

Office of the Information and Privacy Commissioner for  
British Columbia

# Annual Report and Service Plan

2024/25



**oipc**

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 territories of the Lekwungen people of the Songhees and Esquimalt 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 2025

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, 2024 to March 31, 2025.

Yours sincerely,

A handwritten signature in blue ink, appearing to read 'MH', enclosed in a light blue rectangular box.

**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

<b>Commissioner's message</b>	<b>6</b>
<b>Mandate, Vision, Who we serve</b>	<b>10</b>
<b>Our team</b>	<b>12</b>
<b>Year in review</b>	<b>14</b>
<b>Trust in trying times</b>	<b>16</b>
<b>When deception is the norm</b>	<b>18</b>
<b>Trust through transparency</b>	<b>20</b>
<b>Our journey towards accessibility, reconciliation, and inclusion</b>	<b>22</b>
<b>Legal updates</b>	<b>24</b>
<b>Highlights</b>	<b>26</b>
<b>Year in numbers</b>	<b>30</b>
<b>Adjudication</b>	<b>44</b>
<b>Service Plan</b>	<b>46</b>
<b>Financial reporting</b>	<b>56</b>
<b>Resources</b>	<b>58</b>

# 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 2024/25.

When I was appointed to this role in May 2024, I was honoured to join this office and to serve as part of this province's robust and enviable framework of independent oversight.

That appreciation for the transparency and accountability that oversight provides has only deepened over the period covered in this report.

During this time, we saw rising economic uncertainty, global alignment shifts, and increasing polarization in society, along with the continued expansion of artificial intelligence (AI) technologies. These are developments that jolt us out of complacency.

They demand responses. They require us to stand firm in defence of our shared values and fundamental rights to ensure our democracy remains strong and resilient. They call on us to find ways to not only survive these challenges, but to thrive in the face of them.

Our access and privacy rights are essential to that effort because they build trust.

***A robust and well functioning access to information system builds trust between public bodies and the people they serve.***

***It is our single strongest defence in the face of a bombardment of misinformation and disinformation and growing mistrust of institutions.***

***Likewise, in uncertain times, public bodies and businesses can build trust by taking a privacy first approach.***

However, trust is not earned through platitudes or principles on paper that aren't put into practice. It's about doing the work, even – or especially – during challenging



times and amid intense, competing demands.

### **Building trust one access request at a time**

Two of our investigation reports over this past year spoke to that theme.

In September, we released an investigation report that highlighted major failings in Vancouver Coastal Health Authority's duty to assist applicants under the *Freedom of Information and Protection of Privacy Act* (FIPPA). You can read more about the outcome of that investigation on page 16.

Our 2025 investigation report into the records disclosure practices of 160 municipalities across British Columbia also highlighted lost opportunities to build trust and strengthen democracy at the local level.

Among the report's findings were inconsistent approaches to records disclosures, a significant knowledge gap when it came to FIPPA's requirements, and a need to improve proactive disclosure. Details of that report can be found on page 20.

This report highlights that transparency under FIPPA is not just about freedom of

information requests, but about how public bodies can proactively make information available to the public.

Freedom of information will always be a critical backstop for transparency, but at a time when public bodies are under growing operational pressure, the sheer volume of information held is constantly on the rise, and resource issues are real and growing, we need to think more broadly.

Growing transparency, and thus trust, requires thinking about how to make information available from the moment that a statute, policy, or program is conceived.

This notion, of how to transform our public bodies so that they are inherently more transparent, is the theme of an important resolution that I agreed upon with my Federal, Provincial and Territorial colleagues this year – the idea of transparency by default.

### **Dignity and rights in the digital age**

This period also called on us to question outdated conceptions of privacy as being about what we want to "hide" from others.

# COMMISSIONER'S MESSAGE

That framing no longer works when we consider what it means to live in our digital society. Privacy today is about choosing what we share and expressing our individuality through those choices. We should be able to do so without being manipulated with the illusion of choice, or having to accept uses of our information we never could have foreseen, let alone agreed to.

This year's Global Privacy Enforcement Network (GPEN) Sweep showed just how far we need to go to achieve that ideal. Nearly all Canadian websites and apps had features of deceptive design, aimed at manipulating users into making choices that result in providing more information than necessary.

The OIPC and other Canadian regulators found many of these platforms targeted children with their deceptive tactics. More information about this work is on page 18.

AI brings a paradigm shift in privacy. AI applications require enormous amounts of data to train algorithms. How can this be squared with the privacy principle of

collecting and using the minimum amount of data for a specific purpose? Where is this data going to come from and what is the legal authorization for its collection and use?

In December, the Supreme Court of British Columbia upheld our order for the facial recognition company Clearview AI to cease its operations in BC and delete all of the thousands of images of British Columbians it scraped without anyone's consent. The Court ruling said that we do not exhaust our rights to privacy when we go online.

***As AI advances, we need to hold to that line. We need to recognize how much of our identities are comprised in our personal information and stand up for our rights to protect that information - our privacy - just as we would any of our other fundamental rights.***





In that spirit, I call on government to revisit our private sector privacy law, the *Personal Information Protection Act*, to ensure that it is fit for purpose to stand up for these rights in the age of AI.

It has been a remarkable first year in office. I look forward to working with public bodies, private organizations, and the people of British Columbia in the years ahead to strengthen our democratic institutions and protect individual rights. Trust earned through transparency, accountability, and respect for privacy is the foundation of this work and it is my privilege to serve in advancing it.

**Michael Harvey**  
*Information and Privacy Commissioner  
and Registrar of Lobbyists for BC*

# 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.

# VISION

**A community where access to information rights are understood and robustly exercised.**

**A community where privacy is valued, respected, and upheld in the public and private sectors.**

**A community where public agencies are open and accountable to the citizenry they serve.**

The Information and Privacy Commissioner is designated the Registrar of Lobbyists for the purposes of the *Lobbyists Transparency Act* (LTA). See <https://www.lobbyistsregistrar.bc.ca/reports/annual-reports/> for the 2024/25 Annual Report and Service Plan for the Office of the Registrar of Lobbyists.

# WHO WE SERVE

Under FIPPA and PIPA the OIPC serves:

1. the public;
2. the Legislative Assembly of British Columbia; and
3. organizations and public bodies.

## **A dedicated staff, committed to service**

Sixty-three people worked at the Office of the Information and Privacy Commissioner in 2024/25. They were supported by the Corporate Shared Services team responsible for providing finance, HR, IT, and facilities management to the office and 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 2024 PECSF campaign receiving two awards for highest employee participation and for highest average employee donation.

# 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.

## 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.

## 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.

## 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

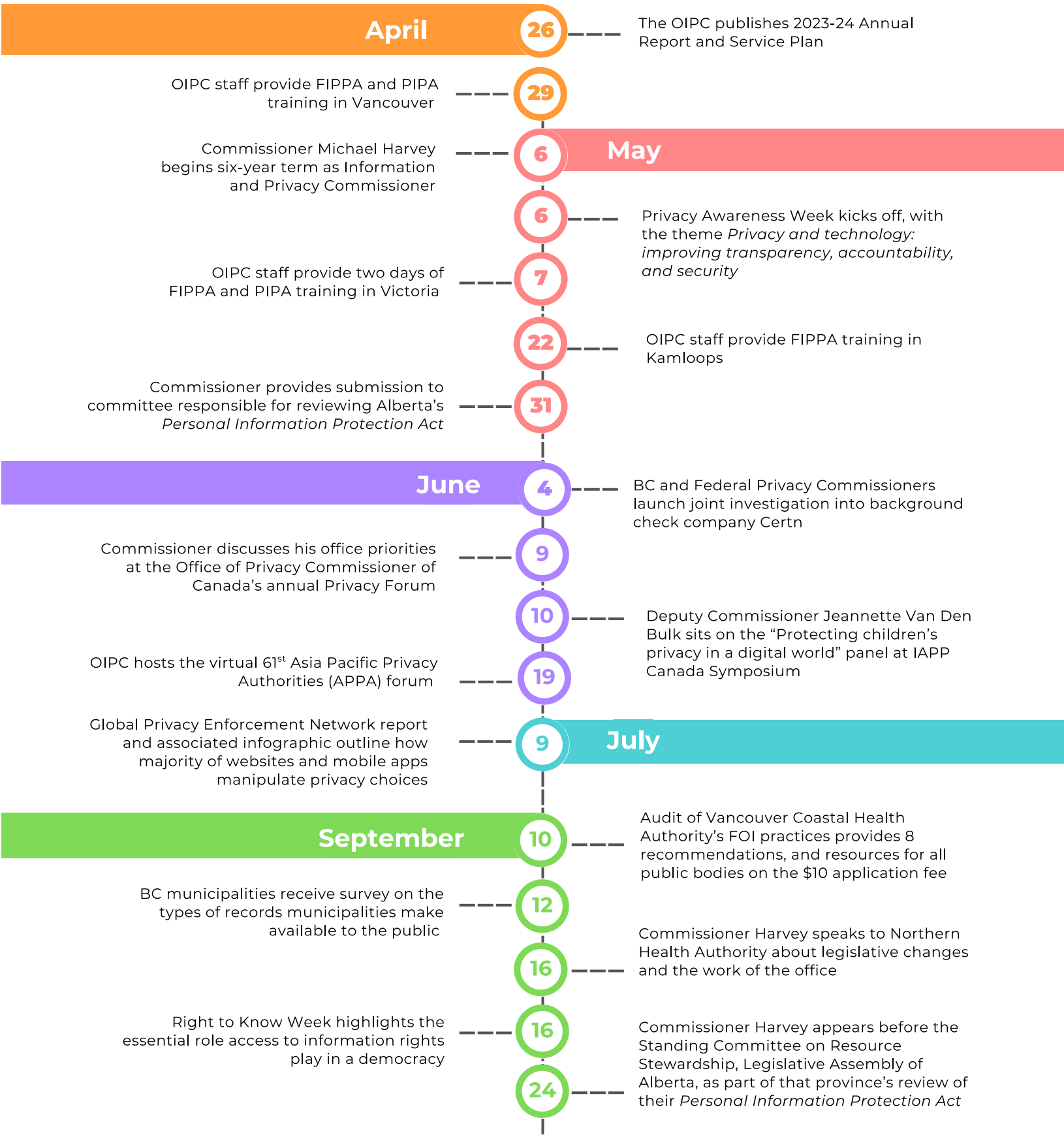
The audit and systemic review (AnSR) team performs audits, systemic reviews and investigations of information access and privacy compliance within public bodies and private sector organizations in relation to legislation, guidelines, and best practices. AnSR projects may be conducted jointly with other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



## October

10

Canadian privacy and access regulators meet in Toronto to address key issues, enhance collaboration among jurisdictions, and reaffirm a shared commitment to protecting the access and privacy rights of Canadians

Commissioner Harvey discusses genomics and privacy in a keynote at the 24<sup>th</sup> Annual Reboot Health Summit

29

Commissioner Harvey discusses artificial intelligence in a keynote at the Focused Education Resources IT4K12 Conference

5

## November

8

Commissioner Harvey and Deputy Twiss participate in numerous panels focused on privacy and access issues at the CBA Privacy and Access conference

Canadian privacy regulators issue joint resolution to address privacy-related harms resulting from deceptive design patterns

13

BC and ON Commissioners publish 2020 investigation report into the 2019 LifeLabs privacy breach, after Ontario Court of Appeal dismisses LifeLabs' bid to block public release of the report

