



Office of the Information
and Privacy Commissioner
for British Columbia

ANNUAL REPORT 2017-2018



OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

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;
- The ***Personal Information Protection Act*** (PIPA), applies to any private sector organization that collects, uses, and discloses the personal information of individuals in BC. PIPA also applies to any organization located within BC that collects, uses, or discloses personal information of any individual inside or outside of BC.

Michael McEvoy is BC's Information and Privacy Commissioner.

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 leaders in the global community. |



OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

October 2018

The Honourable Darryl Plecas
Speaker of the Legislative Assembly
of British Columbia
Room 207, Parliament Buildings
Victoria, BC V8V 1X4

Honourable Speaker:

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

This report covers the period from April 1, 2017 to March 31, 2018.

Yours sincerely,

Michael McEvoy
*Information and Privacy Commissioner
for British Columbia*

Table of Contents

- 4** Commissioner's message
- 6** Our work
- 8** Highlights
- 10** Summary of compliance
- 12** Timing is everything
- 14** Surrey Creep Catcher
- 16** Duty bound
- 18** Rental rights
- 20** Global guidance
- 22** Year in numbers
- 33** Financial reporting
- 35** Resources

COMMISSIONER'S MESSAGE



I am pleased to present our 2017-18 annual report, my first as British Columbia's Information and Privacy Commissioner.

When I began my term on April 1, 2018, I assumed responsibility for an office with a distinguished 25-year record of advancing the access and privacy rights of British Columbians. I owe a debt of gratitude to my predecessors, Elizabeth Denham, David Loukidelis, and David Flaherty.

The issues that confronted all of them grow more complex and challenging with each passing year. Access to information law continues to strain under the weight of increasing demand as government shifts from paper to digital systems. At the same time, democratic institutions themselves are being challenged around the globe. Public bodies need to be more transparent to restore public confidence in these institutions.

A tectonic shift also shook the privacy landscape this past year following sensational revelations about how Facebook and Cambridge Analytica used personal information during the Brexit campaign. I was directly involved with this matter. Prior to my appointment, I assisted the UK Information Commissioner's Office in its investigation of the two organizations.

This massive privacy breach drew the world's attention to the harm that can arise from the improper use of personal information. It also shone a light on the way that data moves across national boundaries. Millions of people were affected, including more than 600,000 Canadians. My experience investigating Facebook/Cambridge Analytica pointed to the critical need for privacy regulators to coordinate efforts on a global basis to properly protect the personal information of the people we serve.

As a result of these and other global events, British Columbians are more aware of their information rights, and with this awareness, the demands on the office continue to increase. Last year, OIPC staff received well over 5,000 queries from the public. Applications to challenge public bodies that withheld information increased by 13% while privacy complaints grew by 10%. Over the following pages, you will find a detailed review of the nature and number of the files undertaken by the office.

My staff addresses each of the files we receive from individuals, organizations, and public bodies with care. I'd like to highlight a few examples of work that makes a difference to British Columbians.

Last fall, my office conducted our fifth report on whether ministries are properly responding to access requests within the timelines set out in the *Freedom of Information and Protection of Privacy Act* (FIPPA). We noted an unhealthy increase in requests for time extensions, an issue that government is working to address.

We also audited the information sharing agreements of the Insurance Corporation of British Columbia (ICBC) last fall. Millions of BC residents are required to provide their personal information to ICBC to obtain a driver's licence, register or insure a vehicle, or process an insurance claim. We wanted to know if ICBC had adequate policies for sharing this data with third parties. While we were satisfied overall, our report recommended improvements, which ICBC has agreed to implement.

“I WILL CONTINUE TO PRESS THE PROVINCIAL GOVERNMENT TO AMEND ACCESS AND PRIVACY LEGISLATION TO KEEP UP WITH ADVANCES IN TECHNOLOGY AND MEET THE NEEDS OF OUR CITIZENS.”

This spring, we investigated how landlords screen prospective tenants, following numerous complaints about rental applications. Investigators found that BC landlords are generally asking for too much personal information from potential tenants. Given the competitive housing market, individuals often feel they have no choice but to answer these invasive questions. I believe that our recommendations will lead to a province-wide change in these screening practices.

Public bodies and organizations use increasingly sophisticated means to collect and use personal information. In many cases, this is not transparent to individuals. These issues were barely imaginable when the *Personal Information Protection Act* (PIPA) became law in 2004, let alone 25 years ago when FIPPA was enacted. For this reason I will continue to press the provincial government to amend access and privacy legislation to keep up with advances in technology and meet the needs of our citizens.

One stark example of the need for change is the lack of a mandatory breach notification law for the private and public sectors. It is unacceptable that public bodies and companies operating in BC are not required to report significant breaches of personal information to my office. More importantly, there is no obligation to report these breaches to the individuals who are directly impacted, making it impossible for affected individuals to take steps to protect themselves.

Another issue that must be addressed involves the lack of transparency when public bodies create subsidiary entities. These entities do the public's business, but for technical reasons are not covered by FIPPA's access to information requirements. These are two of many areas of necessary reform that I will ask our province's legislators to address.

Global events will continue to impact our work over the coming fiscal year, and the OIPC is justly proud of the role it plays as the Secretariat to the Asia Pacific Privacy Authorities (APPA), an organization of 20 privacy regulators around the Pacific Rim. Data follows trade and the fact that BC's largest trading partners are located on the Pacific Rim makes the OIPC role especially important. We are pleased that the Select Standing Committee on Finance and Government Services recognized this fact by providing the OIPC with additional funds to support our office's leading role.

It was my great honour to have been unanimously recommended by the Legislature to serve in the role of Commissioner. I wish to acknowledge Drew McArthur, who ably served our office as Acting Commissioner from July 6, 2016 to March 31, 2018. I reserve my final thank you, and enduring gratitude, to the staff of the OIPC who are steadfastly dedicated to serving the public of British Columbia.



Michael McEvoy
*Information and Privacy Commissioner
for British Columbia*

OUR WORK

Commissioner

The Information and Privacy Commissioner, an independent Officer of the Legislature, oversees the information and privacy practices of public bodies and private organizations. They have 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, comments on the implications of new programs, policies, and technologies on access and privacy rights, and engages in public education and outreach activities.

Case review

Case review officers help individuals file a complaint or seek a review of an access to information request. They identify issues, assist with forms and letters, and initiate the appropriate action. Case review officers are also first responders to privacy breach notifications. They can assist in early resolution of complaints and grant or deny a public body's time extension requests.



In 2017-18, case review officers received 186 privacy breach notifications, an increase of 12% over the previous year. They also processed 1,638 time extension requests, an increase of 28% compared to 2016-17.

Investigation & mediation

OIPC investigators conduct investigations and mediations on access and privacy complaints, review access to information requests, and process privacy breach notifications. They view any records at issue or relevant facts and evidence and work with public bodies, organizations, complainants, and applicants to reach resolutions.



In 2017-18, investigators received **506 requests for review of decisions to withhold information, an increase of 13% from 2016-17.**

Audit & compliance

Audit and compliance proactively assess compliance with the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act* for organizations and public bodies and make recommendations to improve practices, policies, guidelines, and legislation.



In 2017-18, the Commissioner published **two audits involving public sector agencies. The first involved information sharing agreements at ICBC; the second focused on WorkSafeBC's management of access and privacy requests and complaints.**

Adjudication

When a complaint or request for review cannot be resolved between parties, the Commissioner or their delegate will conduct a formal inquiry. Adjudicators assess the evidence and arguments and issue final and binding decisions that have the force of a court of law. Orders can be reviewed by the BC Supreme Court.



