLII

2025 BCCA 83 (CanLII) | Vabuolas v. British Columbia (Information and Privacy Commissioner) | CanLII

Supreme Court of Canada | 41816, John Vabuolas, et al. v. Information and Privacy Commissioner for British Columbia, et al.

HIGHLIGHTS

Access and privacy regulators call for government transparency, privacy-protective EdTech

In October, federal, provincial, and territorial information and privacy commissioners, and ombudspersons responsible for access and privacy, met in Banff, Alberta to discuss urgent issues impacting Canadians' access and privacy rights.

Together, they issued two joint resolutions aimed at protecting fundamental rights as technological innovation reshapes how citizens access information and how children learn. The first of the two resolutions "Trust, transparency, and democracy in an era of misinformation," adopted by those with access to information oversight, called on governments to embrace transparency as an essential defence against a rising tide of misinformation, disinformation, and malinformation.

"Misinformation spreads at an unprecedented rate in our digital age, with algorithms able to move misinformation much quicker than it can be contained. Our best defence against this threat to our democracy is transparency," said Commissioner Harvey.

The resolution called on governments to modernize their access laws, increase proactive disclosure, and take a "transparency by default" approach to program design. The second resolution, passed by those with privacy oversight, focused on educational technologies (EdTech) in Canadian classrooms.

The resolution notes that while these technologies offer tremendous benefits, they can also leave children and youth with little choice but to use platforms that collect and use their personal information and may put them at risk of data breaches, student profiling, biometric surveillance, and deceptive design practices.

Regulators called on governments, schools, and vendors to protect and make children's privacy a priority during initial product design through to assessment, procurement, and deployment.

"This resolution calls on us to shape the future we want for our kids by putting their rights first," said Commissioner Harvey. "By protecting children's privacy rights today, we empower them to benefit from EdTech, while developing the autonomy, digital literacy, and awareness of their own rights that they'll need as adults in the Information Age."

Downloads

Trust, transparency, and democracy in an era of misinformation
Protecting the privacy of children and youth in the classroom through responsible educational technologies

Commissioner addresses youth privacy, health data sharing at Global Privacy Assembly

How can we make sure that young people enjoy the benefits of technological innovation while protecting their privacy and related rights to free expression, safety, and fair treatment? How can we responsibly and effectively share health data across borders?

Countries around the world are grappling with these questions, which were at the center of two discussions Commissioner Harvey joined as part of the 47th Global Privacy Assembly (GPA), held in Seoul, Korea in September.

The GPA brings together more than 130 data protection and privacy authorities from across the world to collaborate on pressing privacy challenges.

Commissioner Harvey moderated a panel titled "Youth Privacy: Mechanics," that challenged the notion that young people must sacrifice their privacy rights to benefit from technology. Panelists from the 5Rights Foundation, the Personal Information Protection Commission of Korea, TikTok, and Apple explored this question from advocacy, regulatory, and industry perspectives. Commissioner Harvey drew out the theme that we don't need to choose between innovation and the rights of children to privacy, but rather that firms can innovate on *how* to protect people's privacy.

The Commissioner also presented on the secondary use of health data for public interest purposes, as part of a side event at the GPA organized by the Organisation for Economic Co-operation and Development (OECD).

Drawing on his experience as a member of the expert panel that developed the Pan-Canadian Health Data Charter, Commissioner Harvey spoke of the importance of taking a person-centric approach to health data sharing.

He emphasized the need for coordination across multiple interwoven strands to make that sharing effective: privacy laws, technical interoperability, data standards, health human resources, and data governance and stewardship.

"We should not be satisfied with anything less than strong privacy protections that enable and accelerate the beneficial use of health data for the public good," he said.

Downloads

Identifying and mitigating harms from privacy-related deceptive design patterns

Responsible information-sharing in situations involving intimate partner violence

Transparency by default: Information regulators call for a new standard in government service

HIGHLIGHTS

Commissioner advocates for the privacy rights of British Columbians in Senate appearance

On February 12, 2026, Commissioner Harvey appeared as a witness before the Senate's Standing Committee on Legal and Constitutional Affairs to speak about Bill C-4, *An Act respecting certain affordability measures for Canadians and another measure*. Commissioner Harvey spoke to Part 4 of the Bill, which proposed amendments to the *Canada Elections Act* that would exempt federal political parties from provincial privacy laws – retroactively to the year 2000.

Unlike the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies only to organizations engaged in commercial activity and to information about employees of federal entities, the provincial *Personal Information Protection Act* (PIPA) applies to organizations and their use of personal information whether or not their activity is commercial in nature. As a result, the OIPC has jurisdiction with oversight of the privacy practices of all political parties operating in BC, be they federal, provincial, or municipal. The extent of PIPA's jurisdiction over federal provincial parties was considered in an order issued by the Commissioner's Delegate, David Loukidelis, (Order P22-02) which was subsequently upheld on judicial review by the BC Supreme Court and is currently pending an appeal at the BC Court of Appeal.

In his remarks, Commissioner Harvey stated that by enacting PIPA, the people of BC determined that they desire a certain level of legal protection from all organizations, including all levels of political parties. As drafted, Bill C-4 would frustrate the democratic will of British Columbians by ousting PIPA "by brute force" and leaving no equivalent protections in its place.

The senators introduced an amendment that would lead to Part 4 expiring after a period of three years. The House of Commons rejected that amendment, and both chambers subsequently passed the bill into law. In the meantime, the federal government has announced its commitment to introducing additional privacy protections to the *Canada Elections Act* within the same parliamentary session.

Download

Speech to the Standing Senate Committee on Legal and Constitutional Affairs
Order P22-02

Order finds Vancouver Police Department required to refuse release of 911 call audio

Recordings from 911 calls contain significant personal information – including voices that may reveal details about a person's identity, emotional state, and background. As such, access requests for those recordings must be assessed carefully.

In Order F25-71, an applicant sought access from the Vancouver Police Department (VPD) to recordings of 911 calls from a crisis line worker who had reported concerns about the applicant.

The content of the calls was not in question as the applicant already had transcripts of both, which the adjudicator found to be accurate. The issue was about access to the voices themselves. The adjudicator noted that during the recordings, the caller is identified by name and their voice is audible, as are the voices of the call-taker and the dispatcher. All three voices allow one to make inferences about gender, age, and first language. As such, the adjudicator found that VPD was required to withhold the information and deny the request.

10 years on, children's privacy protections still lacking: 2025 GPEN Sweep Report

Ten years after the Global Privacy Enforcement Network (GPEN) first examined how children's privacy rights were protected online, a new report from the group found that amid some progress, significant gaps remain – and some risks to children's privacy have increased.

The OIPC BC was among 27 regulators from around the world who participated in the 2025 GPEN Sweep. Together, the regulators examined the privacy policies and practices of 876 platforms commonly used by or targeted at young people.

The report showed progress in some areas since the 2015 sweep, including a significant increase in the use of age assurance, improvements in the accessibility of account deletion, and new approaches to protecting children's privacy.

However, while the report highlighted the increased attention given to children's privacy, regulators also identified serious challenges:

- Age checks were easily bypassed on 72% of platforms;
- More than 40% of websites and apps surveyed were deemed unsuitable for children by GPEN sweepers and lacked effective safeguards to keep them from using the platforms;
- Child-friendly privacy information was missing on most sites;
- Platforms were collecting more personal data from children than ever before; most say they may share personal information with third parties.

Commissioner Harvey said that the report highlighted why enhancing the privacy rights of youth and children is one of the key goals in the office's three-year strategic plan. "Too many websites and apps leave children vulnerable to tracking, profiling, targeting, and exposure to harmful content, while collecting more of their personal information than necessary. We want to see good intentions matched by effective protections to make sure children can thrive online without sacrificing their privacy," he said.

Download
GPEN Sweep Report: Children's Privacy
Children's safety online: GPEN Sweep 2025 (overview infographic)

YEAR IN NUMBERS

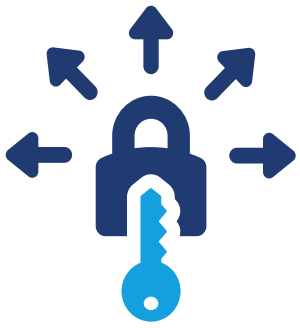
Summary of FIPPA and PIPA files received in 2025/26

	Received 25/26	Closed 25/26	Received 24/25	Closed 24/25
Privacy breach notification				
FIPPA	297	288	208	215
PIPA	234	241	210	200
Complaints				
Privacy complaints	904	887	456	521
Access complaints	784	736	448	490
Requests for review				
Requests for review of decisions to withhold information (RR and 3rd party RR)	1110	972	755	902
Deemed refusal	543	516	348	353
Applications to disregard requests as frivolous or vexatious	25	25	26	23
Time extensions				
Requests by public bodies and organizations (incl. s. 10 FIPPA and s. 31 PIPA)	2502	2503	2626	2626
Requests by applicants seeking a review (incl. s. 53 FIPPA and s. 47 PIPA)	45	37	11	13
Public interest disclosure notification (s. 25)	11	10	19	10
Requests for reconsideration of OIPC decisions	141	156	81	105
Information requests/received				
Requests for information	4496	4478	4111	4112
Non-jurisdictional issue	13	13	19	20
Request for contact information (research)	0	0	2	3
Media enquiries	72	73	70	73
FOI requests for OIPC records	43	39	30	28
s. 60 adjudication of OIPC decisions	2	2	3	3
Commissioner-initiated reports				
Privacy reports	n/a	3	n/a	1
Access reports	n/a	1	n/a	2
Policy				
Policy or issue consultation	229	238	161	150
Legislative reviews	51	53	21	20
Police Act IIO reports	54	59	53	52
Privacy impact assessments	38	43	55	54
Indirect collection	0	0	2	2
Public education and outreach				
Speaking engagements	82	93	54	50
Meetings with public bodies and private organizations	17	20	11	11
Other (includes all file types except those otherwise listed)	38	35	50	50
TOTAL	**11,731**	**11,521**	**9,821**	**10,089**

The OIPC has the authority to process and investigate request for reviews, privacy complaints, and access complaints.*

An individual can **request a review** if a public body does not respond to an access request within 30 business days, denies access to records, or if the individual disagrees with how the records were severed.