25

Commissioner Harvey participates in 62<sup>nd</sup> APPA forum, hosted by the Personal Information Protection Commission of Japan

26

Canadian privacy regulators issue joint resolution to guide the responsible disclosure of personal information in situations involving intimate partner violence

27

## December

10

Canadian information regulators issue joint resolution calling for enhanced transparency in government operations

Commissioner Harvey talks about privacy and the Dark Web in keynote at Thompson Rivers University's Privacy and Access Conference

22

## January

28

Data Privacy Week celebrations challenge the myth that privacy is dead, as Commissioner Harvey joins fellow privacy regulators in a roundtable hosted by the OIPC Saskatchewan

## February

4

Investigation into how municipalities make records available to the public makes four recommendations to address a patchwork approach to records disclosure

Commissioner Harvey discusses principles of handling personal health information in keynote to Canadian Health Information Management Association

7

OIPC staff give training on Privacy Impact Assessments and an overview on the OIPC's processes and practices at the Victoria International Privacy and Security Summit (VIPSS)

11

## March

12

OIPC staff participate in panels on the ethical & responsible use of AI; Canadian law reform; and privacy, security and aging at VIPSS

Commissioner Harvey reinforces the importance of consent in a rights-based approach to privacy in keynote and discusses artificial intelligence on panel at VIPSS

12

26

Commissioner statement reminds 23andMe users of their personal information rights in light of the company's bankruptcy filing



# TRUST IN TRYING TIMES

## *Vancouver Coastal Health audit a reminder of why FOI matters*

In times of crisis, the public's trust in institutions is essential. But as Information and Privacy Commissioner Michael Harvey noted, in a democracy, trust is not a matter of faith. Rather it comes from the type of accountability and transparency that our access to information system provides.


As one of British Columbia's largest health authorities, Vancouver Coastal Health (VCH) understandably focused on its operational pandemic response and in providing core health services during the COVID-19 pandemic. However, an OIPC audit found that VCH failed to carry out this work in the transparent and accountable manner that the public expects and that is the law in this province.

*Vancouver Coastal Health Authority's duty to assist, April 1, 2020 to March 31, 2023*, showed a transformation at VCH that is instructive for all public bodies, from struggling to fulfill the bare minimum of requirements under the *Freedom of Information and Protection of Privacy Act* (FIPPA), to instituting an organization-wide culture change that puts a priority on transparency.

During the period examined, VCH responded to less than one-quarter of requests within FIPPA's 30-day benchmark, and in one-third of cases, did not even provide written acknowledgement that they had received the requests.

The report highlighted several additional areas where VCH failed to comply with FIPPA, including not conducting thorough searches for records, improper timeline extensions, and a failure to document requests.





Application fees were another barrier, with VCH initially offering limited payment options, failing to notify applicants promptly of the need to pay the fee, and mistakenly putting response timelines on hold until fees were paid. VCH was particularly unresponsive to the media during this period – taking an average of 165 days to respond, peaking at 171 days in 2021/2022.

**“Trust will always be essential in our health system – people access these services often when they are at their most vulnerable,” said Commissioner Harvey.**

**“VCH’s core business, as a public health authority, is not just the provision of health services but rather the transparent and accountable provision of health services. De-prioritizing freedom of information is harmful to its core business, just as it would be for any public body.”**

VCH made considerable efforts to improve its FOI practices since the audit was initiated, including ensuring more resources are in place to respond to FOI requests, improved reporting relationships, and new file and document management systems.

The report offers important lessons for all public bodies on the need to prioritize and properly resource the FOI function to ensure they meet their own obligations under the *Freedom of Information and Protection of Privacy Act*.

Eight recommendations cover the need for improved staff training on their obligations under FIPPA and how to apply the act, expanded and more accessible proactive disclosure, better tracking and management of FOI requests, and further internal evaluation to ensure requests are responded to within legislated time limits.

“I hope that readers of this report take away two stories. The first is the story of how, in the face of an unprecedented crisis a public body might be tempted to retreat from transparency and accountability,” said Harvey.

“But the second story is how VCH presents an example of an organization that has learned that becoming less transparent is harmful to the core business – both in the immediate term and in the long run – and decided to drive cultural change throughout the organization.”

### **Download:**

[Audit Report 24-02: Vancouver Coastal Health Authority's duty to assist, April 1, 2020, to March 31, 2023](#)

[News release, video on the report, and overview fact sheet](#)

# WHEN DECEPTION IS THE NORM

## *Global Privacy Enforcement Network Sweep raises alarm on deceptive design patterns*

Online deceptive design patterns take many forms, from complex privacy policies indecipherable to most users, to manipulative interfaces that steer users away from making choices in their own best interests, often at the expense of their privacy.

A study by the Global Privacy Enforcement Network (GPEN) found that these patterns were, by far, the norm, not the exception, on websites and in apps around the world.

The OIPC was among the 26 GPEN member privacy authorities that took part in the network's annual "sweep" – a coordinated international review of privacy practices. As part of its most recent sweep, members examined more than 1,000 websites and mobile applications to identify deceptive design patterns.

The GPEN Sweep report, published in July 2024, found that nearly all of these websites used at least one deceptive design pattern. Sweepers assessed websites using five indicators of deceptive design patterns identified by the Organisation for Economic Co-operation and Development (OECD).

The Office of the Information and Privacy Commissioner for British Columbia, the Office of the Information and Privacy Commissioner for Alberta, and the Office of the Privacy Commissioner of Canada focused their sweep on websites and apps aimed at children.

Michael Harvey, Information and Privacy Commissioner for BC, said that the results of this focused aspect of the sweep were particularly troubling. The regulators not only found a higher incidence of deceptive design

## Canadian Findings

- **Complex and confusing language:** More than 89% of privacy policies were found to be long or use complex language suited for those with a university education.
- **Interface interference:** When asking users to make privacy choices, 42% of websites and apps swept used emotionally charged language to influence user decisions – for example, “No thanks, I’m not into savings,” while 57% made the least privacy protective option the most obvious and easiest for users to select.
- **Nagging:** 35% of websites and apps repeatedly asked users to reconsider their intention to delete their account.
- **Obstruction:** In nearly 40% of cases, sweepers faced obstacles in making privacy choices or accessing privacy information, such as trying to find privacy settings or delete their account.
- **Forced action:** 9% of websites and apps forced users to disclose more personal information when trying to delete their account than they had to provide when they opened it.

patterns in Canada than elsewhere in the world, but that children were often the targets. More than half of the websites presented children with options that encouraged them to input more personal information than necessary – for example by making the option to sign up to a service more prominent than to continue without an account, as well as charged language to dissuade them from choosing more privacy protective options.

“Our children are particularly vulnerable to overcollection of their personal information online,” said Commissioner Harvey. “These websites are deceiving and manipulating our kids into revealing their private information - so that they can use it to further deceive and manipulate them,” he said. “These are real harms to our children and when a child is harmed, so are we all. We call upon websites and apps to end these practices and limit the collection and use of our kids’ personal information.”

Commissioner Harvey and other regulators urged parents and guardians to talk to their

children about the information they share online, how to customize privacy settings, and how to spot deceptive patterns online. The OIPC released an infographic to help them do so.

Recommendations in the report focused on steps organizations can take to design platforms in a way that supports users making informed privacy choices.

GPEN noted that by “offering users online experiences that are free from influence, manipulation, and coercion, organizations can build user trust and make privacy a competitive advantage.”

### Download:

[Deceptive Design Patterns – Report](#)

[Use of Deceptive Design Patterns on Websites and Apps that Appear to be Aimed at Children - Report](#)

[How to identify dark patterns – Infographic](#)

# TRUST THROUGH TRANSPARENCY

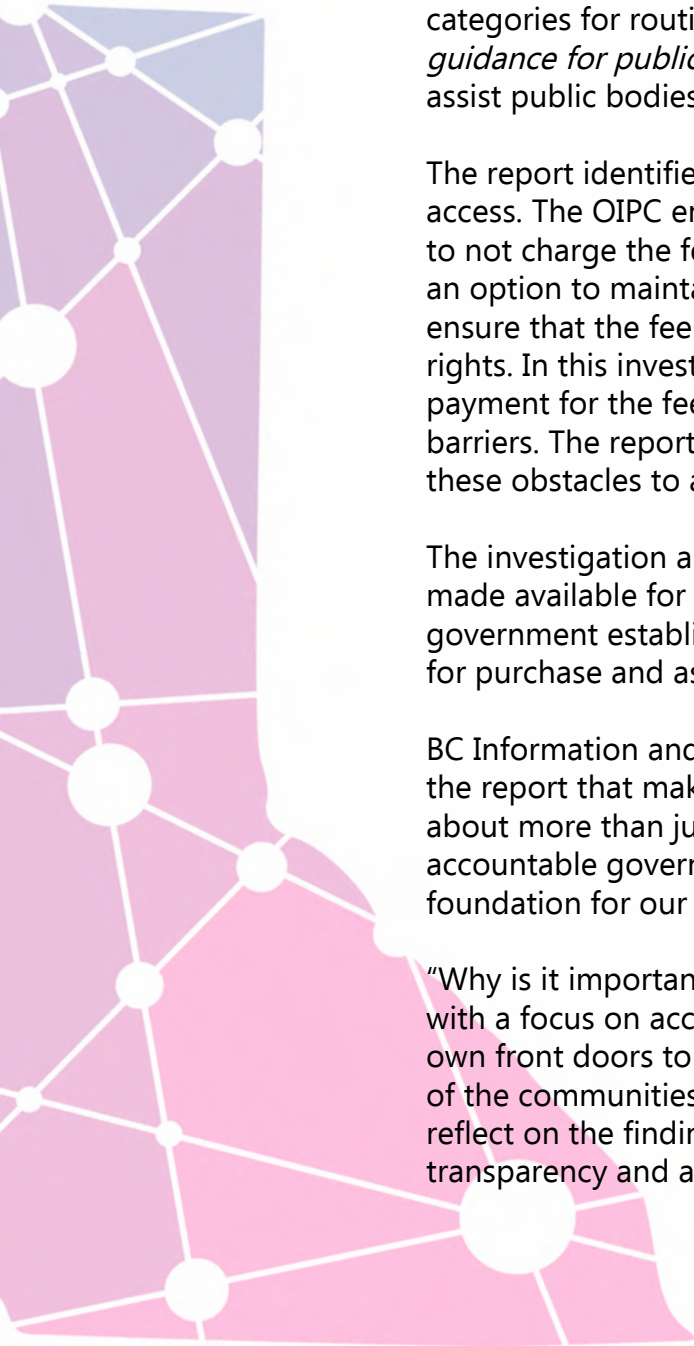
*An OIPC investigation found a patchwork of inconsistent municipal records disclosure practices and other barriers to access to information in municipalities across BC*

Municipal records contain the stories of our shared civic lives – the decisions that impact us, literally, right where we live. When people can access these records in a transparent and equitable manner, they are better able to participate in our democracy. Trust is built through transparency, and municipalities have an opportunity to foster that trust, one access request at a time.

An OIPC investigation report released in February 2025 found that people looking for records in municipalities across British Columbia must navigate a patchwork of inconsistent approaches to records releases and face additional barriers to access.

The report, *Municipal disclosure of records*, focused on three main methods of records disclosure: freedom of information (FOI) processes, proactive disclosure, and records made available for purchase. The OIPC gathered data for the investigation through a survey and received responses from 97% of BC's 160 municipalities.

