Office of the Information
and Privacy Commissioner
for British Columbia

ANNUAL REPORT 2018-2019

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;
- The ***Personal Information Protection Act*** (PIPA), which 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.
Dedication	We are dedicated to protecting privacy and promoting transparency.
Expertise	We use our expertise to enforce and advance rights, resolve and adjudicate disputes, and encourage best practices.
Innovation	We are innovators and recognized leaders in the global community.
Respect	We respect people, organizations, public bodies, and the law.

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

October 2019

Honourable Darryl Plecas
Speaker of the legislative assembly
of British Columbia
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*, I have the honour of presenting the Office of the Information and Privacy Commissioner's Annual Report to the legislative assembly.

This report covers the period from April 1, 2018 to March 31, 2019.

Yours sincerely,

Michael McEvoy
Information and Privacy Commissioner for British Columbia

Table of contents

COMMISSIONER'S MESSAGE

I am pleased to present the 2018-19 annual report of the Office of British Columbia's Information and Privacy Commissioner.

It was a year in which demands on the OIPC increased dramatically. Privacy complaints increased by 22%, requests for information grew by 17%, and the total number of files handled by the OIPC rose by 38%, from 8,791 files to 12,148.

Managing this was possible because of the efforts of a very talented group of people I work with and their deep commitment to public service. Our continuous improvement plan meant that my team could deal with the rise in demand using existing OIPC resources. I am grateful to each of them.

These increased pressures on the OIPC signal that the trust relationship between citizens and the organizations and public bodies that impact their lives is under increasing strain. This has led to a growing public desire to hold these bodies accountable and ensure their transparency.

Over the past year, the work of my office has paralleled the public's desire for accountability. We audited and worked with staff at the City of White Rock to improve their access to information systems. We investigated and guided the City of Nanaimo to make sure the personal information entrusted to them was properly protected.

One area that will benefit from greater transparency is the collection and use of voter information by political parties. Public trust in our system of political campaigning goes to the very heart of our democracy. Prior to taking my post as BC's Commissioner, I helped lead the UK Information Commissioner's Office investigation into what is now known as the Facebook-Cambridge Analytica scandal. I saw firsthand how people's personal information can be exploited and abused in the political campaign process. This was not a practice that anyone would want to wash up on BC's shores. It led my office to investigate how our province's largest political parties collect and use voters' personal information. We found some of their practices were not consistent with their legal obligations, nor were they in line with citizens' expectations.

I am now working with BC's Chief Electoral Officer to have political parties agree on a code of practice that clearly spells out their legal responsibilities. A successful outcome will undoubtedly enhance public trust in our political campaign system.

This past year, I also joined with other Officers of the Legislature to support accountability and transparency. Together with the Merit Commissioner and the Ombudsperson, we sent a letter to members of the BC Legislature calling for the *Freedom of Information and Protection of Privacy Act* to apply to the Assembly's administrative functions.

While investigations, declarations, and audits are means to effect legislative compliance, education is equally important in strengthening access and privacy rights. I am especially proud of PrivacyRight, an initiative designed to inform private organizations of all sizes about their obligations to properly protect people's personal information. Resources we have prepared, including webinars, podcasts, and guidance documents, have already been well utilized by British Columbians. The clear message to private organizations: privacy compliance is good for business.

Rapidly advancing technology has also meant that personal data is beamed across provincial and national borders at light speed. This requires our office to work with privacy commissioners across Canada and globally to properly protect British Columbians' personal information. The Facebook-Cambridge Analytica scandal is a good example. It affected 622,000 users in Canada, including 92,000 in British Columbia. Our joint investigation with the Privacy Commissioner of Canada focused on how privacy laws require Facebook to better protect the personal information of its users.

Personal data flows and trading relationships often move in tandem. Many of British Columbia's trading partners are found in the Asia Pacific region and for that reason, my office plays an active part in the Asia Pacific Privacy Authorities (APPA), serving as Secretariat and Chair of its Governance Committee. The 19 members of APPA share best regulatory practices, evaluate technological developments, and coordinate privacy enforcement actions, among other collaborative efforts. We are grateful that the Select Standing Committee on Finance and Government Services at the legislative assembly of BC recognizes the benefits of global privacy awareness and enforcement by recommending that the OIPC receives additional funds to support our office's leading role.