A **privacy complaint** can be made if there are concerns with how a public body or organization has handled or processed an individual's personal information.



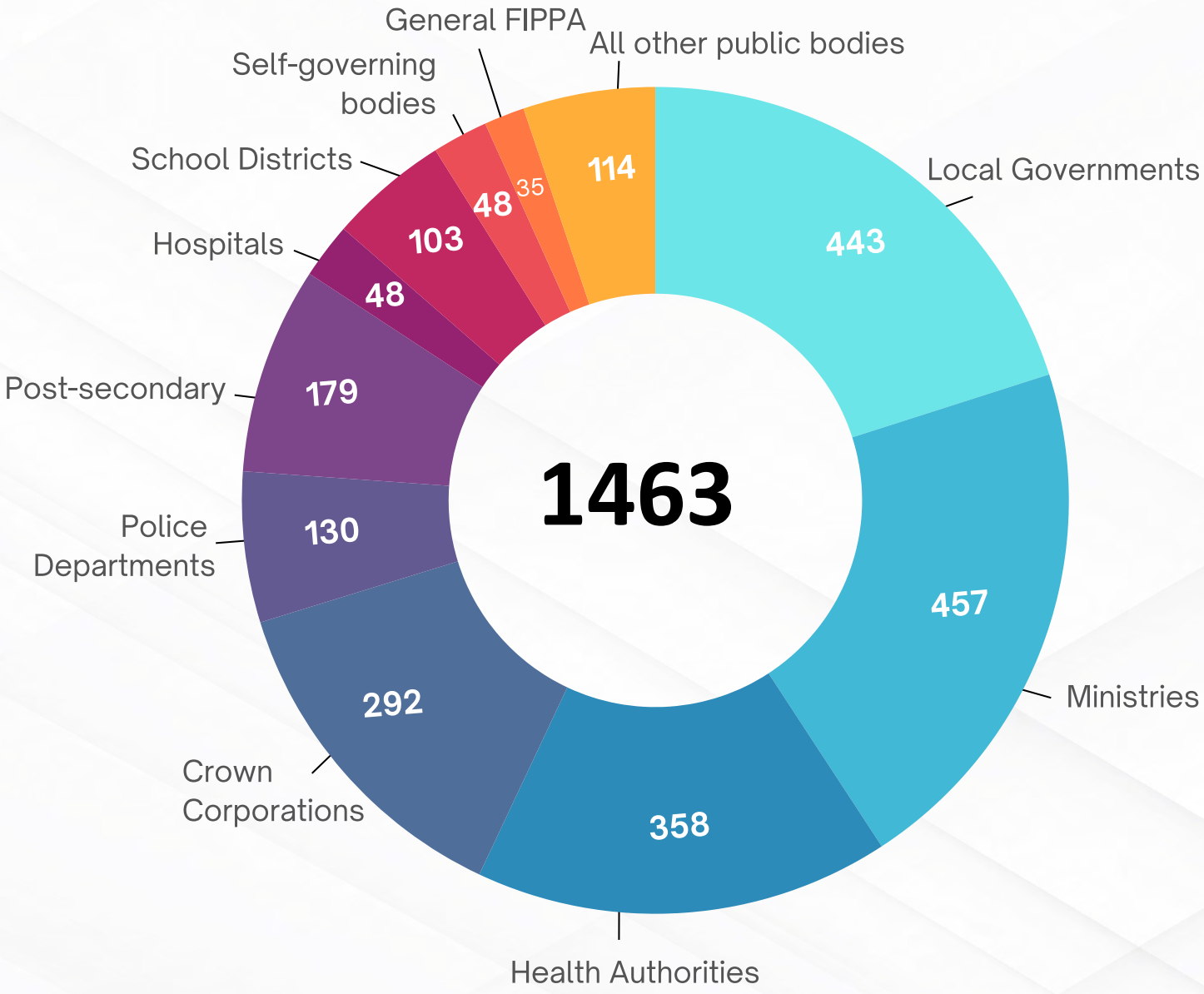
An **access complaint** can be made if there are concerns about how a public body or organization processed an access request.

*Investigator decisions on complaints and reconsiderations are subject to judicial review by the Supreme Court of British Columbia.

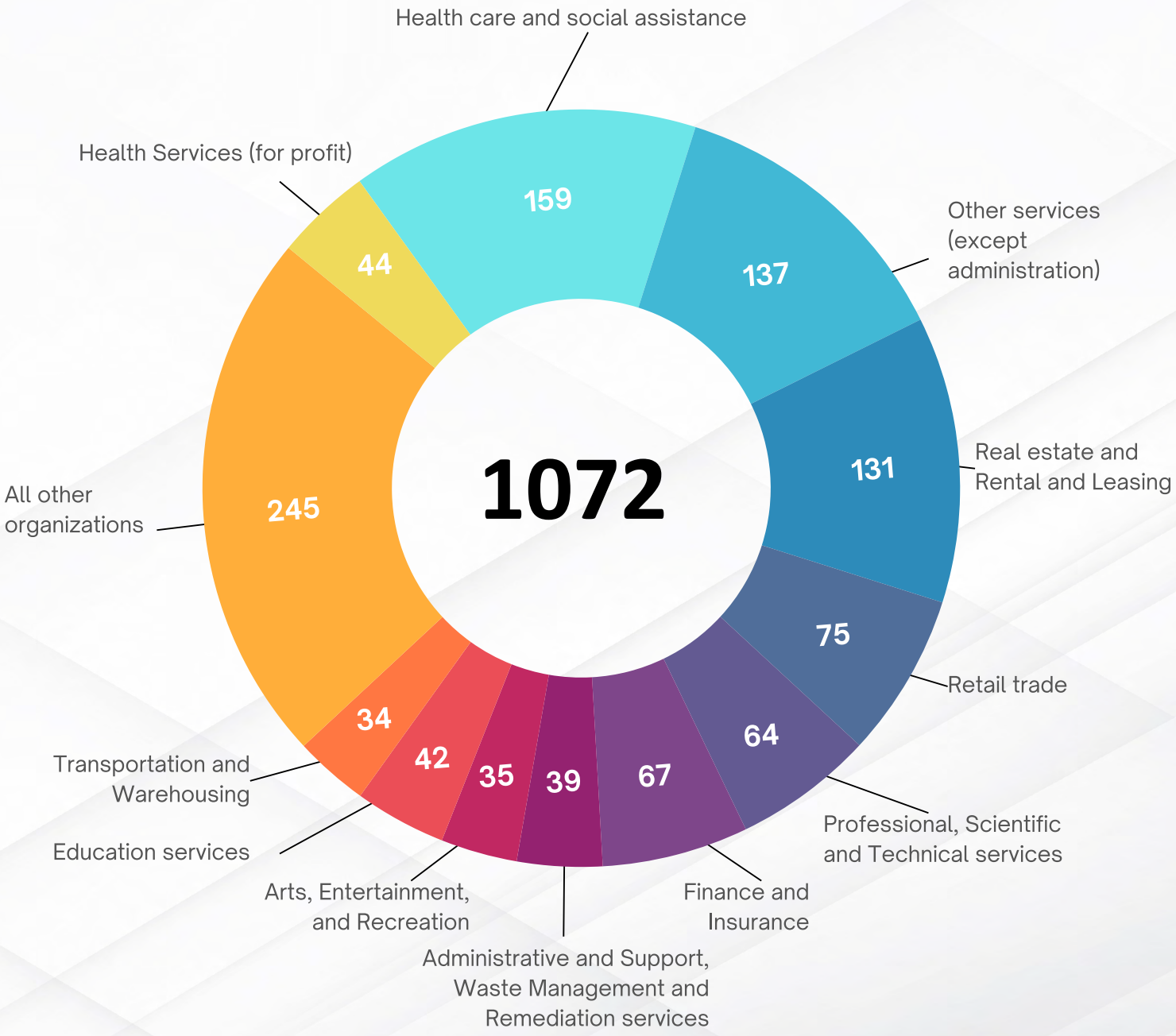
The following pages provide statistics on the requests for review and complaints that come before the office and are handled by the case review and investigations teams for 2025/26.

YEAR IN NUMBERS

The OIPC reports out on the proportion of **FIPPA complaints and requests for review received by public body type** in the fiscal year. This breakdown does not indicate whether the outcome was in favour of the public body or the individual.