In 2017-18, adjudicators issued **57 orders, an increase of 11% from last year.**

Communications

The communications team publicizes the Commissioner's work and engages in public education and outreach to inform and empower individuals to exercise their information and privacy rights. The Office's website, social media presence, media relations, corporate reporting, and open data/proactive disclosure all fall under the communication department's oversight.



In 2017-18, the communications team managed **166 media inquiries, an increase of 24% compared to last year.**

Policy

Policy analysts conduct research and analyze current and emerging access and privacy issues, conduct systemic investigations, review and comment on privacy impact assessments, and consult with public bodies and private organizations. They also review and analyze proposed legislation for implications to access and privacy rights of British Columbians.




In 2017-18, policy analysts opened **206 policy or issue consultation files, an increase of 11% from last year.**

HIGHLIGHTS

OIPC investigates BC landlords and their compliance with PIPA


In BC's competitive rental market, some landlords ask prospective tenants for sensitive personal information in order to select the "best" tenant. Following numerous calls to our office from prospective tenants, the OIPC opened an investigation into tenant screening practices. Investigators found that landlords, who are subject to the *Personal Information Protection Act* (PIPA), generally ask for far too much personal information from potential tenants. This investigation offers 13 recommendations to landlords to improve how they handle tenants' personal information. Read more about the report on page 18.

 **DOWNLOAD:** *Always, sometimes, or never? Personal information and tenant screening* (oipc.bc.ca)

 **DOWNLOAD:** Guidance document: *Private sector landlords and tenants* (oipc.bc.ca)

OIPC releases report into government's response times for access to information requests

In a report issued in September 2017, the OIPC examined the government of BC's compliance with access request timelines as outlined in the *Freedom of Information and Protection of Privacy Act* (FIPPA). The report found a slight improvement in response times but responses to applicants were overdue for one in every five requests. The OIPC made eight recommendations to help government restore timely and efficient access to information and increase government accountability. Read more about the report on page 12.

 **DOWNLOAD:** *Timing is everything: Report card on government's access to information responses* (oipc.bc.ca)

 **DOWNLOAD:** Guidance Document: *10 Tips for public bodies: Managing requests for records* (oipc.bc.ca)

OIPC co-hosts 48th Annual Asia Pacific Privacy Authorities Forum

The OIPC's leadership role as Secretariat for the Asia Pacific Privacy Authorities (APPA) continued throughout 2017-18. In November 2017, the OIPC co-hosted the 48th APPA Forum in Vancouver with the Office of the Privacy Commissioner of Canada. APPA officials and guests discussed global policy trends with a focus on regulations in the digital age. They also explored opportunities for collaboration. APPA members work together to promote Privacy Awareness Week every May. For 2017, the theme was "Trust and Transparency." Activities throughout the week reminded businesses and public bodies to be transparent about the personal information they collect.

Surrey Creep Catcher

In 2016, two individuals complained to our office that an organization known as Surrey Creep Catcher had improperly collected, used, and disclosed their personal information. An OIPC order examined whether Surrey Creep Catcher was authorized by PIPA to collect, use, and disclose the two complainants' personal information. While the individuals voluntarily provided their personal information, they were not informed of the purposes for its collection and use. The OIPC ordered the organization and others to destroy the videos, pictures, and documents that had been shared online. Read more about the order on page 8.

 **DOWNLOAD:** *Order P17-03 Surrey Creep Catcher* (oipc.bc.ca)

OIPC audits WorkSafeBC's access to information and privacy practices

In January 2018, the OIPC published an audit of WorkSafeBC's management of access and privacy requests and complaints. Auditors found that while the provincial agency was fulfilling its duty under FIPPA and OIPC guidelines, there was room for improvement. The OIPC made four recommendations to help WorkSafeBC improve its current practices. Read more about the audit on page 16.

 **DOWNLOAD:** *WorkSafeBC: Management of access and privacy requests and complaints* (oipc.bc.ca)

GPEN regulators "sweep" website privacy practices

In May 2017, the OIPC participated in the fifth annual Global Privacy Enforcement Network (GPEN) privacy sweep. Twenty-four privacy regulators took part in this international review of the privacy notices, communication, and practices of 455 websites and apps. The four-day sweep examined the collection, purpose, and process of using and sharing personal information from the user's perspective. The OIPC specifically examined privacy materials from five polling firms located in British Columbia. It found these firms did not demonstrate awareness of their specific obligations under PIPA or clearly indicate these obligations within their own privacy policies. Overall, the regulators found that website notices are too vague and are generally inadequate.

OIPC audits ICBC information sharing practices

The Insurance Corporation of British Columbia (ICBC) maintains one of BC's most complete personal information data sets. Millions of BC residents are required to provide their personal information to ICBC to obtain a driver's licence, register or insure a vehicle, or process an insurance claim. OIPC auditors examined 94 information sharing agreements to confirm that ICBC fulfills its duty under FIPPA to protect the personal information of British Columbians. While we were satisfied overall, our report recommended improvements, which ICBC has agreed to implement. The report made 12 recommendations in three categories: Information Sharing Agreements, User Access Provisions, and Compliance Monitoring to help improve ICBC's practices.

 **DOWNLOAD:** *Insurance Corporation of British Columbia information sharing agreements* (oipc.bc.ca)

Big Data Surveillance project partnership continues

In 2017-18, the OIPC continued its partnership in the Big Data Surveillance Project, led by Queens University Surveillance Studies Centre. As a partner in the project, the OIPC provides research direction and feedback, with a focus on how advances in big data analytics and surveillance affect the privacy rights of British Columbians. The OIPC will co-host the project's upcoming research workshop on the use of big data analytics in political campaigns.

 **VISIT:** *The Big Data Surveillance Project* (sscqueens.org)

SUMMARY OF COMPLIANCE

AUDIT, SPECIAL, AND INVESTIGATION REPORTS

AUDIT/INVESTIGATION/SPECIAL REPORT	STATUS
<p>September 13, 2017</p> <p><i>Insurance Corporation of British Columbia information sharing agreements</i></p>	<p>Most recommendations have been implemented or are in the process of being implemented. We continue to follow up with ICBC on their progress toward full implementation.</p>
<p>September 20, 2017</p> <p><i>Timing is everything: Report card on government's access to information responses</i></p>	<p>In our view, government must respond more expeditiously to access requests. Government has committed to taking additional steps to address the challenges. We will continue to monitor their progress.</p>



AUDIT/INVESTIGATION/SPECIAL REPORT

STATUS

November 8, 2017

Use of employee surveillance by a BC chicken catching organization

All recommendations implemented.

January 17, 2018

WorkSafeBC: Management of access and privacy requests and complaints

All recommendations implemented.

March 22, 2018

Always, sometimes, or never? Personal information & tenant screening

Many landlords have modified their application forms as a direct result of the report. Our outreach and education with this sector is ongoing.

TIMING IS EVERYTHING

AN OIPC REVIEW OF GOVERNMENT RESPONSES TO ACCESS REQUESTS FOUND ROOM FOR IMPROVEMENT IN TIMELINESS AMIDST AN INCREASED VOLUME OF REQUESTS.



The vitality of any democracy depends on government transparency. In British Columbia, individuals have a right under the *Freedom of Information and Protection of Privacy Act* (FIPPA) to request access to any records held by government. FIPPA, which was passed unanimously by the Legislative Assembly in 1992, was among the earliest of over 100 similar statutes enacted around the world.

Under FIPPA, BC public bodies are obligated to respond to a request for records within 30 business days unless a time extension is permitted by any of the specific circumstances set out in section 10(1). Access rights are frustrated when responses to freedom of information requests exceed the time authorized under FIPPA. For this reason, the OIPC routinely reviews government's timeliness in responding to requests.