The report revealed a disconnect around the proactive disclosure of records, a pillar of a transparent and well functioning FOI system. While all municipalities make some records available for proactive disclosure, nearly a quarter of those surveyed reported that they did not have a proactive disclosure program. By not recognizing or formalizing proactive disclosure, these municipalities might not be fulfilling a key function of FIPPA by making records routinely available. The result is that applicants may be left to file FOI requests, pay a \$10 application fee, and wait up to 30 business days or longer for records that should be freely available on demand.



The report included recommendations that municipalities invest in staff training on routine disclosure and FOI processes and publish meaningful categories for routine disclosure. The OIPC released *Proactive disclosure: guidance for public bodies*, around the time of the report's release, to assist public bodies in improving their proactive disclosure programs.

The report identified the application fee itself as a potential barrier to access. The OIPC encourages public bodies to exercise their discretion to not charge the fee by accepting multiple forms of payment, including an option to maintain applicant anonymity and urges those that do to ensure that the fee does not pose additional barriers to applicants' access rights. In this investigation, 12 of the municipalities surveyed only accepted payment for the fee by mail or in person, creating potential accessibility barriers. The report recommended that municipalities review and address these obstacles to access.

The investigation also found inconsistencies around which records can be made available for purchase. The report recommended that the provincial government establish clear criteria on which records should be provided for purchase and associated costs.

BC Information and Privacy Commissioner Michael Harvey wrote in the report that making municipal records as accessible as possible is about more than just an administrative checkbox; it's about transparent, accountable government and, ultimately, the trust that serves as the foundation for our democracy.

"Why is it important that municipalities rethink their records practices, with a focus on accessibility and transparency? We need only look out our own front doors to answer that question. Municipal records tell the stories of the communities around us," he wrote. "I encourage municipalities to reflect on the findings of this report to strengthen their commitment to transparency and accountability as they carry out their vital work."

### Download:

[Investigation Report 25-01: \*Municipal Disclosure of Records\*](#)

[\*Proactive disclosure: guidance for public bodies\*](#)

[Video and overview sheet](#)

# OUR JOURNEY TOWARDS ACCESSIBILITY, RECONCILIATION, AND INCLUSION

*A special report outlined the OIPC's work to align our services and workplace with our core values and vision*

"How can we make our services more accessible? How can the work we do better reflect and speak to the diversity of people in this province? How are we contributing to reconciliation with Indigenous peoples?"

BC Information and Privacy Commissioner Michael Harvey posed these questions in the introduction to the special report, *Accessibility, reconciliation, and inclusion at BC's Office of the Information and Privacy Commissioner and Office of the Registrar of Lobbyists*, published in September 2024.

Each question invites a conversation, and the report provided both a framework for that discussion and a public statement on the central importance of these considerations to the office's values and vision.

The report tells the story of the OIPC's ongoing journey towards embracing and embedding these values in our workplace and in the services we provide to the public. That journey began in a structured way in 2019, when the office's READI+ (Reconciliation, Equity, Accessibility, Diversity and Inclusion+) group was formed.

Since 2019, the READI+ group has led several initiatives, including making our office more accessible, launching language interpretation services, training staff on



Indigenous cultural safety, and updating communications with gender-inclusive language.

The report builds on that work with 38 specific action points with timelines for implementation across three areas: accessibility, reconciliation, and diversity, equity, & inclusion.

Under the accessibility umbrella, the report meets the requirements of the *Accessible BC Act* for the OIPC to report publicly on how the office plans to identify, remove, and prevent barriers to access for people. Plans include ongoing efforts to ensure that the office's communications are as accessible as possible – including through updates to our website, plain language writing for public-facing documents, and providing content in a variety of mediums.

The office will also make physical accessibility improvements to lighting, signage, and washrooms, as well as educate staff on and provide support related to mental health and neurodivergence.

The office's reconciliation strategy takes a "listening and learning first" approach to building relationships with Indigenous peoples in BC. That means ongoing efforts to deepen relationships with and learn from Indigenous people about their experiences and legal traditions, including data sovereignty principles, identifying and removing barriers to our services, and making sure that we are providing culturally safe services.

The diversity, equity & inclusion strategy aims to advance the office's vision of a workplace that celebrates and reflects British Columbia's diverse identities, cultures and perspectives, and that is responsive to all the communities we serve. Key initiatives under this umbrella include expanding translation services, developing inclusive hiring and meeting practices, using gender-inclusive language in communications, and ongoing education and support for staff.

The OIPC launched an Accessibility, Reconciliation, and Inclusion Feedback form on the office website along with the report to encourage public feedback on the areas covered as well as general thoughts and suggestions.

Annual reports will continue to include updates on our progress towards achieving the priorities and action items outlined in this report. As Commissioner Harvey noted, the report itself is intended to be "a living document that we will update based on feedback and consultations."

### Download:

[\*Accessibility, reconciliation, and inclusion at BC's Office of the Information and Privacy Commissioner and Office of the Registrar of Lobbyists\*](#)

[Accessibility, Reconciliation and Feedback form](#)

# LEGAL UPDATES

*LifeLabs and Clearview AI rulings bolster transparency, strengthen privacy protections*

Two important court rulings upheld the OIPC's authority to call organizations to account to ensure public accountability and transparency after a privacy breach, and to protect people's fundamental right to privacy as new technologies continue to test boundaries.

## **LifeLabs ([LifeLabs LP v. Information and Privacy Commr. \[Ontario\], 2024 ONSC 2194](#))**

A ruling from Ontario's Court of Appeal in November 2024 marked the end of what BC Information and Privacy Commissioner Michael Harvey called a "long road to accountability and transparency" for victims of the 2019 data breach at LifeLabs, Canada's largest provider of laboratory testing services.

The ruling allowed for the publication of a joint investigation report by the OIPC BC and the Information and Privacy Commissioner of Ontario into the breach in which cyber-attackers accessed the personal health information of millions of Canadians, including an estimated 1.3 million from British Columbia.

The investigation examined the impact of the breach, LifeLabs' security measures and response, as well as what the company and other organizations could do to prevent similar breaches.

The report was scheduled for publication in 2020; however, despite implementing all orders and recommendations contained in the report, LifeLabs argued that the report should not be published as it contained information protected by solicitor-client privilege, and contested its publication at multiple levels of Ontario's courts for four years

The November 2024 ruling rejected the company's claim, saying that privilege could not be used to shield facts about privacy breaches from public view.

Following the decision and publication of the report, Commissioner Harvey noted the importance of the decision for public transparency and accountability – particularly in an area as sensitive as personal health information. "I'm pleased with this ruling that affirms overly broad claims of privilege cannot be used to obstruct the vital role of our offices in ensuring public accountability, transparency, and education," he said.



## **Clearview AI (Clearview AI Inc. v. Information and Privacy Commissioner for B.C., 2024 BCSC 2311)**

While public spaces have been redefined in the digital age, our privacy rights are still as applicable when we're online as they are when we're walking down a public street.

A BC Supreme Court ruling in December 2024 affirmed this principle when it rejected Clearview AI's petition against an OIPC order. In 2021, the OIPC and its counterparts in Quebec, Alberta and the federal Office of the Privacy Commissioner found in a joint investigation that the US-based facial recognition company scraped billions of images from people's social media accounts and other online sources to train its facial recognition tool. Millions of these images came from Canadians, many of them children, and all were obtained without consent.

The OIPC ordered Clearview to comply with recommendations in the report and stop offering its facial recognition services in BC; to cease its collection, use, and disclosure of personal information of individuals in BC without their consent; and to delete the information they had already collected of those people.

Clearview contested the order, arguing that BC's *Personal Information Protection Act* (PIPA) didn't apply as the organization had no physical presence in BC, the images were from publicly available sources, and it wasn't feasible to delete the images and biometric information.

The BC Supreme Court rejected each of these assertions. The ruling helped establish guardrails around people's personal information in the digital world by affirming the central importance of consent and the principle that even in this context, we have a

right to control our personal information.

That right is established in PIPA in the private sector and, the ruling noted, the law applies to all companies processing the information of people living in BC – not just those with a physical presence.

The ruling also rejected Clearview's contention that it would be "impossible" to implement the order. The Court found that this was a problem of Clearview's own making and challenges fixing it do not exempt the company from following the law.

Clearview has filed an appeal of the ruling with the BC Court of Appeal. The privacy commissioners of Alberta and Quebec are also facing similar court challenges to their orders by Clearview.

Commissioner Harvey said the ruling was an important early milestone in how emerging technologies, such as artificial intelligence, impact our basic rights. "We're establishing frameworks and guardrails now – through the order and jurisprudence around Clearview for example – for what's acceptable under our privacy laws that will guide the development of the society-changing transformation."

### **DOWNLOAD**

[Joint investigation into LifeLabs data breach](#)

[Report of Findings: 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](#)

[Order P21-08 – Clearview AI](#)

# HIGHLIGHTS

## **Order finds strata's collection and use of personal information contravened PIPA**

While strata corporations are authorized to collect unit owners' personal information under certain circumstances, the *Personal Information Protection Act* (PIPA) limits that collection for purposes a reasonable person would consider appropriate in the circumstances. This was put to the test when the owner of a strata unit complained to the OIPC that the strata corporation violated PIPA when collecting their personal information to verify the unit was their permanent residence, as part of an application to use the unit as a short-term rental.

Collected personal information included identification documents, and forms completed by building staff and an email from an individual outlining their observations about occupancy of the unit. The strata corporation argued the collection was appropriate because it was used for the purpose of ensuring strata units were not used illegally. The adjudicator concluded the strata corporation was not authorized under PIPA to collect and use the unit owner's personal information because its purposes were inappropriate in these circumstances. In particular, the adjudicator determined that the strata corporation knew it was the City's role on licensing short-term rentals to verify principal residence, so the strata corporation's collection and use for this purpose was unnecessarily intrusive on the privacy rights of the complainant. The adjudicator required the strata corporation to stop collecting and using the owner's personal information.

**Download: Order P25-01**

## **Commissioners launch joint investigation of Certn, the landlord background check company**

In British Columbia, PIPA considers the privacy rights of individuals and the needs of organizations to collect, use, and disclose personal information to run their businesses. This is particularly important in the rental market, where hundreds of thousands of people in British Columbia face affordability and housing challenges. Together with the privacy commissioners of Canada and Alberta, the OIPC launched a joint investigation into Certn, a Victoria-based company that completes background checks for landlords across Canada.

The three offices are examining the company's practices with respect to tenant screening to determine if they are compliant with the consent provisions under the privacy laws of their respective jurisdictions. The investigation will also assess whether Certn ensures that the information that it collects, uses, and discloses for the purposes of tenant screening is sufficiently accurate, complete, and up to date; and whether the purposes for which it collects that information are appropriate. The outcome of the investigation will be published on the OIPC website when available.

## Cross-Canada collaboration brings unified voice to access and privacy challenges

Cross-Canada collaboration was more robust than ever this fiscal as the OIPC joined its Federal, Provincial and Territorial (FPT) counterparts in issuing three joint resolutions on critical privacy and access challenges facing the country.

In October, FPT privacy regulators passed two resolutions on privacy at their annual meeting, hosted by the Information and Privacy Commissioner of Ontario.