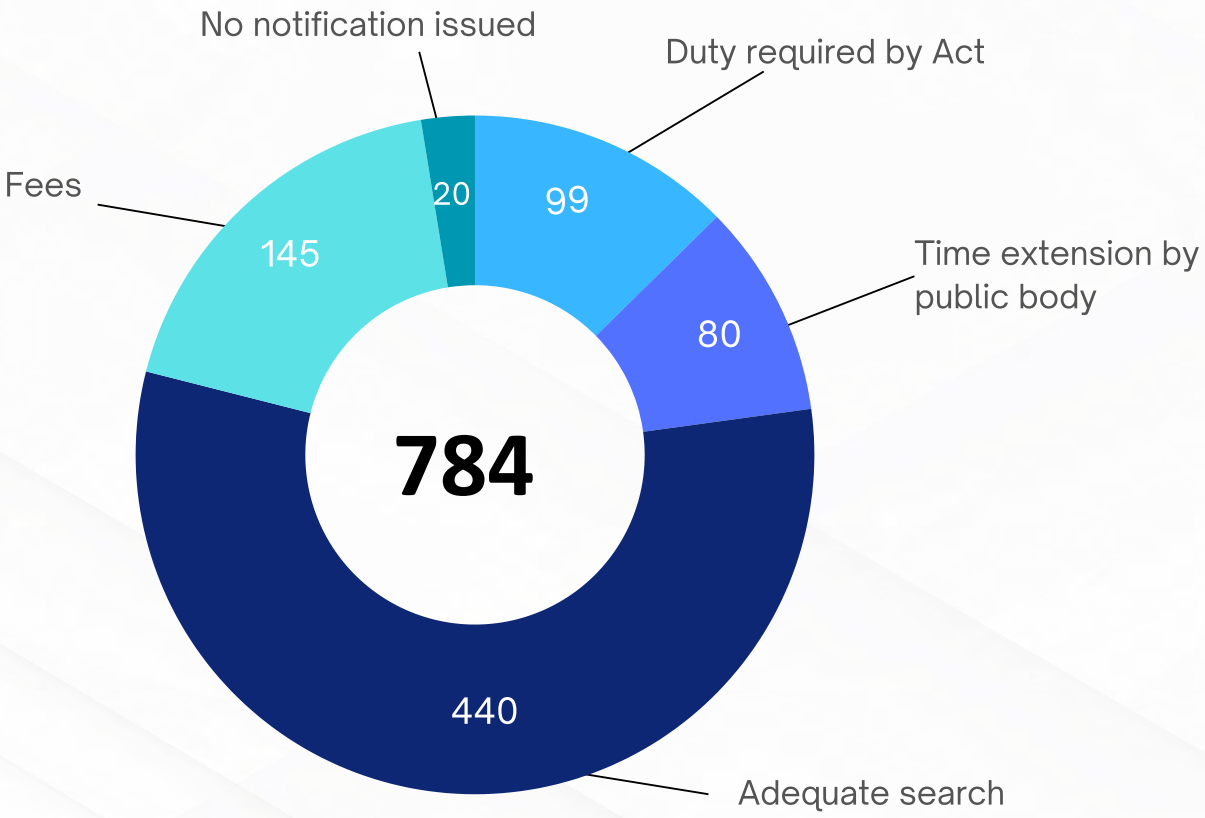


The OIPC reports out on **PIPA complaints and requests for review by sector** in the fiscal year. Inclusion in this list does not indicate whether the outcome was in favour of the organization or the individual.



YEAR IN NUMBERS

The OIPC received **784** **access complaints** in 2025/26. The breakdown of the types of complaints for both FIPPA and PIPA is:



Duty required by Act
Failure to fulfill any duty required by FIPPA (other than an adequate search)

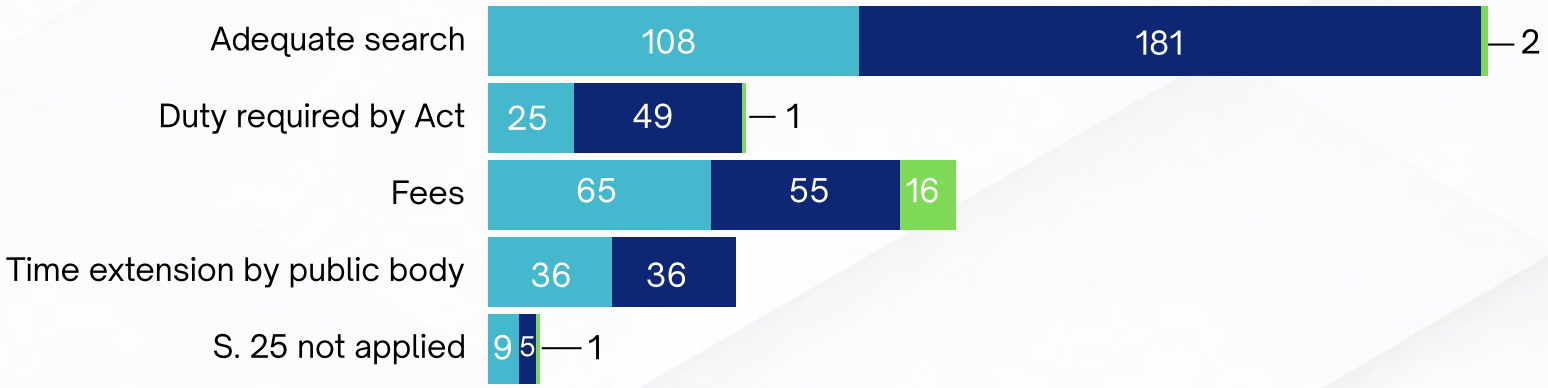
Time extension by public body
Unauthorized time extension taken by public body

Adequate search
Failure to conduct adequate search for records

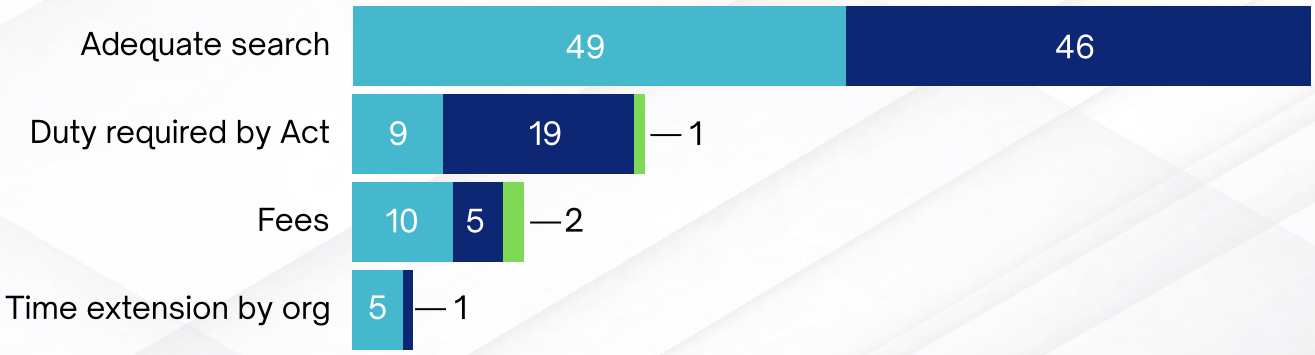
Fees
Unauthorized or excessive processing fees assessed by public body

No notification issued
Failure to notify as required under s. 25 of FIPPA

The OIPC resolved **589 FIPPA access complaints** in 2025/26. A complaint can ultimately result in an investigation, no investigation, or an inquiry. In 2025/26, 243 investigations were conducted on access complaints, 326 complaints resulted in no investigation, and 20 files proceeded to inquiry.



The OIPC resolved 147 **PIPA access complaints** in 2025/26. A complaint can ultimately result in an investigation, no investigation, or an inquiry. In 2025/26, 73 investigations were conducted on access complaints, 71 complaints resulted in no investigation, and 3 files proceeded to inquiry.



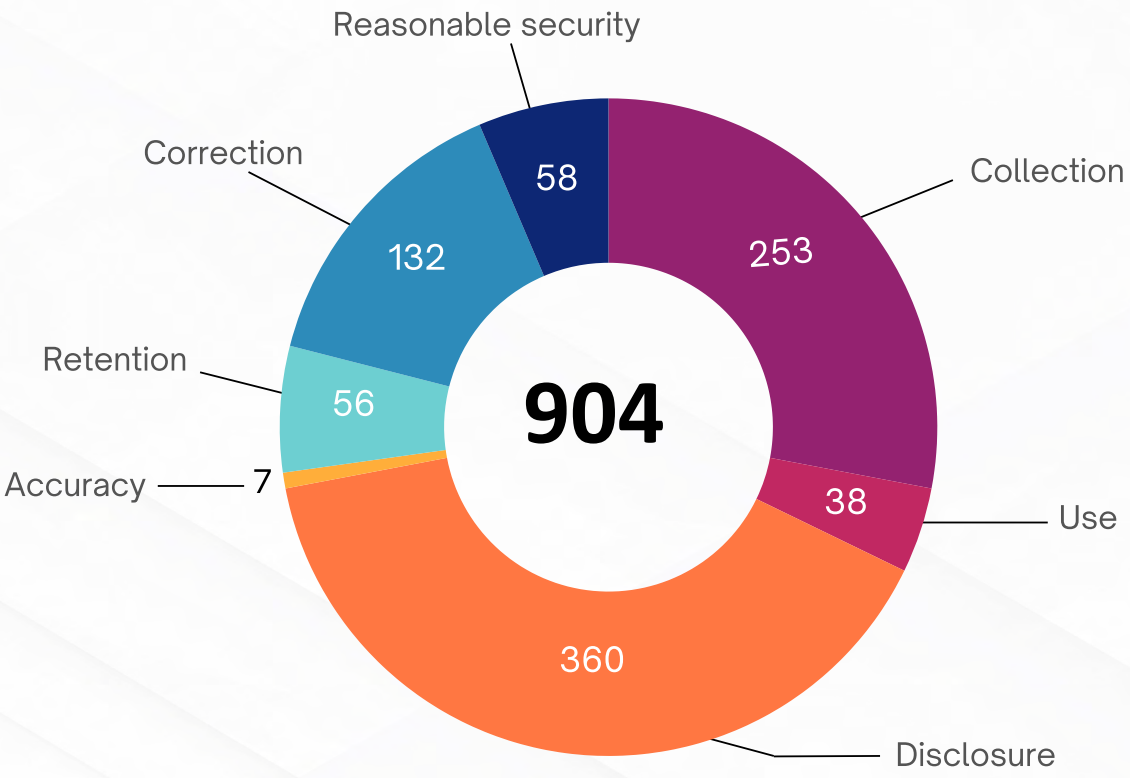
Investigation
Files that were mediated, not substantiated, partially substantiated, substantiated, and withdrawn