Our latest review spanned the period from April 1, 2015 to March 31, 2017 and examined the percentage of requests responded to on time, the average processing days taken, and the average number of days overdue. In 2015-16, the on-time response rate was 74%, the average processing time was 46 days, and the average days overdue was 57. In 2016-17, the on-time response rate improved to 80%, the average processing days remained at 46, but the average days overdue increased to 62.

The improvement in on-time responses meant that more people in BC received responses to requests that were within the timelines permissible under FIPPA. However, people who received overdue responses waited five days longer on average for a response.

Since 2009, the OIPC has published five timeliness reports. In the first report, then Commissioner David Loukidelis wrote, "My overarching aim is remedial, not punitive—once problems are identified, they can be understood and fixed." Through subsequent reports, ever-increasing numbers of access requests, and varying results, the OIPC has repeated this aim.

The OIPC made eight recommendations in our most recent report, including that government allocate resources to close overdue files, expand presumptive sign-off and proactive disclosure programs, and monitor and correct delays in the processing of freedom of information requests. These measures, if adopted, will improve on-time performance. ■



DOWNLOAD: *Timing is everything: Report card on government's access to information responses* (oipc.bc.ca)

SURREY CREEP CATCHER

ORGANIZATIONS THAT POST DIGITAL CONTENT ONLINE ARE SUBJECT TO BC'S PRIVATE SECTOR PRIVACY ACT.

Social media is a powerful tool that allows us to create and share information, ideas, personal messages and other content with friends, family, and even complete strangers through online communities. But sometimes digital content is shared in ways that violate the *Personal Information Protection Act* (PIPA).

In 2016, two individuals complained to the OIPC that an organization known as Surrey Creep Catcher improperly collected, used, and disclosed their personal information.

Surrey Creep Catcher is a BC branch of an organization that purports to protect children by finding and confronting suspected pedophiles or child predators. Its members pose online as fictitious persons, or decoys, by placing ads in the “Strictly Platonic” section of Craigslist. During the online interaction, the decoy indicates they are underage and arranges to meet the individual. When the decoy meets the target, the confrontation is recorded and distributed on social media.

OIPC Order P17-03 examined whether Surrey Creep Catcher was authorized by PIPA to collect, use, and disclose the two complainants’ personal information. Under PIPA, an individual has not given consent unless an organization has provided them with the purpose for consent. While the individuals voluntarily provided their personal information, they were not aware of the true purposes for its collection and use. For this reason, the OIPC concluded that the individuals did not consent to the disclosure of their personal information.

The OIPC also determined that Surrey Creep Catcher’s purpose was not investigative or journalistic. One of the criteria for journalistic purpose under PIPA includes providing an accurate and fair description of facts, opinion, and debate. As Surrey Creep Catcher reproduced the chats and videos with no such description, the order found that Surrey Creep Catcher was not carrying out its activities for a journalistic purpose. It also stated that the organization’s activities did not meet the definition of “investigation;” Surrey Creep Catcher’s true purpose was to “name and shame” the two individuals.

The OIPC found that Surrey Creep Catcher violated PIPA and ordered the organization and others to destroy the videos, pictures, and documents that had been shared online. The majority of the videos were removed after a BC Supreme Court judge reaffirmed the order. Surrey Creep Catcher petitioned the BC Supreme court to judicially review the order. The judge ruled that the organization must comply with the ruling until the judicial review process is complete. ■



DOWNLOAD: *Order P17-03: Surrey Creep Catcher*
(oipc.bc.ca)

DUTY BOUND

AN OIPC AUDIT OF WORKSAFEBBC SHOWED THAT THE PROVINCIAL AGENCY UNDERSTANDS ITS ACCESS AND PRIVACY OBLIGATIONS AND IS AN EXAMPLE FOR OTHER BC PUBLIC BODIES.



If you work or employ workers in British Columbia, chances are you've interacted with WorkSafeBC. The provincial agency oversees a comprehensive no-fault insurance system, regulating workplace health and safety for 2.33 million workers and 231,000 registered employers in British Columbia. While its mandate is to ensure that workers and employers come home safely from work every day, an OIPC audit found that the public agency also prioritizes the access and privacy rights of those it serves.

When work-related injuries or diseases occur, WorkSafeBC collects personal information from individuals in many ways, including insurance claims, reports of unsafe working conditions, or incident investigations. We chose to audit WorkSafeBC because this information is often highly sensitive. Our office also receives a higher number and variety of access and privacy complaints related to the agency compared to many other public bodies.

The OIPC's audit and compliance program is designed to be proactive and broad in scope. Its intent is to hold organizations accountable for adhering to the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). The key objective of this audit was to determine the extent to which WorkSafeBC's processes comply with FIPPA and OIPC guidelines and to provide recommendations where needed to improve the agency's policies and practices.

OIPC auditors reviewed the management of access and privacy requests and complaints by WorkSafeBC from 2014 to 2016 and found that the agency met its legislated timelines in response to applicants 94 percent of the time. The agency also conducted appropriate searches for records and rarely applied fees. The audit concluded that WorkSafeBC was a good example of a public body acting in accordance with privacy laws.

The OIPC audit report included four recommendations to help WorkSafeBC improve its request for records and complaint responses processes, including fully documenting all requests for records, and implementing an electronic case management system to manage requests for records and complaints and associated documentation. ■



DOWNLOAD: *WorkSafeBC: Management of access and privacy requests and complaints* (oipc.bc.ca)

RENTAL RIGHTS

THIS OIPC INVESTIGATION FOUND THAT BC LANDLORDS COLLECT TOO MUCH PERSONAL INFORMATION FROM POTENTIAL TENANTS.



About 1.5 million people live in rental housing in British Columbia, almost 30% of all households. With high demand and low vacancy rates, anyone looking for a place to rent in BC understands the challenge of finding accommodation, whether it's a basement suite or high-end condo. In this competitive rental market, some landlords ask prospective tenants for sensitive personal information in order to select the "best" tenant. Following numerous calls from prospective tenants, the OIPC investigated tenant screening practices.

To review the privacy awareness of landlords in BC, OIPC investigators asked eight for-profit and five not-for-profit landlords and rental management companies to provide our office with copies of their residential tenancy applications. These landlords collectively represent 200,000 rental units in BC. We also asked how that personal information is stored and used, how long it is retained, and if any of it is disclosed to other persons or organizations. Finally, we asked these landlords to explain how their collection, use, and disclosure of personal information was authorized by the *Personal Information Protection Act (PIPA)*.

Landlords can collect personal information about a prospective tenant in two ways. The first is to collect the information directly from the individual. The second way a landlord can collect information is through indirect means, such as a reference from a previous landlord.

Section 7(2) of PIPA states that landlords must not, as a condition of supplying a product or service, require an individual to consent to the collection, use, or disclosure of personal information unless the information is necessary to provide the product or service. Providing rental housing is a service. This means that a landlord cannot refuse to rent to someone who will not provide personal information unless that information is necessary to determine suitability as a tenant.

OIPC investigators found that the applications contained many invasive questions. Reports to our office from individuals were also concerning. One individual, for example, had been asked for three months of detailed bank statements; another was asked to consent to an inspection of their current residence before their application would be approved.

Overall, this investigation set out 13 recommendations to landlords that should help level the playing field for tenants, including limiting the amount of required personal information on tenant application forms, clearly stating the specific purpose for the collection of personal information from prospective tenants, and only requiring a credit check when a prospective tenant cannot provide sufficient references about previous tenancies or satisfactory employment and income verification.