The first called on organizations to adopt privacy-first design practices to respond to the overwhelming use of deceptive design practices in the online world. The resolution stemmed from the results of the 2024 Global Privacy Enforcement Network (GPEN) sweep that found deceptive design patterns – patterns that manipulate users into making choices that compromise privacy rights – on most websites and apps, including 99% of Canadian digital platforms.

Information and Privacy Commissioner Michael Harvey noted the dangers these patterns posed, particularly when targeting young people. “Our resolution calls on all of us to push back – to refuse to accept deceptive design patterns as ‘business as usual,’” he said.

The second resolution responded to an urgent need to dispel a harmful myth about

privacy: that it can be a barrier to providing victims of intimate partner violence (IPV) with the help they need. With 123,319 IPV incidents reported to police in 2023, privacy authorities noted the urgency of stating in a unified and emphatic voice that privacy laws permit the disclosure of personal information when there is a serious risk to a person’s health or safety. The aim of the resolution was to provide clarity for professionals across sectors and empower them to act decisively when they need to share to help people facing IPV.

In December, Canada’s information commissioners and ombudspersons issued a third resolution that called on their respective governments to prioritize transparency when designing and implementing new systems, administrative processes, procedures, and governance models. They also stressed the importance of transparency as a defence against a rising tide of misinformation and disinformation, to strengthen trust with citizens.

“Transparency is the foundation of trust and trust must be earned,” said Commissioner Harvey. “Transparency must not be an afterthought – it is the core business of a democratic government.”

### DOWNLOAD

[\*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 participates in review of Alberta's PIPA

BC's PIPA and Alberta's PIPA both hold substantially similar status with the federal privacy legislation when it comes to oversight of the private sector – with Quebec being the only other province with its own private sector legislation. So when Alberta underwent a statutory review process for their private sector Act in 2024, Commissioner Harvey was uniquely positioned to provide valuable insight on recommendations to Alberta's PIPA based on BC's provincial context and the flow of data across provincial borders.

Commissioner Harvey highlighted for the Standing Committee five key recommendations from the most recent statutory review of BC PIPA in 2020/2021, and recommended that political parties and non-profit organizations be included in Alberta's PIPA, as they are in BC's PIPA. In written and oral presentations, Commissioner Harvey stressed that all organizations collecting, using, and disclosing personal information need to be regulated to ensure a trusted system of privacy protection. He also recommended that Alberta provide specific protection for children's personal information, noting the vulnerability of young people in today's digital realm.

**Download: [Speech to the Standing Committee on Resource Stewardship, Legislative Assembly of Alberta](#)**

## Order provides clarity on “business of the public body” under FIPPA

As part of the amendments to the *Freedom of Information and Protection of Privacy Act* (FIPPA) in 2021, section 3(5)(b) was added, providing that Part 2 of the Act does not apply to “a record that does not relate to the business of the public body.” If s. 3(5)(b) applies, an applicant has no right of access to the record under FIPPA. Order F24-40 provides clarity on what the phrase “the business of the public body” means and when it can be relied upon by public bodies. An applicant requested an agreement involving Tsal'álh (formerly Seton Lake Indian Band) and the local passenger rail service, which BC Rail Company refused citing various provisions under FIPPA.

During the inquiry, the adjudicator interpreted s. 3(5)(b) and said it applies to records that relate to a public body's past and present mandate, purpose, transactions, operations, programs, policies, procedures, decisions or obligations. It does not apply to records related to personal matters. The adjudicator found that s. 3(5)(b) did not apply to the agreement, so the applicant had a right of access to it subject to any FIPPA exceptions to disclosure the company applied. Ultimately, the adjudicator concluded the company was authorized to refuse to disclose the agreement to the applicant under s. 17(1) (disclosure harmful to financial or economic interests) and it was not required to disclose any information in the agreement under s. 25(1)(b) (disclosure clearly in the public interest).

**Download: [Order F24-40](#)**

## **OIPC BC concludes successful eight-year term as APPA Secretariat**

In June 2024, the Office of the Information and Privacy Commissioner (OIPC) for BC concluded its role as Secretariat of the Asia Pacific Privacy Authorities (APPA) Forum. The OIPC took on the role in 2016 and, in the eight years that followed, oversaw 17 Forums and hosted two of its own. The Personal Data Protection Commission of Singapore has now taken on the position of APPA Secretariat.

The OIPC proudly played a leading role in the regional network during a time when the urgency of its mandate grew more pressing with each passing year. This period saw profound challenges to privacy protections: the proliferation of social media platforms collecting vast amounts of user data; advances in facial recognition technologies; the challenges posed by the shift to digital during the COVID-19 pandemic; and, most recently, the rapid emergence of artificial intelligence systems. The ultimate objective is to enhance the protection of British Columbia's personal information.

The APPA Forum helps address these challenges, which cannot be contained within national borders, through information sharing and regional cooperation. Countries in the Pacific Rim are some of Canada's most important partners for trade and investment and how personal information is regulated in different countries is increasingly vital to these relationships in the rapidly developing Information Economy.

The OIPC remains an active participant in the organization.

# YEAR IN NUMBERS

Summary of FIPPA and PIPA files received in 2024/25				
	Received 24/25	Closed 24/25	Received 23/24	Closed 23/24
<b>Privacy breach notification</b>				
FIPPA	208	215	213	208
PIPA	210	200	198	198
<b>Privacy complaints</b>	456	521	361	378
<b>Access complaints</b>	448	490	417	440
<b>Requests for review</b>				
Requests for review of decisions to withhold information (RR and 3rd party RR)	755	902	668	573
Deemed refusal	348	353	264	265
<b>Applications to disregard requests as frivolous or vexatious</b>	26	23	20	23
<b>Time extensions</b>				
Requests by public bodies and organizations (incl. s. 10 FIPPA and s. 31 PIPA)	2626	2626	2548	2544
Requests by applicants seeking a review (incl. s. 53 FIPPA and s. 47 PIPA)	11	13	42	42
<b>Public interest disclosure notification (s. 25)</b>	10	10	9	10
<b>Requests for reconsideration of OIPC decisions</b>	81	105	66	65
<b>Information requests/received</b>				
Requests for information	4111	4112	4395	4393
Non-jurisdictional issue	19	20	10	10
Request for contact information (research)	2	3	5	2
<b>Media enquiries</b>	70	73	86	86
<b>FOI requests for OIPC records</b>	30	28	13	14
s. 60 adjudication of OIPC decisions	3	3	2	2
<b>Commissioner-initiated reports</b>				
Privacy reports	n/a	1	n/a	3
Access reports	n/a	2	n/a	1
<b>Policy</b>				
Policy or issue consultation	161	150	252	243
Legislative reviews	21	20	18	20
Police Act IIO reports	53	52	37	37
Privacy impact assessments	55	54	46	46
Indirect collection	2	2	1	1
<b>Public education and outreach</b>				
Speaking engagements	54	50	70	83
Meetings with public bodies and private organizations	11	11	14	11
<b>Other (includes all file types except those otherwise listed)</b>	50	50	90	94
<b>TOTAL</b>	<b>9,821</b>	<b>10,089</b>	<b>9,844</b>	<b>9,791</b>



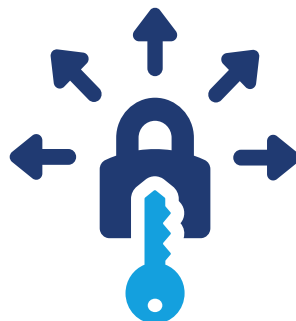
## The OIPC has the authority to process and investigate request for reviews, privacy complaints, and access complaints.\*



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.



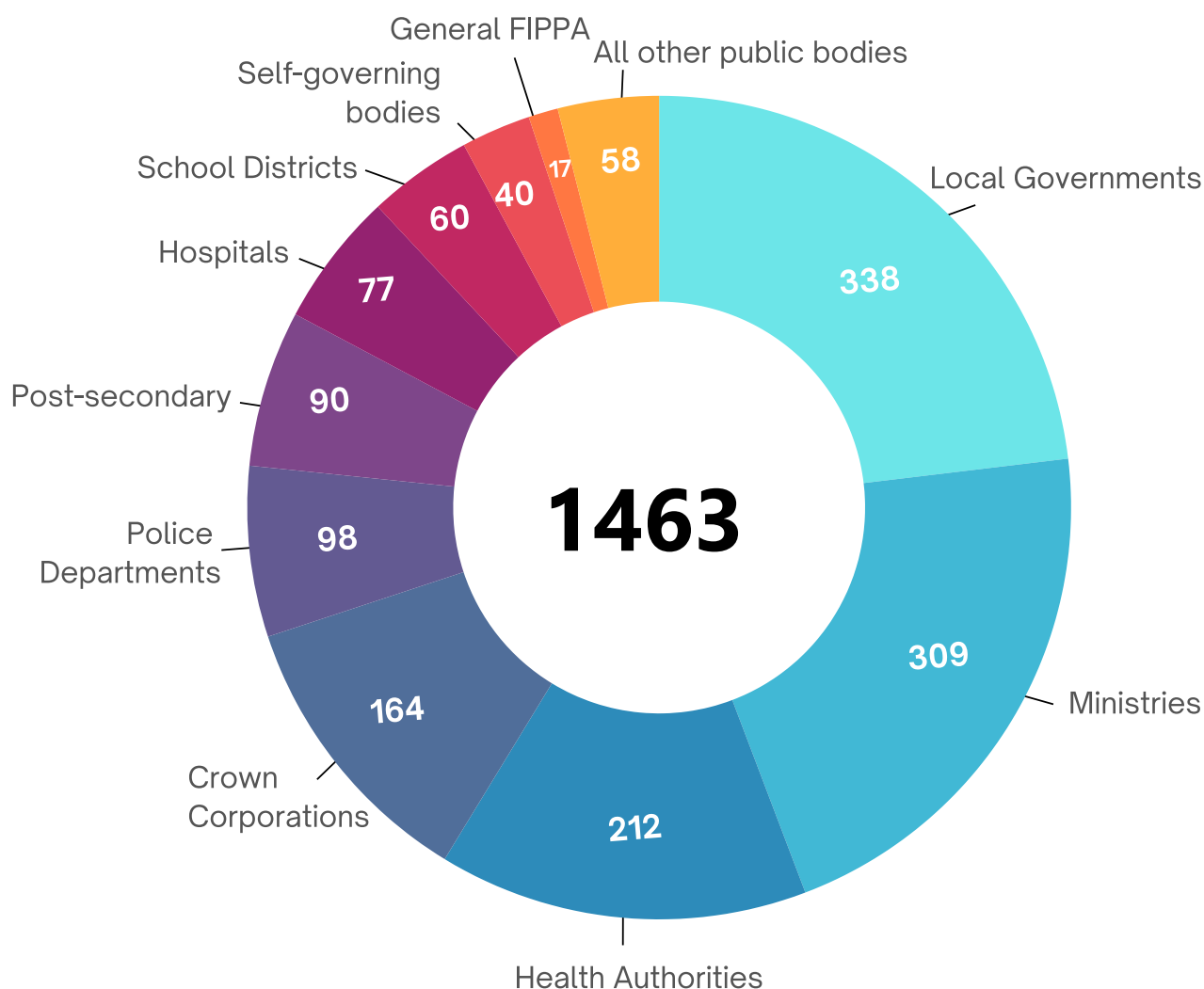
An **access complaint** can be made if there are concerns about how a public body or organization processed an access request.