No investigation
Files with no jurisdiction, no reviewable issue, or files in which the OIPC referred the complainant back to the public body or declined/continued an investigation

Inquiry
Files that proceeded to inquiry

YEAR IN NUMBERS

The OIPC received **904 privacy complaints** in 2025/26. The breakdown of complaints for both FIPPA and PIPA is:



Collection
Unauthorized collection of information

Use
Unauthorized use by the public body or private organization

Disclosure
Unauthorized disclsoure by a public body or private organization

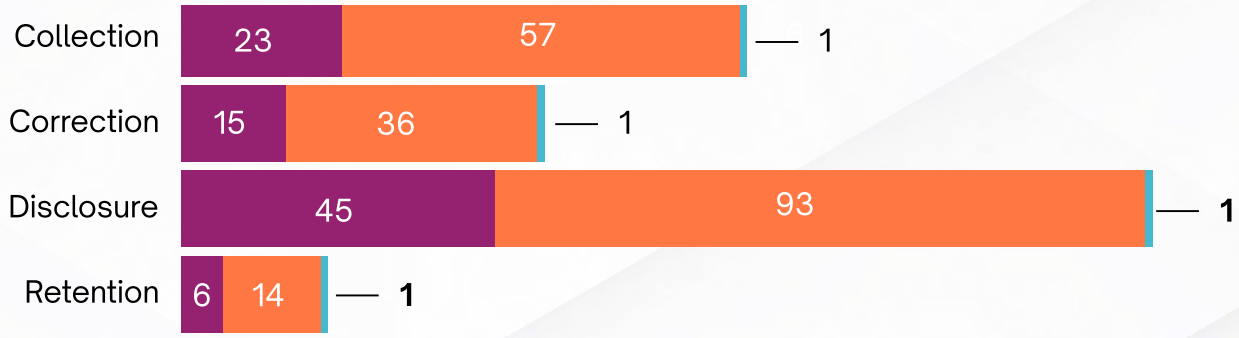
Accuracy
Personal information in the custody or control of a public body is inaccurate or incomplete

Correction
Refusal to correct or annotate information in a record

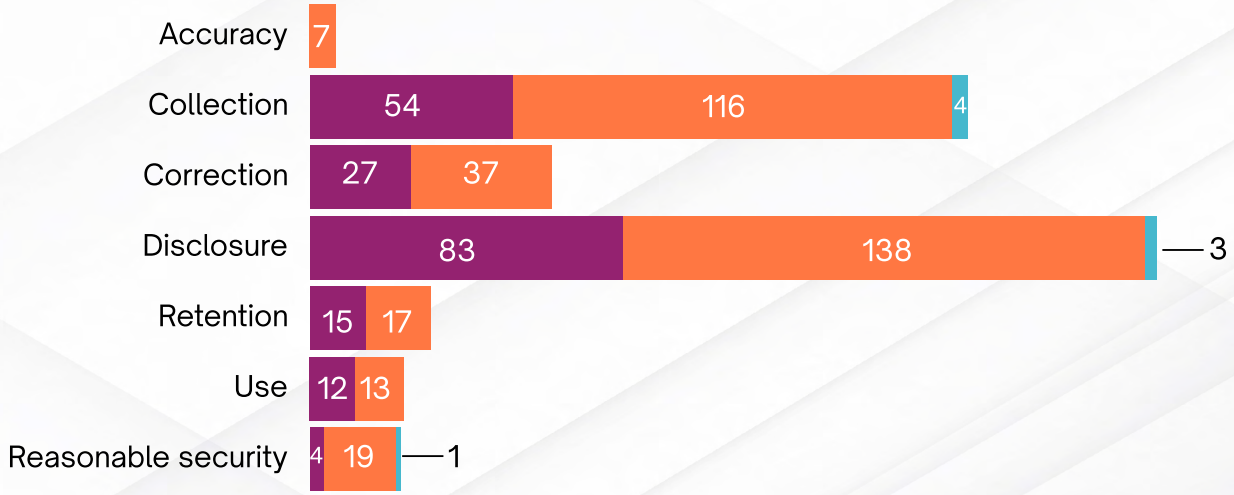
Reasonable security
Failure to implement reasonable security measures

Retention
Failure to retain information for the time required

The OIPC resolved **337 FIPPA privacy complaints** in 2025/26. A complaint can ultimately result in an investigation, no investigation, or an inquiry. In 2025/26, 103 investigations were conducted on privacy complaints, 229 complaints resulted in no investigation, and 5 files proceeded to inquiry.



The OIPC resolved **550 PIPA privacy complaints** in 2025/26. A complaint can ultimately result in an investigation, no investigation, or an inquiry. In 2025/26, 195 investigations were conducted on access complaints, 347 complaints resulted in no investigation, and 8 files proceeded to inquiry.



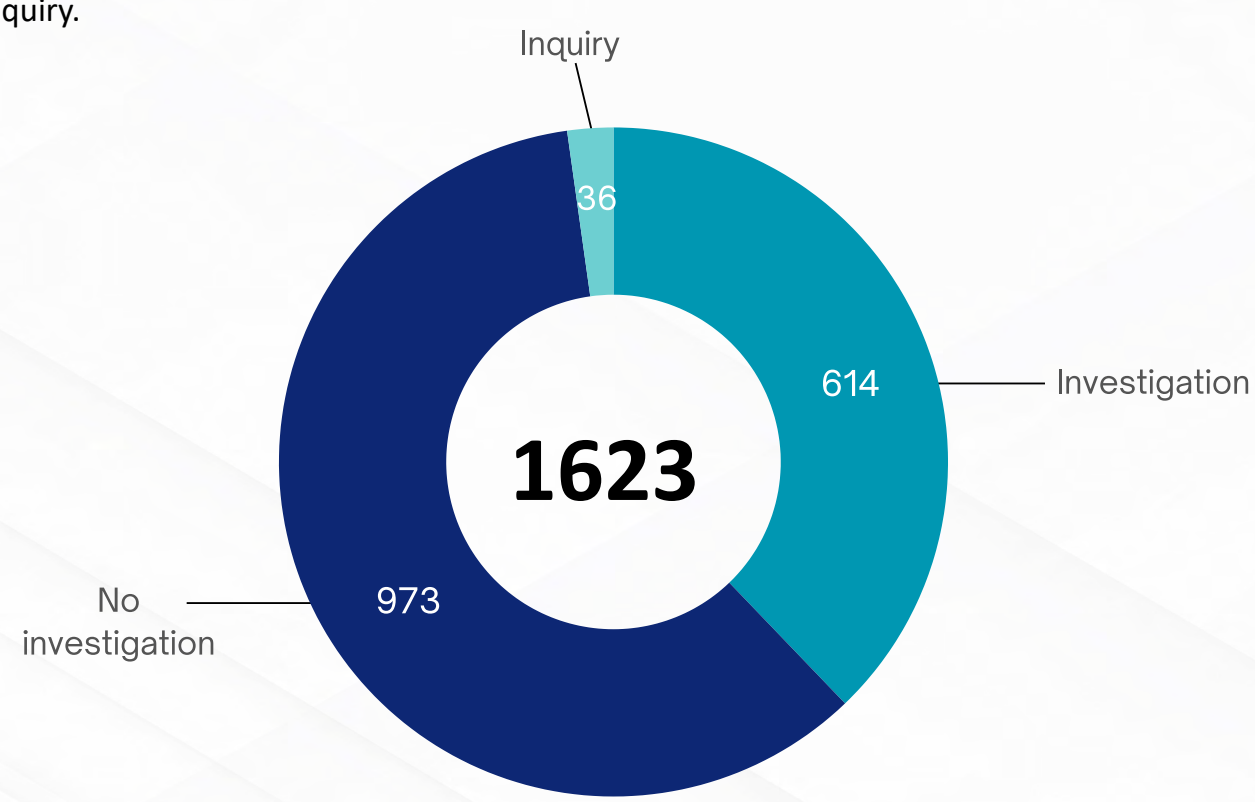
Investigation
Files that were mediated, not substantiated, partially substantiated, substantiated, and withdrawn

No investigation
Files with no jurisdiction, no reviewable issue, or files in which the OIPC referred the complainant back to the public body or declined/continued an investigation

Inquiry
Files that proceeded to inquiry

YEAR IN NUMBERS

Overall, the OIPC resolved **1623 FIPPA and PIPA access and privacy complaints** in 2025/26. There were 614 investigations, 973 files resulted in no investigation, and 36 proceeded to inquiry.