Our office also recommended that landlords do not collect information about prospective tenants from social media platforms or internet search engines. Only information collected from publicly available sources such as professional or business directories, public registries authorized by provincial, federal, or municipal statutes, and online publications such as newspapers or magazines is authorized under PIPA. Renters often compete with hundreds of other applicants, leading landlords to think they can request any information they want. As this report found, that is not how BC privacy laws work. ■



DOWNLOAD: *Always, sometimes, or never? Personal information and tenant screening* (oipc.bc.ca)

DOWNLOAD: *Guidance document: Private sector landlords and tenants* (oipc.bc.ca)

GLOBAL GUIDANCE

THE OIPC COOPERATES WITH PROVINCIAL, FEDERAL, AND INTERNATIONAL REGULATORS TO ENSURE THAT THE PRIVACY RIGHTS OF BRITISH COLUMBIANS ARE PROTECTED, HERE IN BC AND AROUND THE WORLD.



It was once thought that protecting the privacy of British Columbians could be accomplished solely through domestic legislation. The problem is that our privacy laws, however protective, extend only to the edges of our borders. In our digital era, the personal data of British Columbians can be stored and used anywhere in the world. Strong provincial privacy laws can potentially be rendered meaningless if personal information is surrendered to organizations outside our borders.

In light of this, how can the privacy rights of citizens be properly secured? The answer is cooperation between provincial, federal, and international regulators. In Canada, the OIPC works with our provincial and federal counterparts on enforcement actions as well as guidance and other joint undertakings. In 2017, for example, Canadian commissioners sent a joint letter to members of the Council of Ministers of Education, stressing the importance of digital privacy education in Canadian schools. We have also strengthened our ties with the International Conference of Data Protection and Privacy Commissioners (ICDPPC), and we take a leading role in the Global Privacy Enforcement Network (GPEN).



DOWNLOAD: [Guidance document: *Competitive advantage: Compliance with PIPA and the GDPR*](#)
(oipc.bc.ca)

APPA

Asia Pacific Privacy Authorities



We are especially proud of our work as Secretariat to the Asia Pacific Privacy Authorities (APPA). APPA consists of 20 privacy regulators, all located around the Pacific Rim. This role is especially critical for the OIPC because our province conducts the vast majority of our trade with Pacific Rim countries. Where trade happens, personal data most often follows. We were pleased that the Select Standing Committee on Finance and Government Services of the BC Legislature acknowledged our work by providing \$100,000 over two years to help resource the Secretariat. We are currently in year two of our three-year term.

APPA meets twice each year to focus on common enforcement matters and seek ways to coordinate processes and approaches that benefit our respective citizenry. From November 15 to 17, 2017, the OIPC co-hosted the 48th APPA Forum in Vancouver with the Office of the Privacy Commissioner of Canada. At the forum, APPA officials and invited guests shared insights and perspectives, discussed global privacy trends, and looked for opportunities for joint regulatory guidance and enforcement activities across the Asia Pacific Region.

We collaborate with our international partners in an attempt to align our data protection regimes, so businesses can move personal information lawfully and securely between jurisdictions. This work takes on an even greater significance with the introduction of Europe's General Data Protection Regulation (GDPR) in May 2018. This Regulation includes strict provisions about transferring personal data outside of the EU. Its territorial scope extends to BC-based organizations offering goods and services in the EU or those that monitor the behaviour of EU citizens. In March 2018, we provided guidance to BC-based organizations to help them comply with the GDPR. We will continue to work with our provincial, federal, and international colleagues to ensure that the privacy rights of British Columbians are properly protected. ■

YEAR IN NUMBERS

Detailed information about the 2017-18 fiscal year is presented over the next eight pages. Here is a summary of some of the key findings:



Files received

The OIPC received 8,791 files in 2017-18. In 2016-17, 8,318 files were received.

+6%



Time extensions

The OIPC received 1,638 requests by public bodies and private organizations for time extensions in 2017-18 compared to 1,282 in 2016-17.

+28%



Privacy breach notifications

The OIPC received 186 privacy breach notifications in 2017-18. In 2016-17, 166 were received.

+12%



Request for review

The OIPC received 506 requests for review of decisions to withhold information in 2017-18. In 2016-17, 446 requests for review were received.

+13%



Policy or issue consultations

The OIPC received 206 requests for policy or issue consultations in 2017-18 compared to 186 in 2016-17.

+11%



Media inquiries

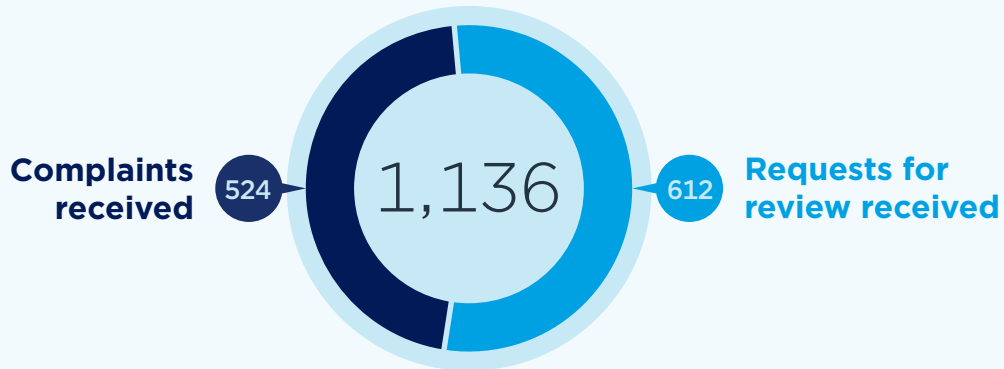
The OIPC received 166 media inquiries in 2017-18 compared to 134 in 2016-17.

+24%

Summary of all FIPPA and PIPA files received and closed in 2017-18 and 2016-17

FILE TYPE	Received 2017-18	Closed 2017-18	Received 2016-17	Closed 2016-17
Complaints				
Access complaints	439	379	447	503
Privacy complaints	273	260	248	275
Requests for review				
Requests for review of decisions to withhold information	506	389	446	613
Deemed refusal	160	167	197	195
Time extensions				
Requests by public bodies and private organizations	1,638	1,633	1,282	1,279
Requests by applicants seeking a review	34	31	12	10
Reconsideration of decisions				
Internal reconsideration of OIPC decisions	60	53	41	44
Information requested				
Requests for information and correspondence received	4,669	4,666	4,788	4,796
Media inquiries	166	160	134	129
FOI requests for OIPC records	15	15	17	17
Non-jurisdictional issue	23	21	11	11
No reviewable issue	97	93	91	90
Files initiated by public bodies and private organizations				
Applications to disregard requests as frivolous or vexatious	7	10	9	6
Privacy impact assessments	48	42	49	38
Privacy breach notification	186	195	166	164
Public interest notification	16	17	11	10
Policy or issue consultation	206	189	186	167
Police Act IIO reports	21	22	11	11
Request for contact information (research)			1	2
OIPC initiatives				
Investigations	18	11	11	7
Legislative reviews	20	18	18	21
Projects	27	22	17	28
Public education and outreach				
Speaking engagements and conferences	42	40	41	60
Meetings with public bodies and private organizations	33	29	7	17
Site visits	0	0	1	1
Other (section 56 and internal reviews)	87	91	76	63
TOTAL	8,791	8,553	8,318	8,557