\*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 2024/25.**

# YEAR IN NUMBERS

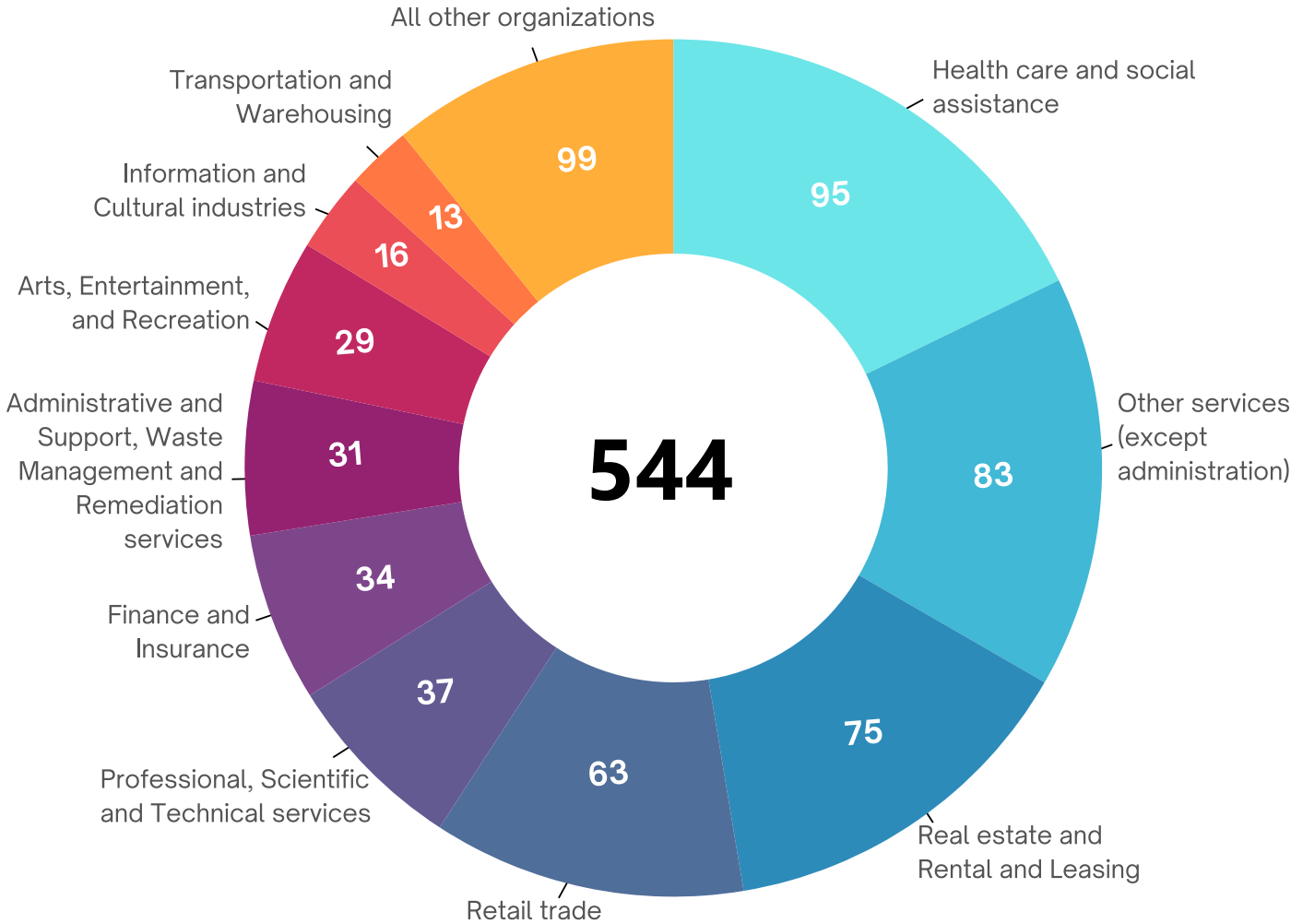
The OIPC reports out on the proportion of **FIPPA complaints and requests for review received by public body type** in the fiscal year. This breakdown does not indicate whether the outcome was in favour of the public body or the individual.





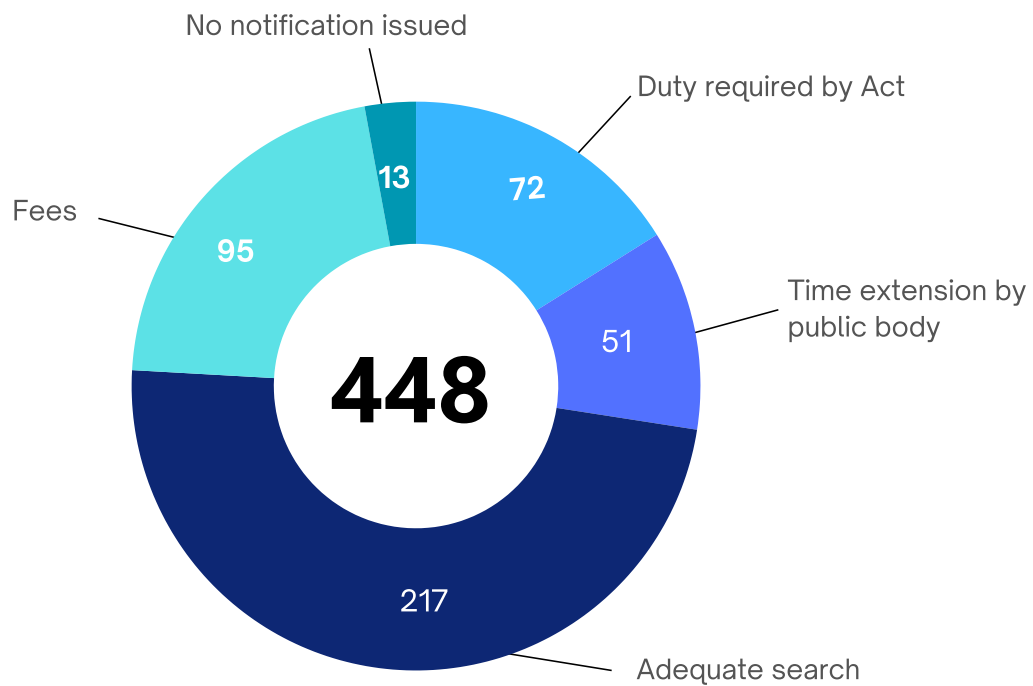


The OIPC reports out on **PIPA complaints and requests for review by sector** in the fiscal year. Inclusion in this list does not indicate whether the outcome was in favour of the organization or the individual.



# YEAR IN NUMBERS

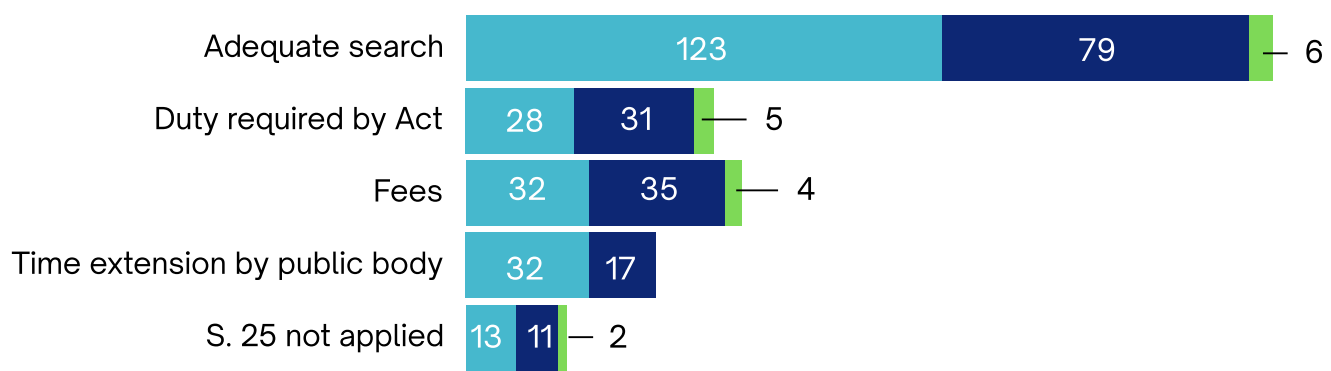
The OIPC received **448 access complaints** in 2024/25. The breakdown of the types of complaints for both FIPPA and PIPA is:



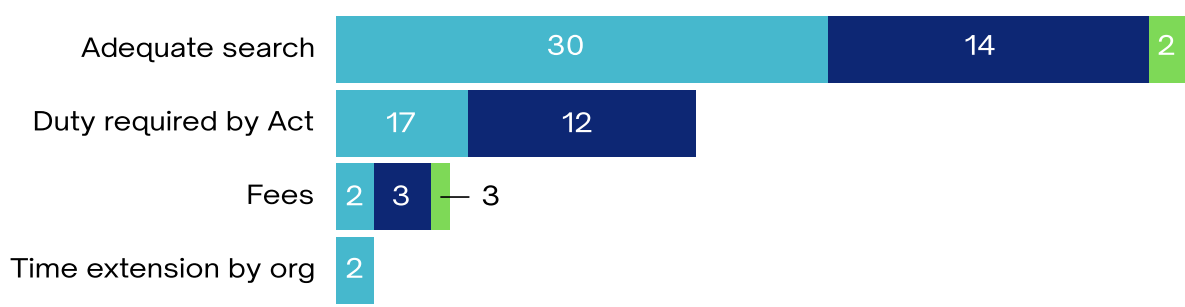
- Duty required by Act**  
Failure to fulfill any duty required by FIPPA (other than an adequate search)
- Time extension by public body**  
Unauthorized time extension taken by public body
- Adequate search**  
Failure to conduct adequate search for records
- Fees**  
Unauthorized or excessive processing fees assessed by public body
- No notification issued**  
Failure to notify as required under s. 25 of FIPPA



The OIPC resolved **418 FIPPA access complaints** in 2024/25. A complaint can ultimately result in an investigation, no investigation, or an inquiry. In 2024/25, 228 investigations were conducted on access complaints, 173 complaints resulted in no investigation, and 17 files proceeded to inquiry.



The OIPC resolved **72 PIPA access complaints** in 2024/25. A complaint can ultimately result in an investigation, no investigation, or an inquiry. In 2024/25, 37 investigations were conducted on access complaints, 32 complaints resulted in no investigation, and three files proceeded to inquiry.