Investigation

Files that were mediated, not substantiated, partially substantiated, substantiated, and withdrawn

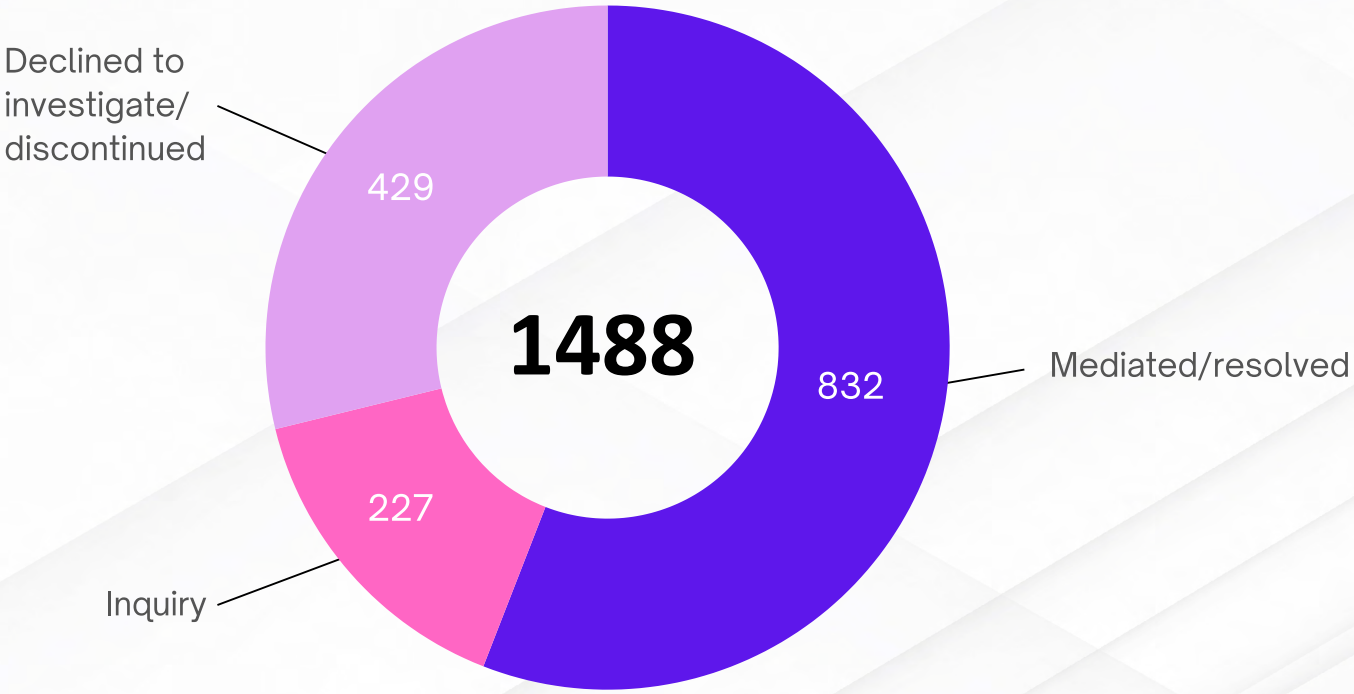
No investigation

Files with no jurisdiction, no reviewable issue, or files in which the OIPC referred the complainant back to the public body or declined/ continued an investigation

Inquiry

Files that proceeded to inquiry

Overall, the OIPC resolved **1488 FIPPA and PIPA requests for review** in 2025/26. There were 832 files that were mediated/resolved, 227 proceeded to inquiry, and 429 were declined or discontinued.



Mediated/resolved

Files that were mediated, not substantiated, partially substantiated, substantiated, and withdrawn

Inquiry

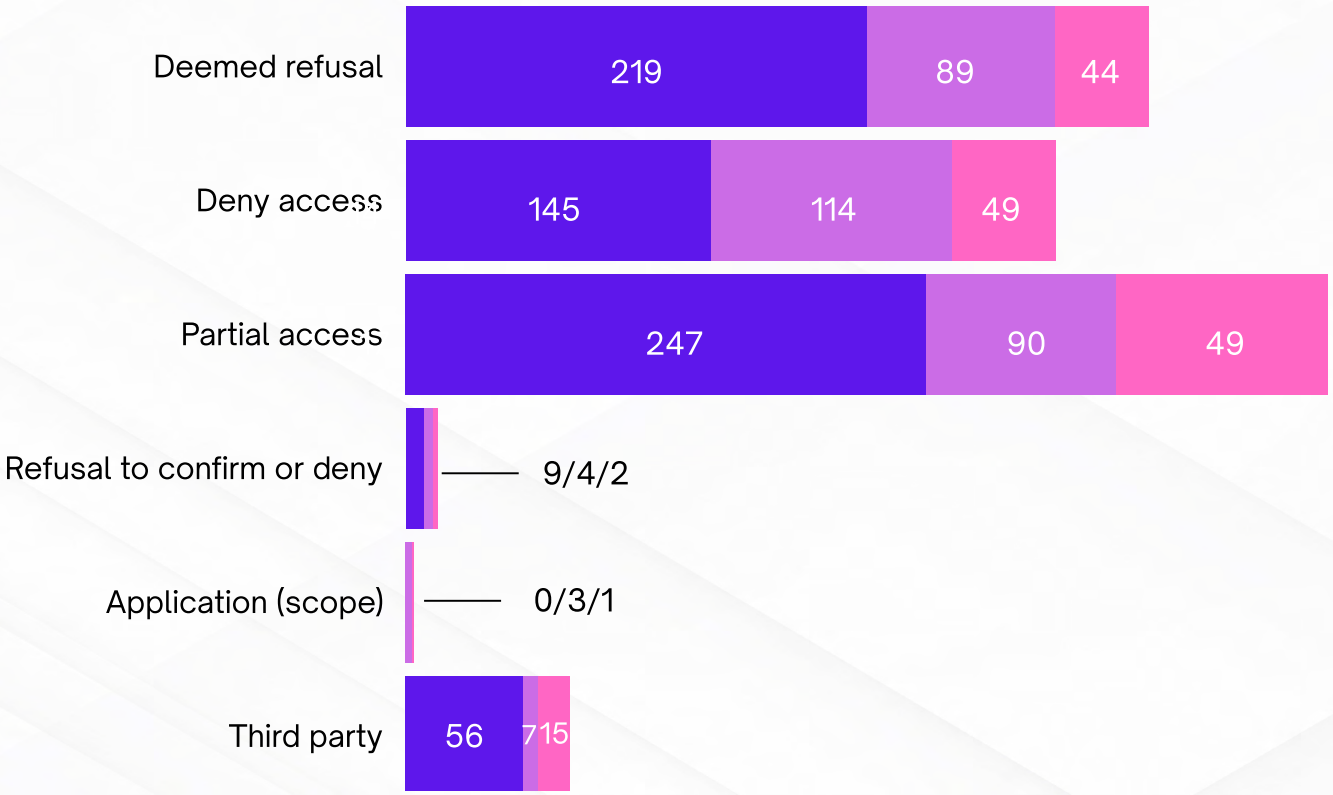
Files that proceeded to inquiry

Declined to investigate/discontinued

Files that were declined or discontinued, closed due to no jurisdiction, no reviewable issue, or the applicant referred back to the public body

YEAR IN NUMBERS

The OIPC resolved **1194 FIPPA requests for review** in 2025/26. A request for review can ultimately be resolved through mediation, declined or discontinued, or proceed to an inquiry. In 2025/26, 676 FIPPA request for review files were mediated/resolved, 307 files were declined or discontinued, and 211 files proceeded to inquiry.

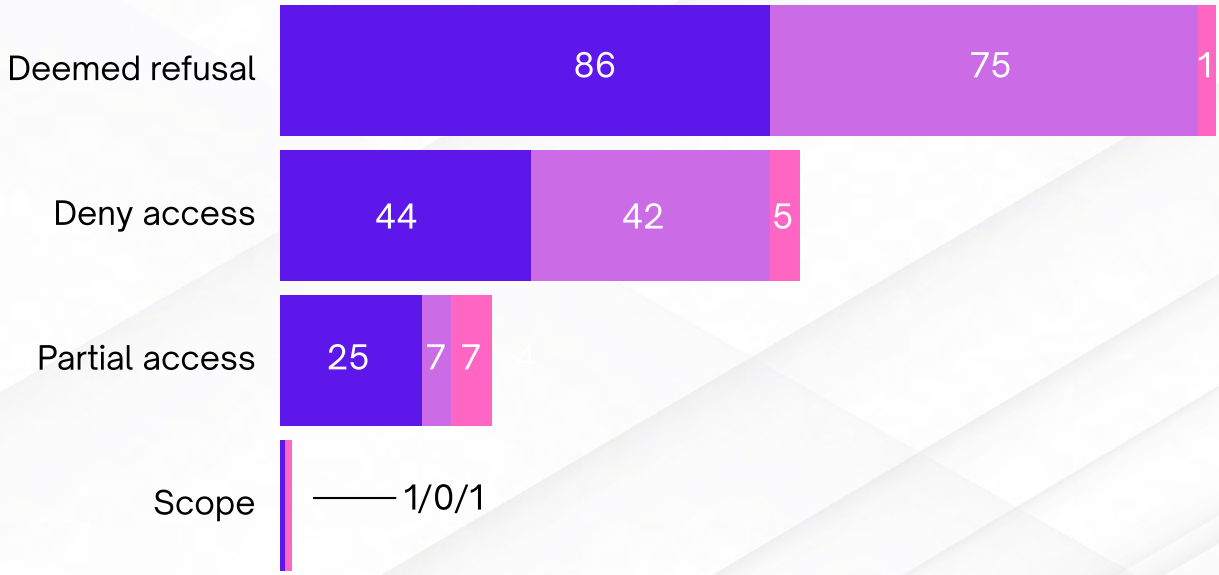


Mediated/resolved
Files that were mediated or withdrawn

Declined to investigate/discontinued
Files with no jurisdiction, no reviewable issue, or files in which the OIPC referred the complainant back to the public body or declined/discontinued an investigation

Inquiry
Files that proceeded to inquiry

The OIPC resolved **294 PIPA requests for review** in 2025/26. A request for review can ultimately be resolved through mediation, declined or discontinued, or proceed to an inquiry. In 2025/26, 156 PIPA request for review files were mediated/resolved, 122 files were declined or discontinued, and 16 files proceeded to inquiry.