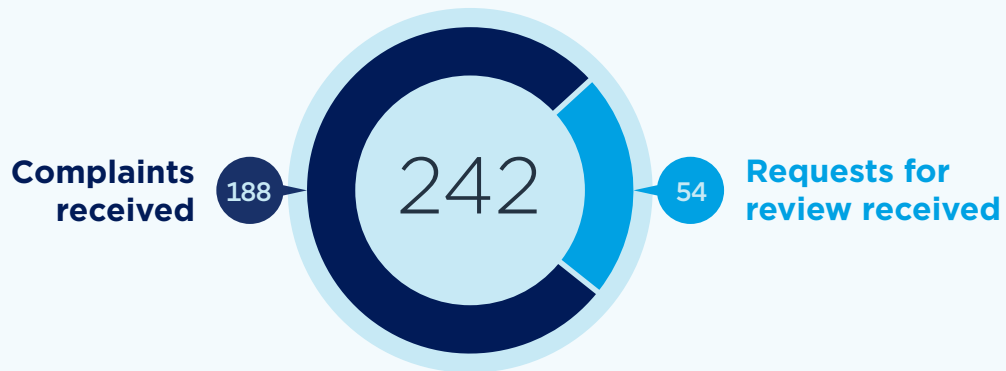
Number of FIPPA complaints and requests for review received in 2017-18 by public body



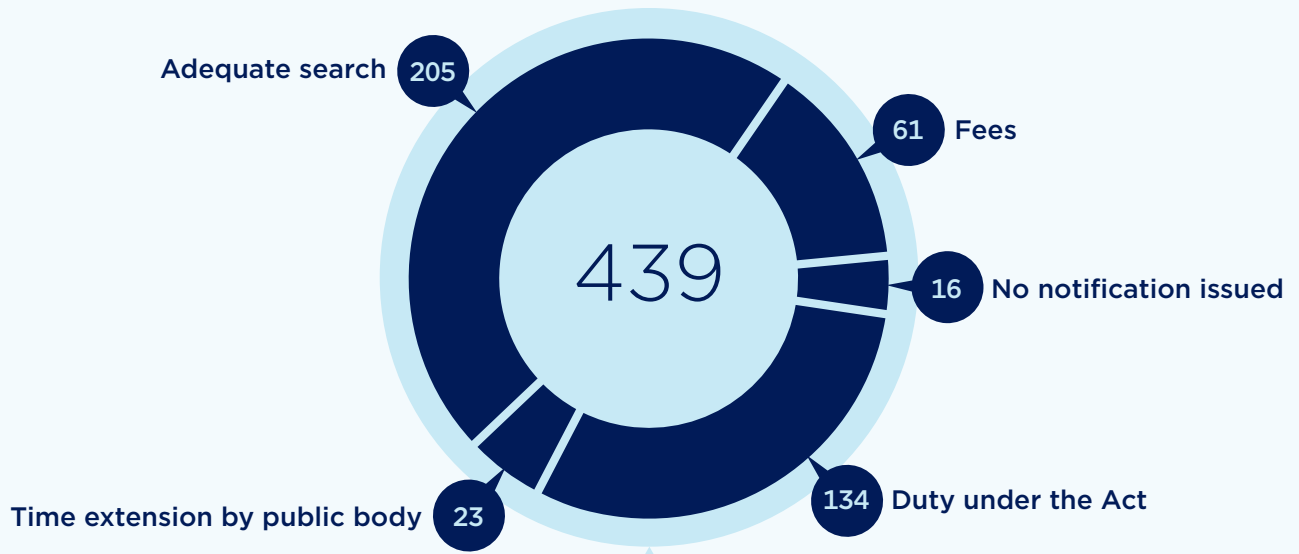
1	Insurance Corporation of British Columbia	59	23	36
2	Ministry of Finance	49	18	31
3	City of Vancouver	41	23	18
4	City of White Rock	40	15	25
5	Vancouver Island Health Authority	38	19	19
6	Ministry of Public Safety and Solicitor General	34	17	17
7	Ministry of the Attorney General	31	10	21
8	University of British Columbia	31	9	22
9	BC Hydro	28	10	18
10	Vancouver Police Department	27	4	23
Top 10		378	148	230
All other public bodies		758	376	382

NOTE: The number of requests for review and complaints against a public body does not necessarily indicate non-compliance, but may be reflective of its business model or quantity of personal information involved in its activities. The majority of ICBC requests for review, for example, are filed by lawyers performing due diligence on behalf of clients involved in motor vehicle accident lawsuits.

Number of PIPA complaints and requests for review received in 2017-18 by sector

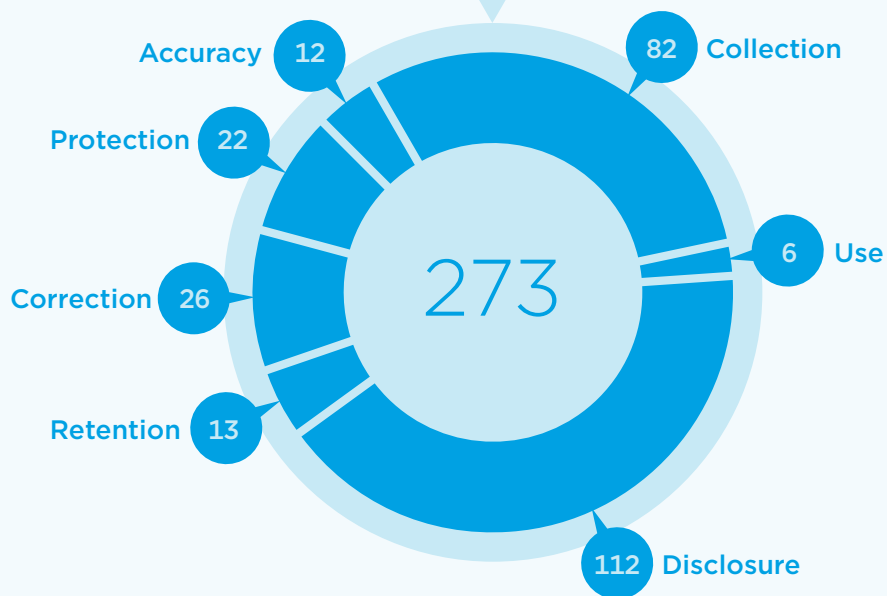


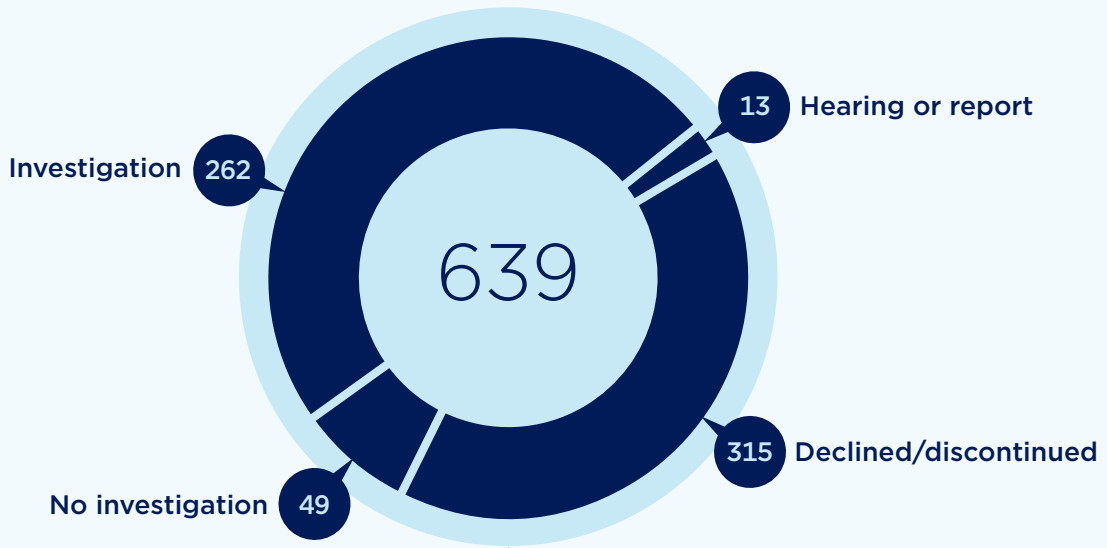
1	Services	73	58	15
2	Health	47	28	19
3	Retail trade	21	17	4
4	Real estate	18	16	2
5	Admin. support	16	14	2
6	Finance/insurance	16	14	2
7	Professional science and technology	12	10	2
8	Accommodation	9	9	0
9	Info/cultural	5	5	0
10	Mining and oil/gas	4	4	0
Top 10		221	175	46
	Other	21	13	8