**Investigation**

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

**No investigation**

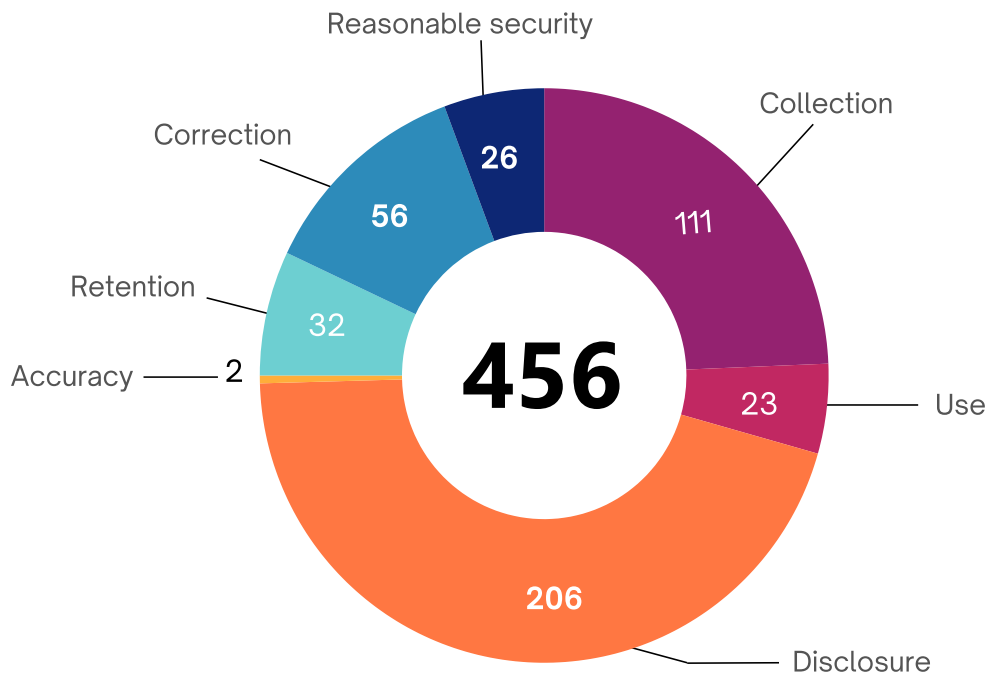
Files with no jurisdiction, no reviewable issue, or files in which the OIPC referred the complainant back to the public body or declined/continued an investigation

**Inquiry**

Files that proceeded to inquiry

# YEAR IN NUMBERS

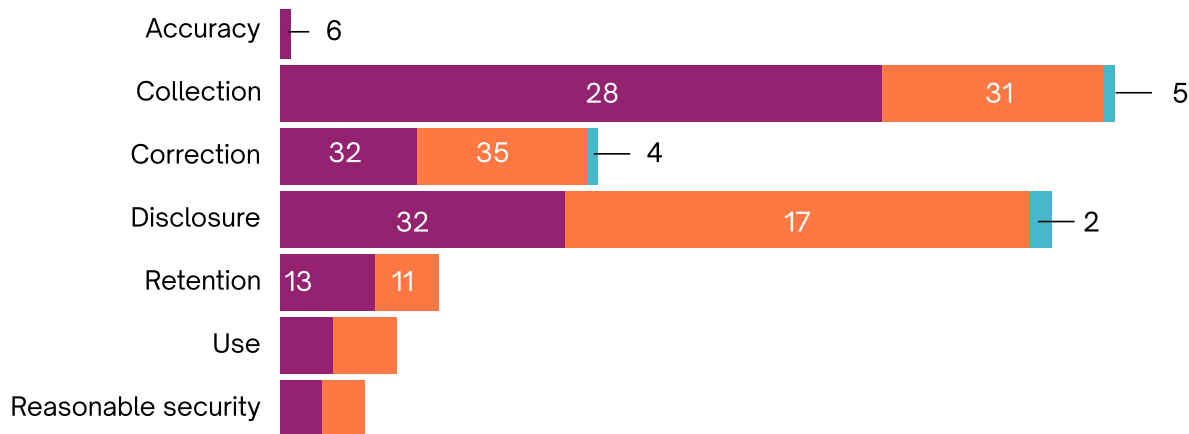
The OIPC received **456 privacy complaints** in 2024/25. The breakdown of complaints for both FIPPA and PIPA is:



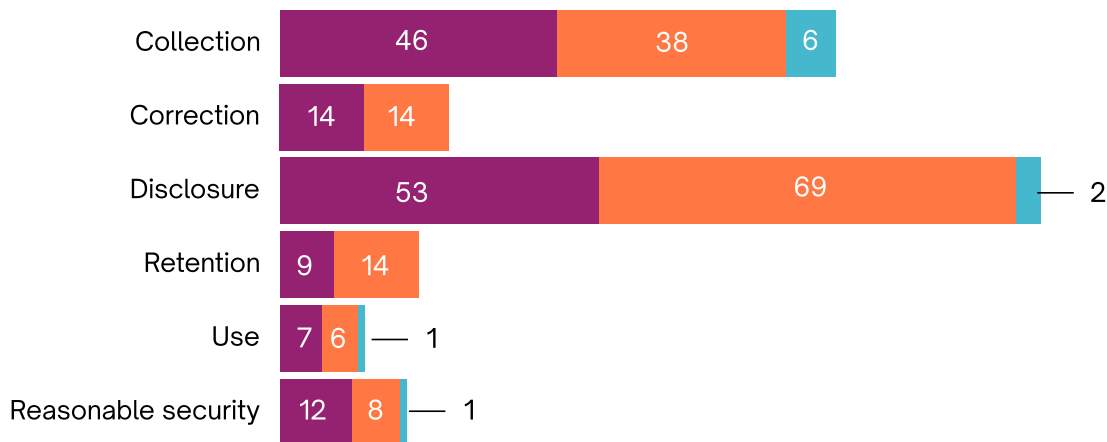
- Collection**  
Unauthorized collection of information
- Use**  
Unauthorized use by the public body or private organization
- Disclosure**  
Unauthorized disclosure by a public body or private organization
- Accuracy**  
Personal information in the custody or control of a public body is inaccurate 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 **217 FIPPA privacy complaints** in 2024/25. A complaint can ultimately result in an investigation, no investigation, or an inquiry. In 2024/25, 116 investigations were conducted on privacy complaints, 97 complaints resulted in no investigation, and 4 files proceeded to inquiry.



The OIPC resolved **304 PIPA privacy complaints** in 2024/25. A complaint can ultimately result in an investigation, no investigation, or an inquiry. In 2024/25, 141 investigations were conducted on access complaints, 149 complaints resulted in no investigation, and 14 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

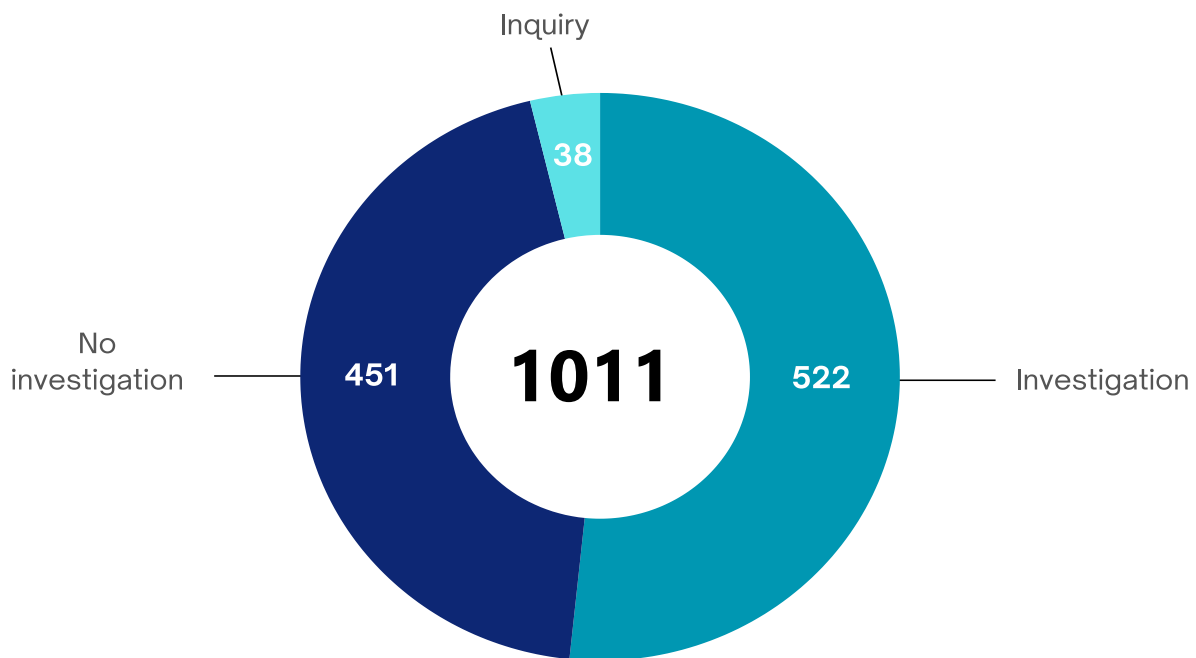


**Inquiry**

Files that proceeded to inquiry

# YEAR IN NUMBERS

Overall, the OIPC resolved **1011 FIPPA and PIPA access and privacy complaints** in 2024/25. There were 522 investigations, 451 files resulted in no investigation, and 38 proceeded to inquiry.



### Investigation

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



### No investigation

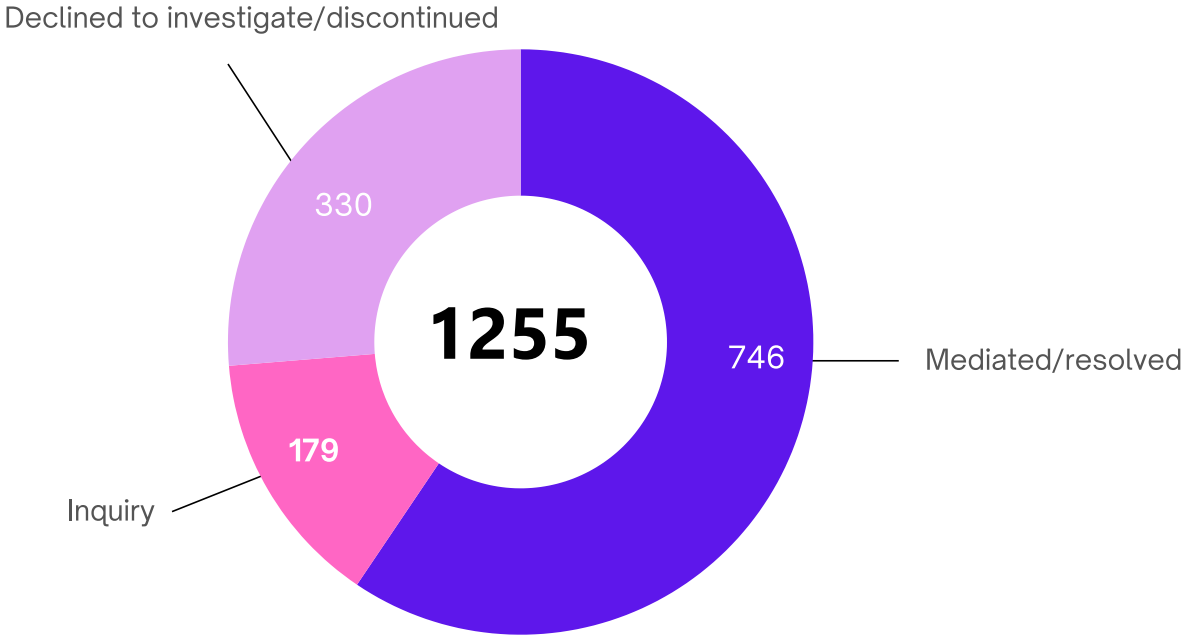
Files with no jurisdiction, no reviewable issue, or files in which the OIPC referred the complainant back to the public body or declined/continued an investigation