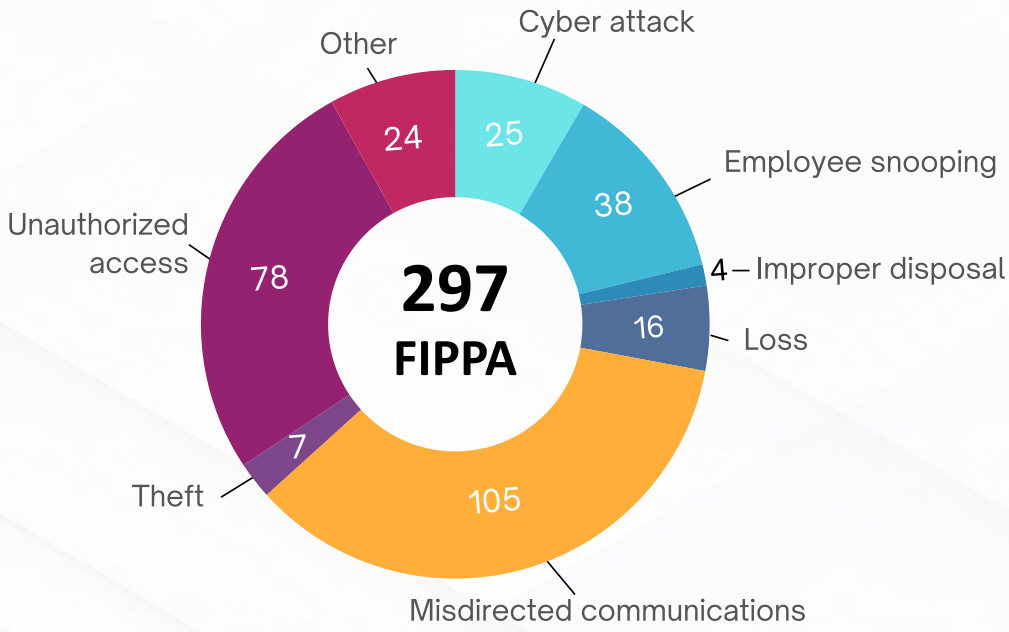
Mediated/resolved
Files that were mediated or withdrawn

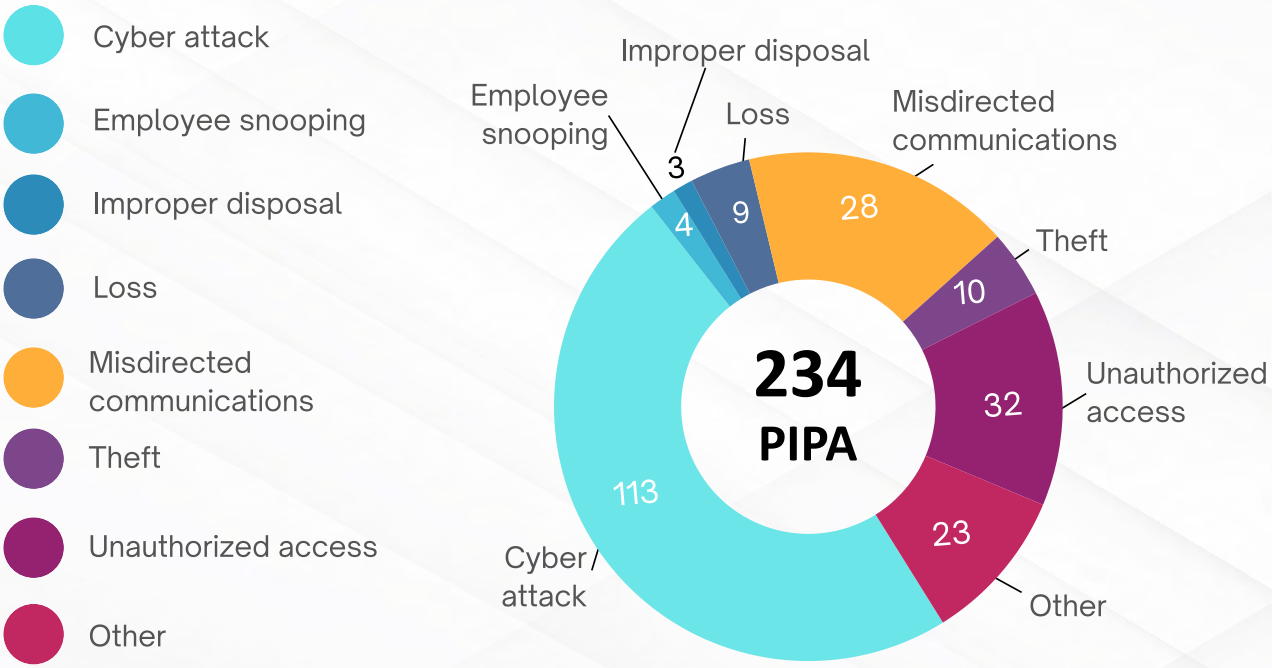
Declined to investigate/discontinued
Files with no jurisdiction, no reviewable issue, or files in which the OIPC referred the complainant back to the public body or declined/discontinued an investigation

Inquiry
Files that proceeded to inquiry

YEAR IN NUMBERS

The OIPC documents the **cause of breaches** when incidents are reported to the Commissioner's office. Public bodies and organizations can focus training and security measures based on the cause of their breaches.





Complaints and requests for review files closed by stage of resolution

April 1, 2025-March 31, 2026

The two main types of files processed by the OIPC are **access and privacy complaints**, and **requests for review** of access to information responses.

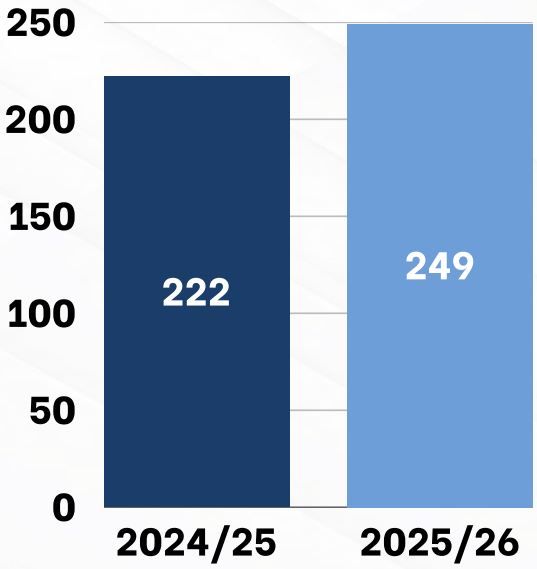
Complaints and requests for review are often resolved early on by case review officers or investigators. Some files that cannot be resolved during these stages are sent to adjudication.

ADJUDICATION

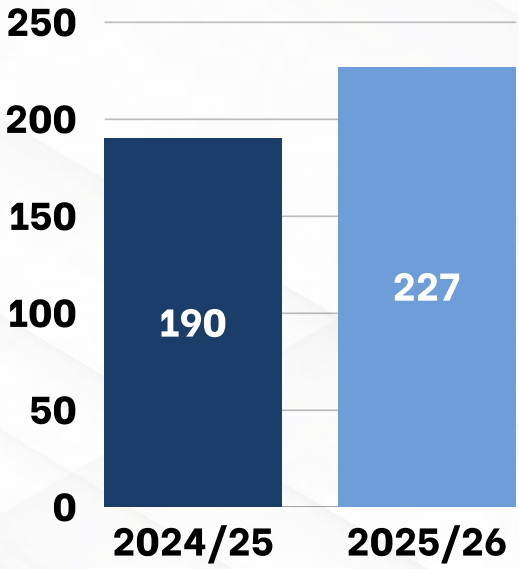
When investigation and mediation do not resolve a dispute, the Commissioner or their delegate may conduct an inquiry. At the inquiry, the adjudicator reviews written evidence and arguments, decides all questions of fact and law and issues a binding order. Orders are subject to judicial review by the Supreme Court of British Columbia.