Breakdown of access complaints received in 2017-18 (FIPPA & PIPA)

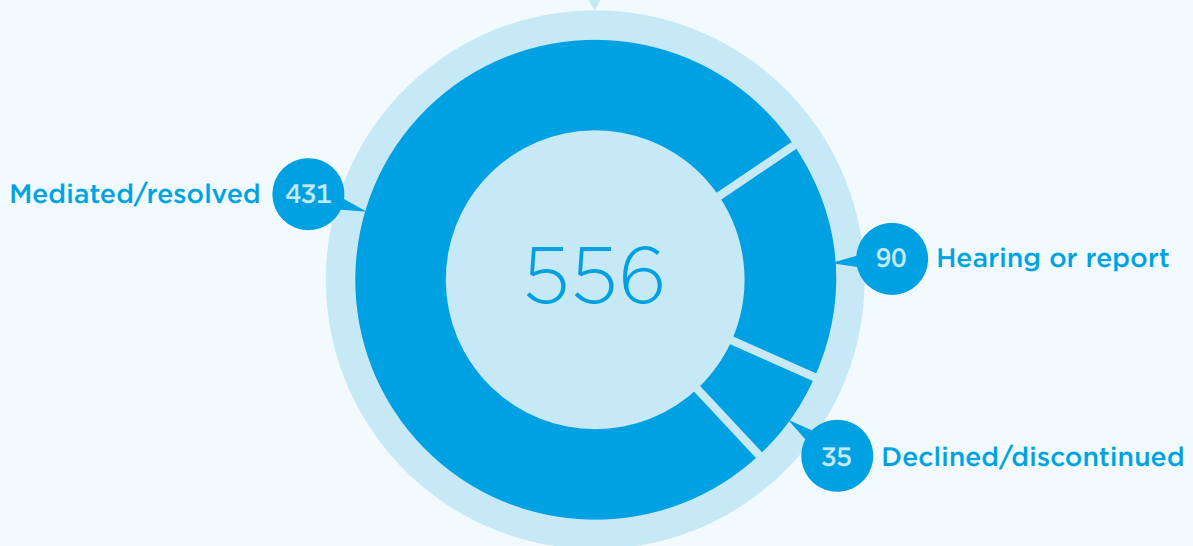
Breakdown of privacy complaints received in 2017-18 (FIPPA & PIPA)



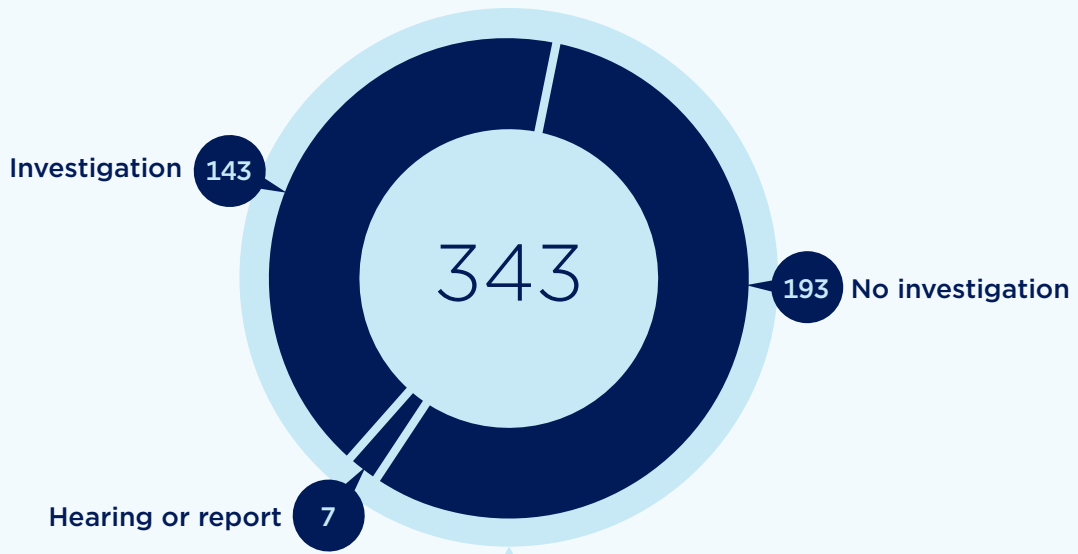


Outcome of all complaints closed in 2017-18 (FIPPA and PIPA)

Outcome of all requests for review closed in 2017-18 (FIPPA and PIPA)

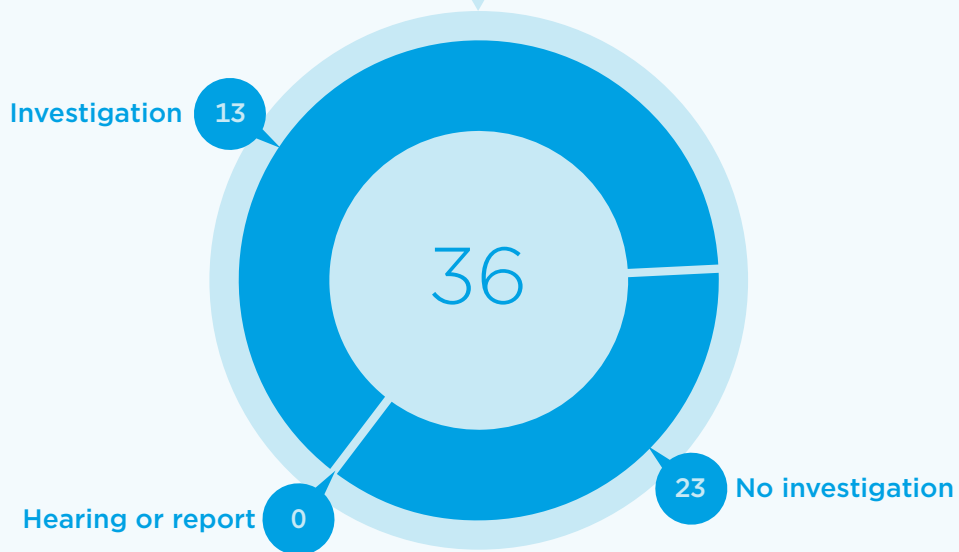


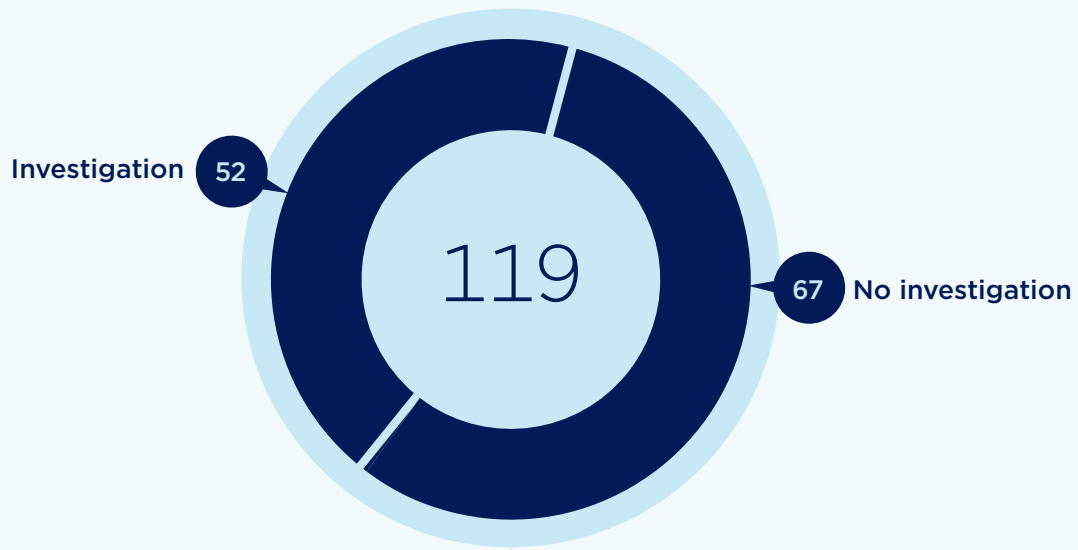
NOTE: Files can be declined or discontinued for various reasons, for example, if the OIPC lacks jurisdiction, the issue is beyond the scope of the legislation, or if the applicant is referred back to the public body/organization.