### Inquiry

Files that proceeded to inquiry

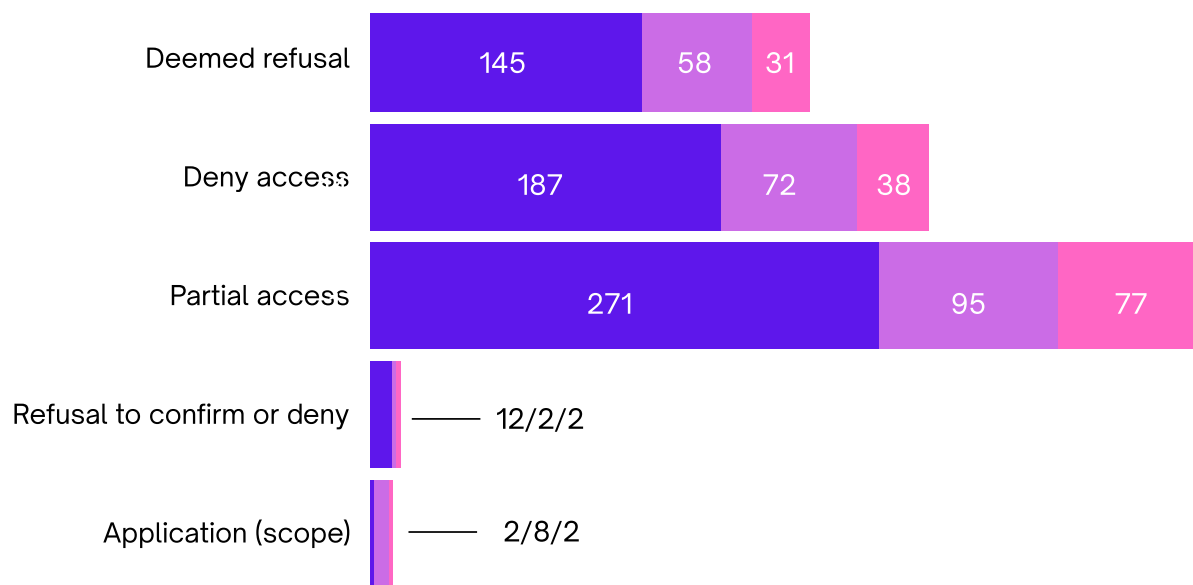
Overall, the OIPC resolved **1255 FIPPA and PIPA requests for review** in 2024/25. There were 746 files that were mediated/resolved, 179 proceeded to inquiry, and 330 were declined or discontinued.



- 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 **1060 FIPPA requests for review** in 2024/25. A request for review can ultimately be resolved through mediation, be declined or discontinued, or proceed to an inquiry. In 2024/25, 641 FIPPA request for review files were mediated/resolved, 254 files were declined or discontinued, and 165 files proceeded to inquiry.



**Mediated/resolved**  
Files that were mediated or withdrawn

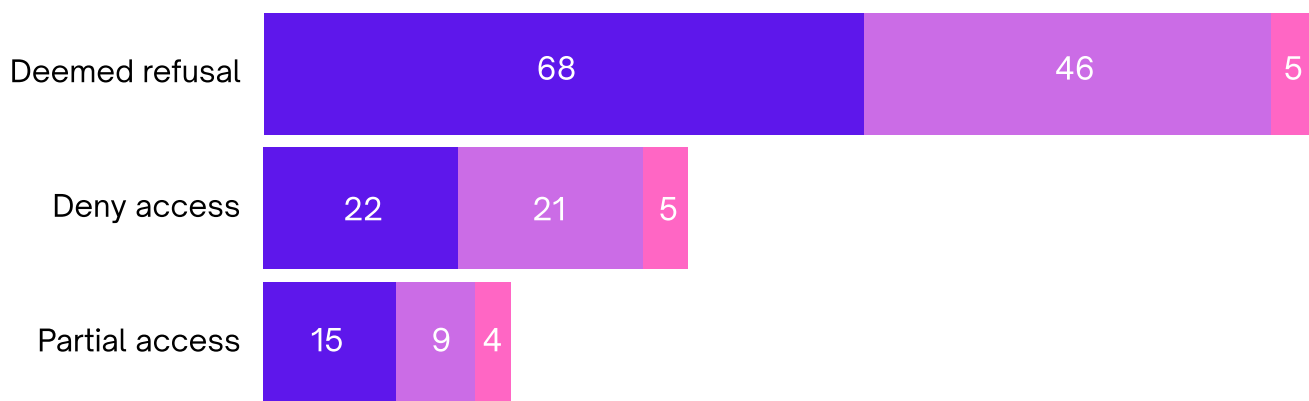
**Declined to investigate/discontinued**  
Files with no jurisdiction, no reviewable issue, or files in which the OIPC referred the complainant back to the public body or declined/discontinued an investigation

**Inquiry**  
Files that proceeded to inquiry





The OIPC resolved **195 PIPA requests for review** in 2024/25. A request for review can ultimately be resolved through mediation, be declined or discontinued, or proceed to an inquiry. In 2024/25, 105 PIPA request for review files were mediated/resolved, 76 files were declined or discontinued, and 14 files proceeded to inquiry.



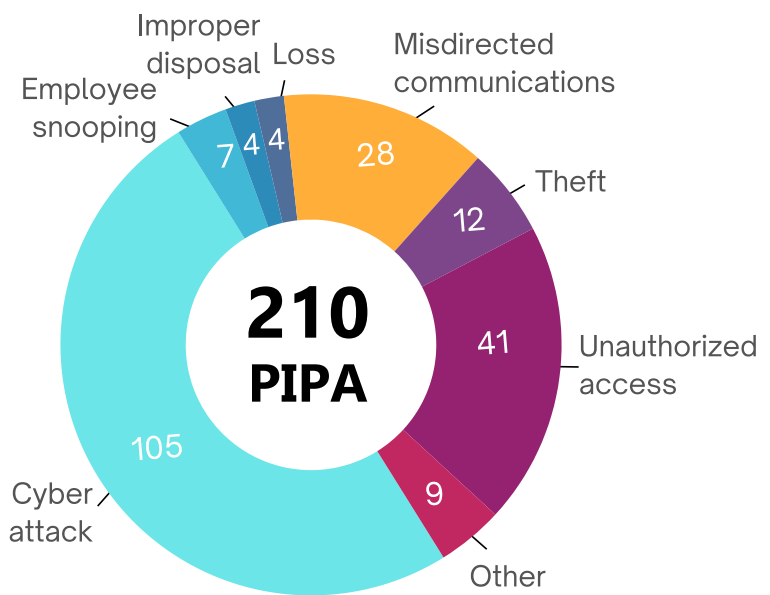
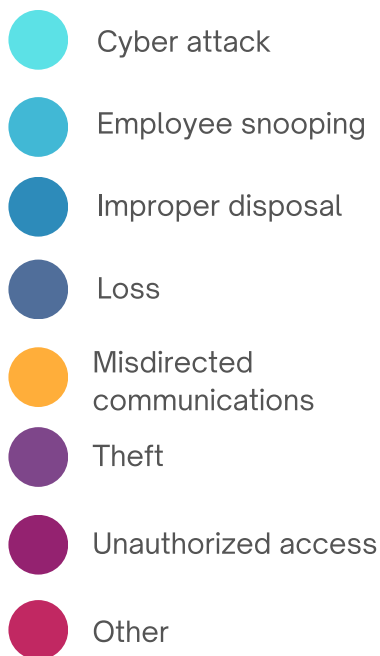
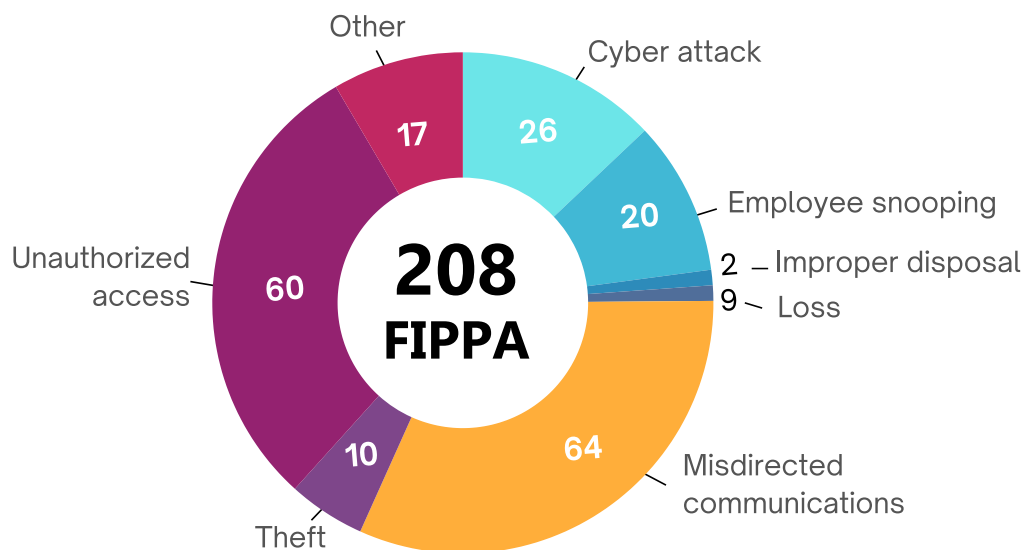
**Mediated/resolved**  
Files that were mediated or withdrawn

**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, 2024-March 31, 2025



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

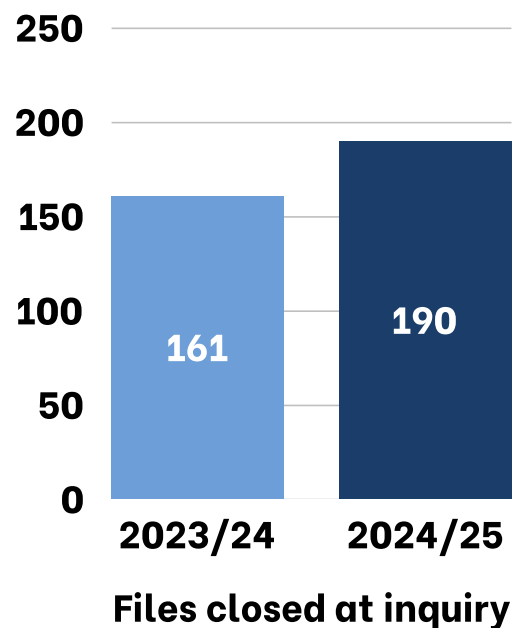
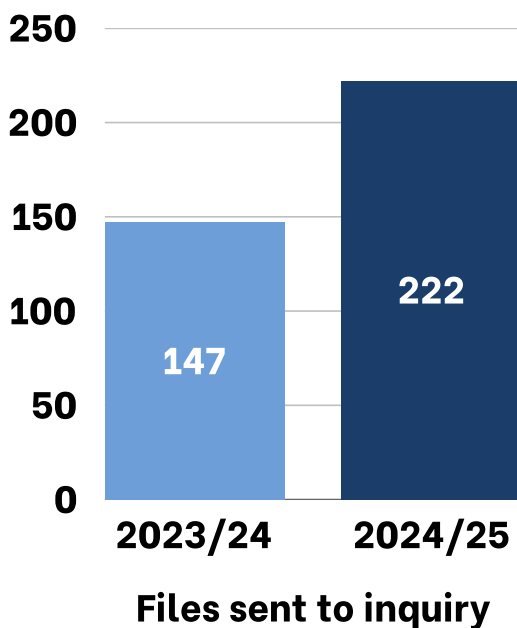
Complaints and requests for review are often resolved early on by case review officers or investigators. Some files that cannot be resolved during these stages are sent to adjudication.