The following orders provide a snapshot of the varied nature of the cases handled at adjudication over the past year:

- An applicant requested to participate in an OIPC inquiry anonymously. (Decision F25-02)
- An applicant requested access from the Minister of the Attorney General for records regarding a criminal matter. This order is under judicial review. (Order F26-13)
- A journalist requested access to messages sent and received on a messaging app by three Vancouver Board of Parks and Recreation commissioners. (Order F26-18)
- The executor of a deceased person's estate successfully established that they were an appropriate person authorized to exercise the deceased's access rights, and sought access to the deceased's medical records. (Order F25-55)

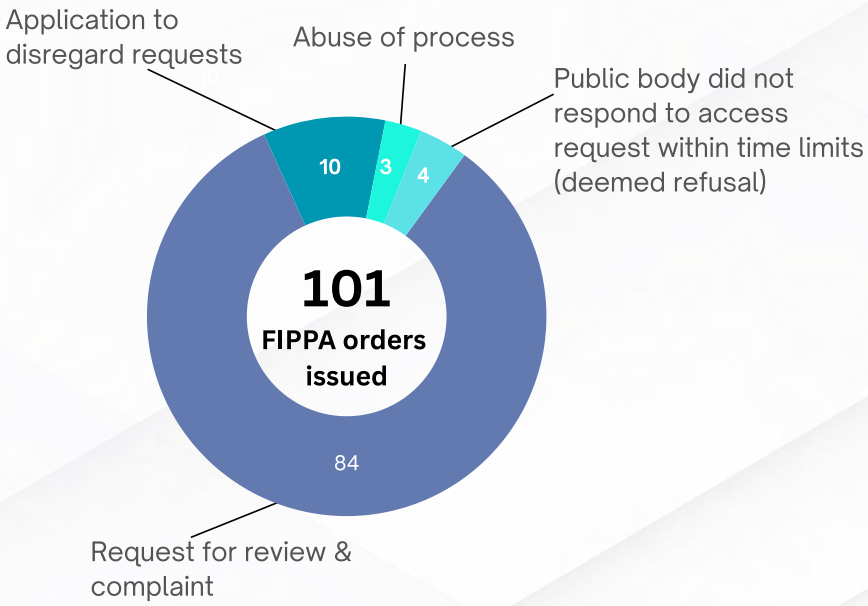


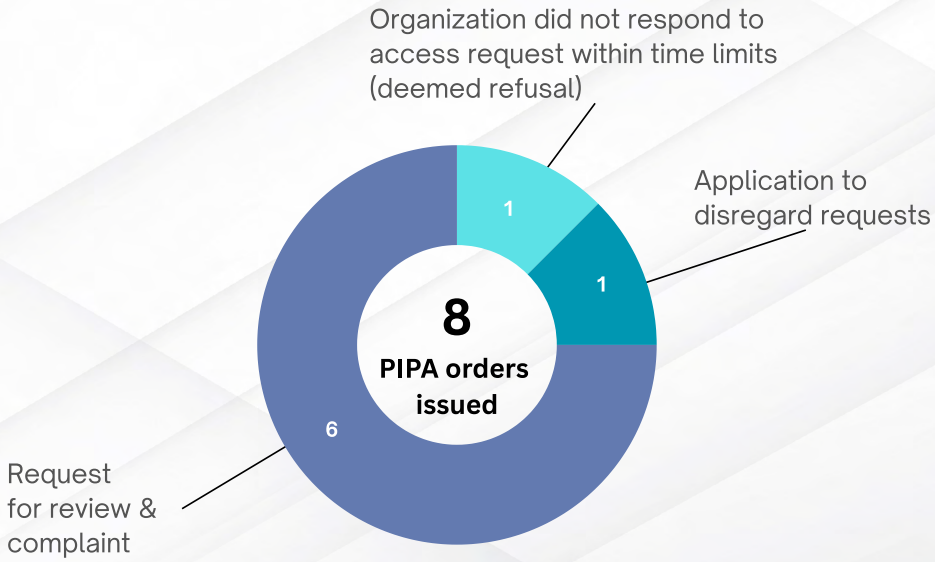
Files sent to inquiry



Files closed at inquiry

Breakdown of orders issued





SERVICE PLAN

SERVICE PLAN GOAL 1

Uphold privacy rights and monitor protection of personal information

This goal includes education and consultation support to public and private sector organizations in having effective privacy management programs in place.

OIPC case review officers and investigators handle a large number of privacy complaints from people in BC. When processing complaints, OIPC staff educate public bodies and organizations as appropriate to promote privacy rights and the protection of the personal information of people in BC.

Audit, special and investigation reports represent Commissioner-initiated audits and investigations into matters of broad public interest, and they often provide recommendations and guidance relating to privacy management programs. They are a compliance and education tool for public bodies, organizations, and the people of BC in relation to privacy rights and responsibilities under PIPA and FIPPA. Performance measures for these reports and uptake of the corresponding recommendations are under Goal 1 when they relate to privacy, and Goal 2 when they relate to access to information.

The OIPC published three investigation reports involving privacy matters. *Joint investigation of TikTok Pte Ltd* was conducted with the federal privacy commissioner and provincial counterparts in Quebec and Alberta into TikTok, and found that measures in place to keep children off the popular video-sharing platform and to prevent the collection and use of sensitive personal information for profiling and targeting purposes were inadequate (see page 16).

City of Richmond's Public Safety Camera System Field Test investigated the City of Richmond's use of ultra-high resolution surveillance cameras at a key intersection resulted in an order for the City to remove the cameras. The investigation determined FIPPA does not authorize the City to use the surveillance cameras to collect personal information for law enforcement purposes (see page 22).

Finally, *Privacy breaches following the Lapu Lapu Day Festival* revealed 71 snooping incidents by 36 healthcare workers following the Lapu Lapu Day tragedy, across three health authorities in BC (see page 26).

The strategies outlined remain relevant to the OIPC and have been maintained.

Strategies

- Secure government support for legislative and policy reforms that would restore British Columbia as a leader in privacy;
- Work with government to implement reforms, and educate and train public bodies and organizations;
- Promote OIPC's privacy management guidance documents and develop new resources; and
- Conduct audits and systemic investigations to ensure compliance with FIPPA and PIPA, including examining Privacy Management Programs.

Performance Measure		2025/26		26/27	27/28	28/29	29/30
		Target	Actual	Target	Target	Target	Target
1	Number of audits, special reports, compliance reviews and systemic investigations that uphold privacy rights and monitor protection of personal information	3	3	3	3	3	3
2	Number of new or revised guidance documents to raise awareness about privacy issues under FIPPA or PIPA	3	3	3	3	3	3

SERVICE PLAN GOAL 2

Promote and advocate for an open, accountable, and transparent public sector

This goal integrates the Commissioner's mandates to inform the public about relevant legislation and to comment on the implications for access to information of proposed legislative schemes, programs, or activities of public bodies.

OIPC case review officers and investigators handle many requests for review from people in BC. When processing requests for reviews, OIPC staff educate public bodies and organizations as appropriate to promote freedom of information rights and responsibilities and to promote transparency and accountability under FIPPA and PIPA.

Audit, special and investigation reports represent Commissioner-initiated audits and investigations into matters of broad public interest. They are a compliance and education tool for public bodies, organizations, and the people of BC in relation to access to information rights and responsibilities under PIPA and FIPPA. Performance measures for these reports and uptake of the corresponding recommendations are under Goal 1 when they relate to privacy, and Goal 2 when they relate to access to information.

The Commissioner published one report in 2025/26 relating to access to information. *The University of British Columbia's duty to assist* detailed how system delays, a backlog of overdue requests, and process errors led to UBC having the lowest rate of compliance with FIPPA time limits of any public body in 10 years of OIPC Duty to Assist audits, with a 90% failure rate of meeting response timelines (see page 18).

The OIPC also issued a new infographic and guidance document on *Requesting records of a deceased individual*, guidance on *Use of personal email accounts and messaging apps for public body business,* and *Guidance on FIPPA's FOI process*.

The strategies outlined remain relevant to the OIPC and have been maintained.

Strategies

- Increase the number of public bodies that have implemented effective open information programs;
- Promote open information through our education mandate, and by creating scalable guidance documents;
- Provide support to freedom of information experts/leaders in public bodies by holding a speaker's series on access and privacy;
- Secure government support for legislative and policy reforms that would restore British Columbia as a leader in access to information; and
- Monitor and comment on the quality and timeliness of public bodies' responses to access to information requests by assessing and reporting on the underlying causes for responses to access requests that are not on time in accordance with the timelines set out by FIPPA.

Performance Measure		2025/26		26/27	27/28	28/29	29/30
		Target	Actual	Target	Target	Target	Target
3	Number of audits, special reports, compliance reviews and systemic investigations that promote an open, accountable, and transparent public sector	2	1	2	2	2	2
4	Number of new or revised guidance documents to raise awareness of access issues under FIPPA	2	3	2	2	2	2

SERVICE PLAN GOAL 3

Promote information and privacy rights and obligations to public bodies, organizations, and individuals

Promoting awareness of information rights and privacy remains a key goal of our office. The OIPC will continue to support its education mandate through interviews and presentations, including speaking engagements, training, conferences, and other events.

Speaking engagements are an effective method of outreach to inform public bodies, organizations, and the public about FIPPA and PIPA. Performance Measure 5 shows that the OIPC completed 82 speaking engagements in 2025/26.

In 2025/26, the OIPC held eight consultation sessions across seven cities in BC to hear from people living in BC about what the OIPC's priorities should be over the next three years. The sessions included discussions between the Commissioner and participants on the need for trust and transparency in the access to information system, trusted innovation in a world of rapidly evolving technologies, and rights equity in exercising privacy and access rights.

The OIPC also expanded its social media presence with Bluesky, and a dedicated plan for educational content across social media platforms.