Outcome of access complaints closed in 2017-18 (FIPPA)

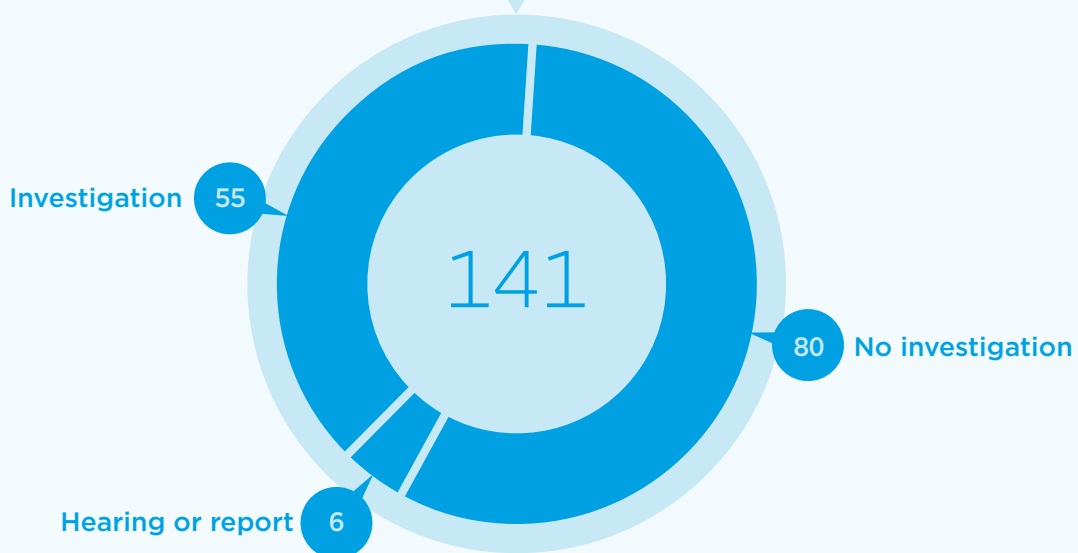
Outcome of access complaints closed in 2017-18 (PIPA)

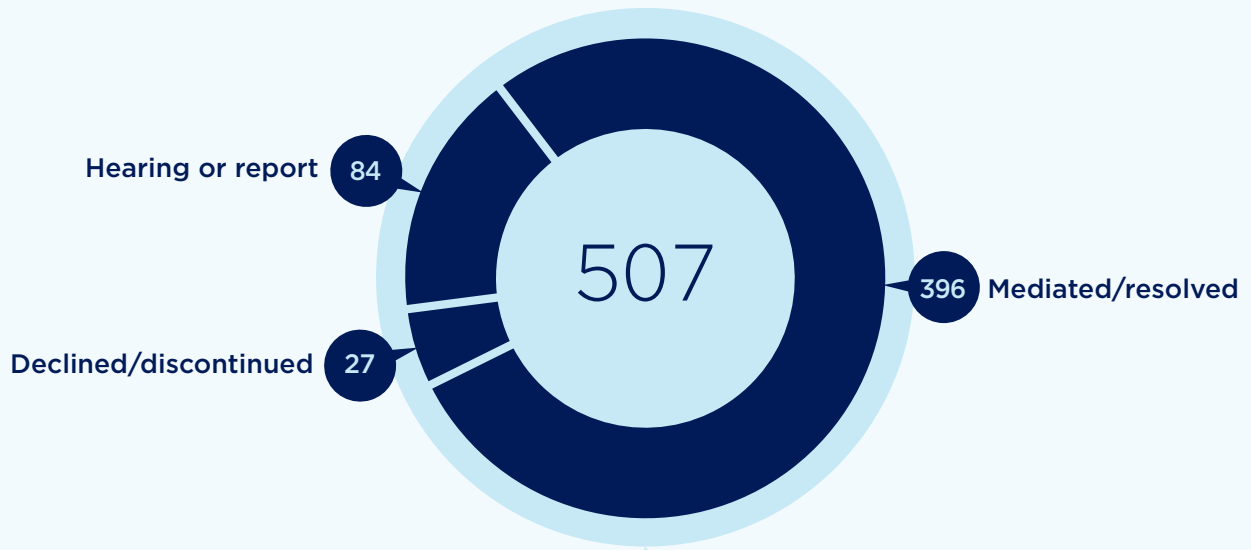




Outcome of privacy complaints closed in 2017-18 (FIPPA)

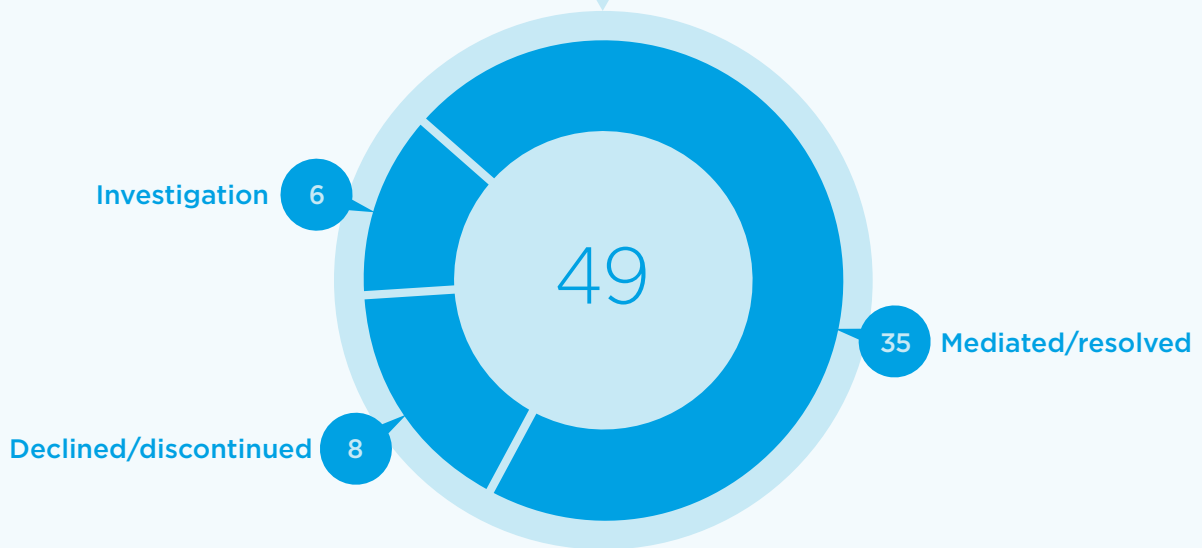
Outcome of privacy complaints closed in 2017-18 (PIPA)





Outcome of requests for review resolved in 2017-18 (FIPPA)

Outcome of requests for review resolved in 2017-18 (PIPA)



NOTE: Files can be declined or discontinued for various reasons, for example, if the OIPC lacks jurisdiction, the issue is beyond the scope of the legislation, or if the applicant is referred back to the public body/organization.