# 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.

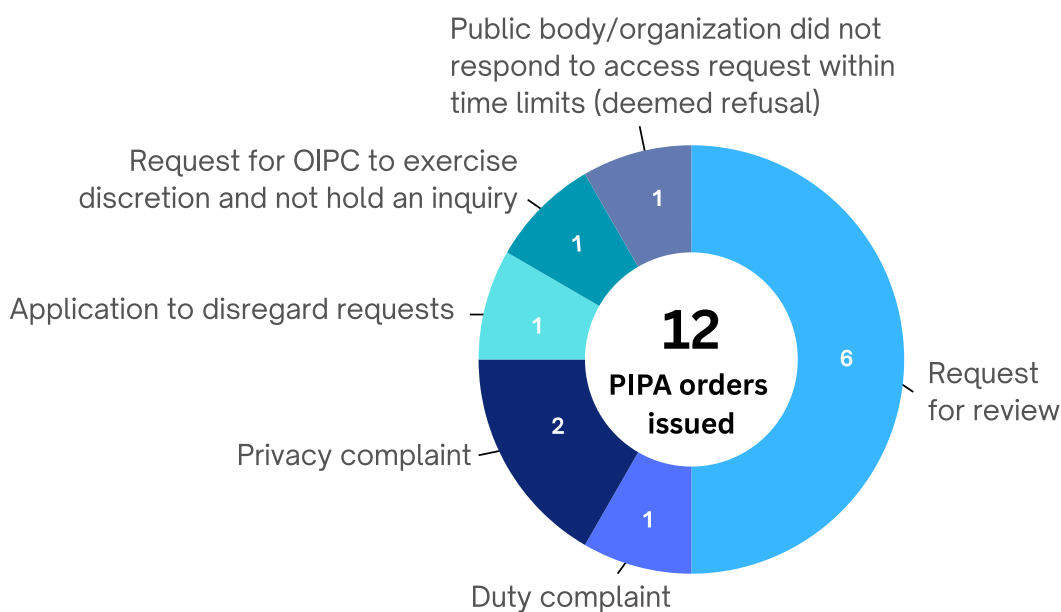
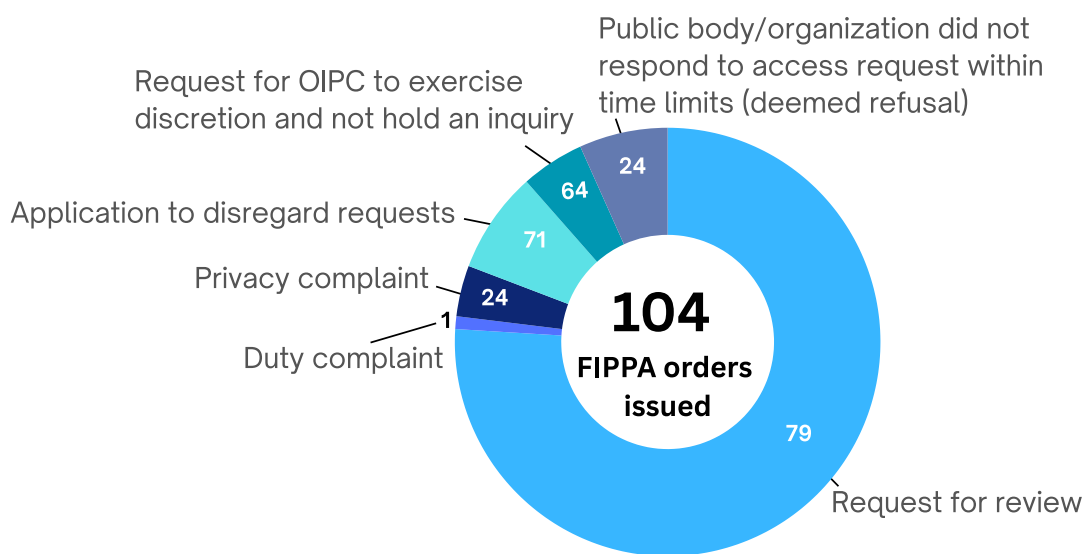
The following orders provide a snapshot of the varied nature of the cases handled at adjudication over the past year:

- An applicant complained a PAWsh Oasis Pet Resort publicly disclosed her name and details of her finances, her dog, and her conversations with staff members when the Resort posted a reply to the complainant's negative online review. ([Order P25-03](#))
- The South Coast British Columbia Transportation Authority (TransLink) requested authorization from the Commissioner to disregard an individual's 252 outstanding access requests. ([Order F24-38](#))
- A journalist requested the Ministry of Health provide him access to an itemized spreadsheet of PharmaNet data related to 26 years of prescribing and dispensing of benzodiazepines, stimulants, and narcotics, including opioids in British Columbia. ([Order F25-06](#))
- A nursing educator requested the British Columbia College of Nurses and Midwives provide her access to the College's entire file about a professional practice complaint she made against a former nursing student. ([Order F24-95](#))





## 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 participated in one joint report related to privacy with the Global Privacy Enforcement Network on deceptive design patterns. The OIPC's review focused on websites and apps aimed at children and found a higher incidence of deceptive design patterns in Canada than elsewhere in the world. The OIPC published an accompanying infographic to help parents, guardians, and children spot deceptive designs online. As the recommendations in the report were developed for all organizations, a percentage of implementations recommended does not apply and is not captured in Performance Measure 2.

The OIPC will replace Performance Measure 2 in 2025/26 with a Performance Measure on guidance documents, which better reflects service provided by the OIPC to public bodies and organizations.

The OIPC also conducted field and investigation work on several privacy reports in 2024/25. However, due to factors outside of the control of the office, publication of these reports will happen in a later fiscal year.

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	2024/25		25/26	26/27	27/28	28/29
	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	1	3	3	3	3
2 Percentage of related audit, compliance review, and systemic investigation report recommendations implemented	95%	N/A	N/A	N/A	N/A	N/A
Number of new or revised guidance documents to raise awareness about privacy issues under FIPPA or PIPA	N/A	N/A	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 two reports in 2024/25 relating to access to information. [\*Vancouver Coastal Health Authority's duty to assist\*](#) looked at whether the health authority met its duty to assist applicants and examined areas where the Vancouver Coastal Health Authority performed well, and areas where it required improvement to comply with legislation and OIPC guidelines. Vancouver Coastal Health has implemented four out of the six recommendations and are currently implementing the remaining two. The remaining recommendation for government has not been implemented.

[\*Municipal disclosure of records\*](#) investigated how municipalities make records available to the public, by looking at the types of, and costs for, records made available through the FOI process, proactive disclosure, or where records are made available for purchase.

The OIPC also issued one new infographic on [\*FIPPA and the application fee\*](#), and a new guidance document [\*Proactive disclosure: guidance for public bodies\*](#).

The OIPC will replace Performance Measure 4 in 2025/26 with a Performance Measure on guidance documents, which better reflects service provided by OIPC to public bodies and organizations.

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	2024/25		25/26	26/27	27/28	28/29
	Target	Actual	Target	Target	Target	Target
<b>3</b> Number of audits, special reports, compliance reviews and systemic investigations that promote an open, accountable, and transparent public sector	3	2	3	3	3	3
<b>4</b> Percentage of related audit, compliance review, and systemic investigation report recommendations implemented	95%	67%	N/A	N/A	N/A	N/A
Number of new or revised guidance documents to raise awareness about access issues under FIPPA or PIPA	N/A	N/A	3	3	3	3



## 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 49 speaking engagements in 2024/25.

In 2024/25, the OIPC held five in-person training sessions on FIPPA and PIPA in Kamloops, Victoria, and Vancouver. Staff outlined the fundamentals of both laws, and practical steps that both public bodies and private sector organizations could take to comply with the legislation, including developing robust privacy management programs, and how OIPC resources and staff are available to support them in their efforts.

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 2024/25 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	2024/25		25/26	26/27	27/28	28/29
	Target	Actual	Target	Target	Target	Target
<b>5</b> Number of OIPC presentations	50	49	50	50	50	50



# SERVICE PLAN GOAL 4

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

During the 2024/25 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.

The OIPC published a special report, [\*Accessibility, reconciliation, and inclusion at BC's Office of the Information and Privacy Commissioner and Office of the Registrar of Lobbyists\*](#) outlining the OIPC's commitment to these values.

The report lays out the office's plan to identify, remove, and prevent barriers to individuals in the areas of accessibility, reconciliation, and diversity & inclusion. Thirty-eight actions were identified across the three areas. The OIPC also created a webform to receive feedback from the public on the plan, and will report out on progress through the Annual Report and Service Plan.

The OIPC also implemented a number of internal efficiencies to improve service to the public. Improvements included:

- An early resolution project to address more straightforward reviews and complaints. The result was more timely resolution to the parties involved and a reduction in the overall number of files waiting for assignment to investigators.
- An improved submission form for parties to specify and focus the issues to be decided at adjudication.
- A new operating system to reduce administrative burdens, such as data entry for time extension requests and breach notification webforms.

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	2024/25		25/26	26/27	27/28	28/29
	Target	Actual	Target	Target	Target	Target
<b>6</b> Percentage of requests for review settled without inquiry	90%	87%	90%	90%	90%	90%
<b>7</b> Percentage of request for review files resolved within 90 business days of assignment	85%	80%	85%	85%	85%	85%
<b>8</b> Percentage of complaint files resolved within 120 business days	90%	80%	90%	90%	90%	90%
<b>9</b> Number of orders published per year	144	116	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 expenses, and the total remaining unused appropriation (unaudited) for the current and previous fiscal years:

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 to \$784,000 in contingencies

2023/24	Operating	Capital
Appropriation**	\$10,911,000	\$277,000
Total operating expenses	\$10,792,704	-
Capital acquisitions	-	\$275,074
Unused appropriation	\$118,296	\$1,926

\*\* includes access to \$1,639,000 in 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).

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
<b>Total tangible capital assets</b>	<b>\$1,078,604</b>	<b>(\$734,220)</b>	<b>\$344,383</b>

2023/24	Closing cost	Closing accumulated amortization	Net book value (March 31, 2024)
Computer hardware and software	\$1,086,761	(\$588,259)	\$498,503
Tenant improvements	\$0	\$0	\$0
Furniture and equipment	\$17,083	(\$14,225)	\$2,858
<b>Total tangible capital assets</b>	<b>\$1,103,844</b>	<b>(\$602,484)</b>	<b>\$501,361</b>

## 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, 2024 and March 31, 2025.

# 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 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 \(FIPPA\)](#)
- [How do I request records?](#)
- [How do I request a review?](#)
- [Instructions for written inquiries](#)
- [PIPA and workplace drug and alcohol searches: a guide for organizations](#)
- [Proactive disclosure: guidance for public bodies](#)
- [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](#)
- [Tip sheet: 10 tips for public bodies managing requests for records](#)

## 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](#)
- [Instructions for written inquiries](#)
- [Obtaining meaningful consent](#)
- [Political campaign activity code of practice](#)
- [Political campaign activity guidance](#)
- [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](#)
- [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](#)
- [Tips for public bodies and organizations setting up remote workspaces](#)

## Infographics

- [FIPPA and the application fee](#)
- [How to identify dark 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](#)
- [Responsible information sharing in situations involving intimate partner violence](#)
- [Tips for requesting records](#)
- [Transparency by default: information regulators call for a new standard in government review](#)



**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](mailto:info@oipc.bc.ca)

[oipc.bc.ca](http://oipc.bc.ca)