The goal of promoting information and privacy rights is mutually reinforcing of OIPC Goals 1 and 2. This goal also includes responding to media enquiries and promoting information and privacy rights through digital media. In 2025/26 the OIPC handled 73 media enquiries and continued to implement a digital media and accessibility strategy.

The OIPC recognized Right to Know Week, Data Privacy Day, and Privacy Awareness Week through social media campaigns highlighting key resources, and speaking events.

The strategies outlined remain relevant to the OIPC and have been maintained.

Strategies

- Meet the growing demand from public bodies and organizations for education and training in FIPPA and PIPA compliance by developing curricula and external resources so that public bodies and organizations can train their own employees;
- Facilitate public awareness of privacy and access rights by developing and implementing social media strategies for stimulating interest and discussion of individual information rights, and implement them with our other communications strategies; and
- Promote access and privacy issues in the public domain by responding to requests for media interviews and seeking out opportunities for public commentary.

Performance Measure	2025/26		26/27	27/28	28/29	29/30
	Target	Actual	Target	Target	Target	Target
5 Number of OIPC presentations	50	82	50	50	50	50

SERVICE PLAN GOAL 4

Enhance the quality and capacity of the OIPC's people, systems, processes and culture

During the 2025/26 fiscal year, the OIPC integrated a number of action items recommended by the office's Reconciliation, Equity, Accessibility, Diversity, Inclusion plus (READI+) team to support OIPC's people, systems, processes, and culture. The Commissioner and staff are committed to further developing an inclusive and healthy workplace focused on continuous staff learning and ensuring our services to the public are equitable and accessible for all.

In the past year, the READI+ team brought in training for all staff in the areas of accessibility, First Nations Data Sovereignty and neurodiversity in alignment with our READI+ action items. Additionally, OIPC staff received presentations on various topics such as neurotechnology and artificial intelligence throughout the year to expand our knowledge in the areas of privacy and access, and vicarious trauma to support a healthy workplace and culture.

In 2025/26, the OIPC established an Early Resolution Investigator to resolves matters that are more straight-forward to address. This means that those files that can be promptly resolved are addressed in early resolution, reducing the files waiting to be assigned to an investigator.

Through investigation and policy work the OIPC provides education to organizations and public bodies about their responsibilities under FIPPA and PIPA. This work assists public bodies and organizations with responding to and preventing contraventions. Greater familiarity with access and privacy law makes it easier for public bodies and organizations to engage with OIPC processes and to resolve matters that affect both them and individuals seeking to engage their access and privacy rights.

The strategies outlined remain relevant to the OIPC and have been maintained.

Strategies

- Ensure the timely resolution of complaints, reviews, and requests for information through ongoing review of internal processes and standards and developing best practice guidelines;
- Leverage relationships with functional counterparts at other oversight agencies;
- Create opportunities for skills, knowledge, and professional development for OIPC staff; and
- Promote a positive workplace culture, collaboration, and engagement among OIPC staff.

Performance Measure		2025/26		26/27	27/28	28/29	29/30
		Target	Actual	Target	Target	Target	Target
6	Percentage of requests for review settled without inquiry	90%	86%	90%	90%	90%	90%
7	Percentage of request for review files resolved within 90 business days of assignment	85%	88%	85%	85%	85%	85%
8	Percentage of complaint files resolved within 120 business days	90%	95%	90%	90%	90%	90%
9	Number of orders published per year	120	109	120	120	120	120

FINANCIAL REPORTING

Nature of operations

The Information and Privacy Commissioner is an independent Officer of the Legislature whose mandate is established under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). In addition, the Commissioner is the Registrar of Lobbyists and oversees and enforces the *Lobbyists Transparency Act.*

Funding for the operation of the Office of the Information and Privacy Commissioner is provided through a vote appropriation (Vote 6) of the Legislative Assembly. The vote provides separately for operating expenses and capital acquisitions, and all payments or recoveries are processed through the Province's Consolidated Revenue Fund.

The Office receives approval from the Legislative Assembly to spend funds through this appropriation. There are two components: operating and capital. Any unused appropriation cannot be carried forward for use in subsequent years.

The following table compares the Office's voted appropriations, total operating and capital aquisitions, and the total remaining unused appropriation (unaudited) for the current and previous fiscal years:

2025/26	Operating	Capital
Appropriation*	$11,773,250	$117,000
Total operating expenses	$11,542,020	-
Capital acquisitions	-	$91,040
Unused appropriation	$231,230	$25,960

**includes access of up to $840,250 in operating and $19,000 in capital contingencies*

2024/25	Operating	Capital
Appropriation**	$11,795,000	$105,000
Total operating expenses	$11,574,275	-
Capital acquisitions	-	$35,126
Unused appropriation	$220,725	$69,874

*** includes access of up to $784,000 in operating contingencies*

Tangible capital assets

Tangible capital assets are recorded at historical cost less accumulated depreciation. Depreciation begins when the asset is put into use and is recorded on the straight-line method over the estimated useful life of the asset.

The following table shows the Office's capital assets (unaudited).

2025/26	Closing cost	Closing accumulated amortization	Net book value (March 31, 2026)
Computer hardware and software	$1,055,044	($727,537)	$327,507
Tenant improvements	$0	$0	$0
Furniture and equipment	$11,324	($5,521)	$5,803
Total tangible capital assets	**$1,066,368**	**($733,058)**	**$333,310**

2024/25	Closing cost	Closing accumulated amortization	Net book value (March 31, 2025)
Computer hardware and software	$1,058,402	($721,950)	$336,452
Tenant improvements	$0	$0	$0
Furniture and equipment	$20,202	($12,270)	$7,931
Total tangible capital assets	**$1,078,604**	**($734,220)**	**$344,383**

Public Interest Disclosure Act

British Columbia's *Public Interest Disclosure Act* (PIDA) allows BC government ministry employees, employees of independent offices, like the OIPC and ORL, and the Legislative Assembly, as well as former public servants to report specific kinds of serious wrongdoing without fear of reprisal.

PIDA requires public bodies in British Columbia to report on investigations into wrongdoing started under the Act, the number of disclosures made internally, and the number of disclosures received by the Office of the Ombudsperson.

The Office of the Information and Privacy Commissioner and the Office of the Registrar of Lobbyists have not had any investigations or disclosures under PIDA between April 1, 2025 and March 31, 2026.

RESOURCES

Getting started

- Access to data for health research
- BC physician privacy toolkit
- Developing a privacy policy under PIPA
- Early notice and PIA procedures for public bodies
- Guide to OIPC processes (FIPPA and PIPA)
- Guide to OIPC audits, systemic investigations, and compliance reviews
- Guide to PIPA for business and organizations
- Privacy impact assessments for the private sector
- Privacy management program self-assessment

Access (General)

- Common or integrated programs or activities
- Guidance for conducting adequate search investigations (FIPPA)
- Guidance on FIPPA's FOI process
- How do I request records?
- Instructions for written inquiries
- PIPA and workplace drug and alcohol searches: a guide for organizations
- Proactive disclosure: guidance for public bodies
- Requesting records of a deceased individual
- Section 25: The duty to warn and disclose
- Time extension guidelines for public bodies
- Tip sheet: requesting records from a public body or private organization

Privacy (General)

- Direct-to-consumer genetic testing and privacy
- Disclosure of personal information of individuals in crisis
- Employee privacy rights
- Guide for organizations collecting personal information online
- Identity theft resources
- Information sharing agreements
- Obtaining meaningful consent
- Political campaign activity code of practice
- Political campaign activity guidance
- Privacy breach quick reference guide for small and medium-sized businesses
- Privacy guidelines for strata corporations and strata agents
- Privacy-proofing your retail business
- Privacy tips for seniors: protect your personal information
- Private sector landlord and tenants
- Protecting personal information away from the office
- Protecting personal information: cannabis transactions
- Public sector surveillance guidelines
- Reasonable security measures for personal information disclosures outside Canada
- Responding to PIPA privacy complaints
- Securing personal information: A self-assessment for public bodies and organizations

Comprehensive privacy management

- Accountable privacy management in BC's public sector
- Getting accountability right with a privacy management program

Privacy breaches

- Privacy breaches: tools and resources for public bodies
- Privacy breach checklist for private organizations
- Privacy breach checklist for public bodies
- Privacy breaches: tools and resources for the private sector

Technology and social media

- Guidance for the use of body-worn cameras by law enforcement authorities
- Guidelines for online consent
- Guidelines for conducting social media background checks
- Mobile devices: tips for security & privacy
- PIPA and AI scribes: best practices for healthcare organizations in BC
- Tips for public bodies and organizations setting up remote workspaces
- Use of personal email accounts and messaging apps for public body business

Infographics

- AI scribes and BC privacy law: obligations for organizations
- FIPPA and the application fee
- How to identify deceptive design patterns
- How to make a complaint
- How to make an access request
- How to request a review
- Identifying and mitigating harms from privacy-related deceptive design patterns
- Protect your privacy when using AI tools
- Responsible information sharing in situations involving intimate partner violence
- Requesting records of deceased individuals
- Talking to kids about online privacy
- Tips for requesting records
- Transparency by default: information regulators call for a new standard in government review
- Tip sheet: 10 tips for public bodies managing requests for records

oipc

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

PO Box 9038, Stn. Prov. Govt.
Victoria, BC V8W 9A4

Telephone: 250.387.5629
Toll-Free in BC: 1.800.663.7867

Email: info@oipc.bc.ca

oipc.bc.ca