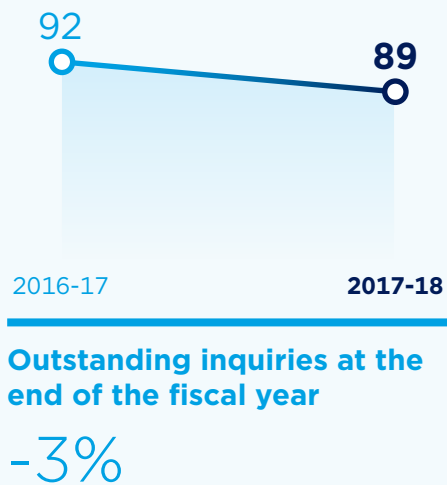
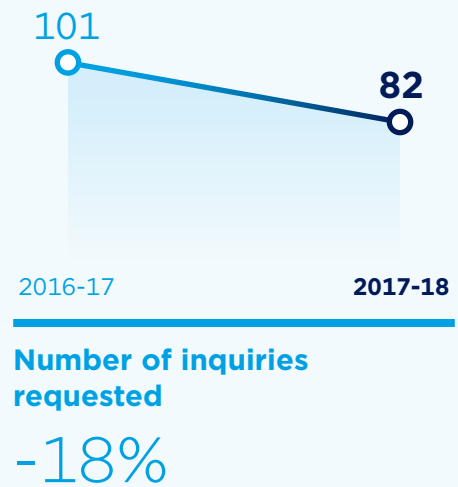
ADJUDICATION

The number of inquiry requests to the OIPC decreased from 101 in 2016-17 to 82 in 2017-18. The number of active inquiries at year-end also decreased, from 92 in 2016-17 to 89 in 2017-18. In total, adjudicators issued 57 orders, an increase from 51 in the previous fiscal year.

Adjudicators continue to develop and advance BC's privacy and access to information laws. Order F17-56 was the first occasion in which access to information in PRIME, a multi-jurisdictional police database, was considered. The OIPC invited and received submissions from the BC Association of Chiefs of Police and the BC Freedom of Information and Privacy Association. Ultimately, the adjudicator determined that by virtue of the *Police Act*, the public cannot access PRIME records by requesting them from the public body that operates PRIME (PrimeCorp). Rather, access requests must be made to the particular law enforcement agency from which the information originates. This ensures that law enforcement can maintain the integrity of their investigation files when an access request is made under FIPPA.

The application for records subject to solicitor client privilege held by public bodies is a frequent and challenging issue for adjudicators. In *Alberta (Information and Privacy Commissioner) v University of Calgary*, the Supreme Court of Canada held that Alberta's Information and Privacy Commissioner does not have the power to order production of records over which a public body has claimed solicitor client privilege. In Order F17-30, the senior adjudicator considered the implications of *University of Calgary* on BC's legislation. She concluded that unlike Alberta, BC's legislation provides the Commissioner with the authority to order records when necessary to fairly decide the dispute. The ability to review the records in dispute is an essential oversight power of the Commissioner. ■

ADJUDICATION *...continued*



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). FIPPA applies to more than 2,900 public agencies and accords access to information and protection of privacy rights to citizens. PIPA regulates the collection, use, access, disclosure, and retention of personal information by more than one million private sector organizations.

The Commissioner has a broad mandate to protect the rights given to the public under FIPPA and PIPA. This includes conducting reviews of access to information requests, investigating complaints, monitoring general compliance with the Acts, and promoting freedom of information and protection of privacy principles.

In addition, the Commissioner is also the Registrar of Lobbyists and oversees compliance and enforcement of the *Lobbyists Registration Act*.

Funding for the operation of the Office of the Information and Privacy Commissioner is provided through a vote appropriation (Vote 5) 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.

As well, part of the Office's funding is dedicated solely for the purpose of carrying out judicial review work, such as proceedings brought against the Office of the Information and Privacy Commissioner. Any portion of the dedicated funding that is unused for that purpose during the fiscal year is returned to the Consolidated Revenue Fund at fiscal year-end.

Accounting policies and procedures

This financial reporting has been prepared per the policies and procedures as set out in the Province of British Columbia's Core Policy and Procedures Manual (or CPPM), found at: <http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/CPMtoc.htm>. Section 1.2.4, Governance, Application, describes the entities that are required to follow the CPPM, which includes the Office of the Information and Privacy Commissioner.

Voted, used and unused appropriations

The Office receives approval from the Legislative Assembly to spend funds through an appropriation that includes 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 year:

	2017-18		2016-17	
	Operating	Capital	Operating	Capital
Appropriation	\$6,064,000	\$45,000	\$5,964,000	\$45,000
Total operating expenses	\$5,912,198	-	\$5,857,303	-
Capital acquisitions	-	\$28,109	-	\$24,596
Unused appropriation	\$151,802	\$16,891	\$106,697	\$20,404

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):

2017-18			
	Closing Cost	Closing Accumulated Amortization	Net Book Value (March 31/16)
Computer hardware and software	\$307,898	-\$272,742	\$35,156
Tenant improvements	\$552,302	-\$552,302	\$0
Furniture and equipment	\$98,400	-\$85,901	\$12,499
Leasehold commitments	\$958,600	-\$910,946	\$47,654.58

2016-17			
	Closing Cost	Closing Accumulated Amortization	Net Book Value (March 31/16)
Computer hardware and software	\$282,785	-\$248,114	\$34,671
Tenant improvements	\$552,302	-\$552,302	\$0
Furniture and equipment	\$95,403	-\$79,973	\$15,430
Leasehold commitments	\$930,490	-\$880,389	\$50,101

RESOURCES

Getting started

- Guide to OIPC processes (FIPPA and PIPA)
- A guide to PIPA for business and organizations
- A guide to FIPPA for individuals
- Early notice and PIA procedures for public bodies
- Access to data for health research
- BC physician privacy toolkit

Access (General)

- How do I request records?
- How do I request a review?
- Instructions for written inquiries
- Tip sheet: requesting records from a public body or private organization
- Tip sheet: 10 tips for public bodies managing requests for information
- Time extension guidelines for public bodies
- Guidelines for conducting adequate search investigations (FIPPA)

Privacy (General)

- Private sector landlords and tenants
- Information sharing agreements
- Guidelines to develop a privacy policy
- Employee privacy rights
- Guide to using overt video surveillance
- Direct to consumer genetic testing and privacy
- Privacy proofing your retail business
- Protecting personal information away from the office
- Identity theft resources
- Privacy emergency kit

Audit and Compliance

- Audit and Compliance Program Charter

Comprehensive privacy management

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

Privacy breaches

- Key steps to responding to privacy breaches
- Breach notification assessment tool
- Privacy breach policy template
- Privacy breach checklist
- Privacy breaches: tools and resources

Technology and social media

- Mobile devices: tips for security & privacy
- Cloud computing guidelines (public and private sector)
- Good privacy practices for developing mobile apps
- Public sector surveillance guidelines
- Guidelines for overt video surveillance in the private sector
- Use of personal email accounts for public business
- Guidance for the use of body-worn cameras by law enforcement authorities
- Guidelines for online consent
- Guidelines for social media background checks



To request copies of these resources, or to get more information about BC's access and privacy laws, email info@oipc.bc.ca or visit oipc.bc.ca



OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.



OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information and
Privacy Commissioner for British Columbia

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

Telephone: 250.387.5629

Toll Free in B.C.: 1.800.663.7867

Email: info@oipc.bc.ca

 [@BCInfoPrivacy](https://twitter.com/BCInfoPrivacy)

oipc.bc.ca