Finally, the public's increased desire for accountability and transparency can only be fully addressed by legal reform. Fast-changing technologies add to the urgency of the need for change. Successive special legislative committees of the legislature have recommended that government amend privacy and access legislation to protect citizens' rights. One stark example is what happens when someone's personal information is breached by a public body or a private organization. In such cases, there is no requirement for my office to be told about it nor does legislation require that the public body or organization notify the person whose information has been breached. This is unacceptable, especially at a time when governments and businesses collect vast amounts of especially sensitive information about people.

Mandatory reporting of breaches that can result in harm is one of many reforms needed to ensure access and privacy legislation properly serve their public purposes. It is up to government to initiate these needed changes and legislators to give their assent.

Michael McEvoy
Information and Privacy Commissioner for British Columbia

"THE PUBLIC'S INCREASED DESIRE FOR ACCOUNTABILITY AND TRANSPARENCY CAN ONLY BE FULLY ADDRESSED BY LEGAL REFORM. FAST-CHANGING TECHNOLOGIES ADD TO THE URGENCY OF THE NEED FOR CHANGE."

OUR TEAM

The 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, 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.

Investigation & mediation

OIPC investigators conduct investigations and mediations on access and privacy complaints, review access to information requests, and process 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.

Adjudication

When a complaint or request for review cannot be resolved informally, the Commissioner or their delegate may 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.

Policy

Policy analysts 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 the access and privacy rights of British Columbians.

Audit & compliance

The audit and compliance team proactively assesses compliance of organizations and public bodies with BC's privacy and access laws and makes recommendations to improve practices, policies, guidelines, and legislation.

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.

A modest team with a big mandate

There were 40 people in the Office of the Information and Privacy Commissioner in 2018-19. An additional 18 Corporate Shared Services people provided finance, administration, HR, IT, and facilities support to our office as well as the three other Officers of the Legislature in our building, including the Office of the Merit Commissioner, the Office of the Police Complaint Commissioner, and the Office of the Ombudsperson.

Long service awards

The Commissioner introduced a Long Service Program in 2016 to honour the dedicated staff of the OIPC. These awards are presented annually at five-year increments. For the 2018-19 fiscal year, we distributed Long Service certificates to five individuals: two received five-year certificates, two received 15-year certificates, and one received a 25-year certificate for their service to our office and the people of British Columbia.

Community service

OIPC staff take pride in and have long supported community causes. This includes the Provincial Employees Community Services Fund (PECSF), as well as other local charities, such as Our Place, The Mustard Seed, and Canadian Blood Services. The OIPC received two awards for the 2018 PECSF campaign: Highest Participation Rate and Highest Average Donation for a small entity.

YEAR AT A GLANCE 2018-2019

Time extensions

The OIPC received 3,854 requests from public bodies and private organizations for time extensions to respond to a request compared to 1,638 in 2017-18.

+135%

Privacy complaints

The OIPC received 332 privacy complaints compared to 273 in 2017-18.

+22%

Policy consultations

The OIPC received 392 requests for consultations about policy-related matters compared to 206 in 2017-18.

+90%

Privacy breach notifications

The OIPC received 194 privacy breach notifications compared to 186 in 2017-18.

+4%

Requests for information

The OIPC received 5,481 requests for information compared to 4,669 requests in 2017-18. These are general requests from the public, public bodies, and organizations.

+17%

Total files

The OIPC received 12,148 files compared to 8,791 files in 2017-18

+38%

HIGHLIGHTS

OIPC investigates use of personal information by political parties

BC's *Personal Information Protection Act* (PIPA) governs how organizations, including political parties, collect, use, or disclose information about individuals. After receiving complaints about how BC's political parties had treated their personal information, the OIPC opened an investigation into the privacy practices of the BC NDP, Green, and Liberal parties. Commissioner McEvoy found that political parties are generally collecting too much information from potential voters without proper consent. He made 17 recommendations for BC political parties to improve their practices. The parties have made some progress in responding to the recommendations, particularly in regards to training campaign volunteers.

DOWNLOAD: *Full disclosure: Political parties, campaign data, and voter consent* (oipc.bc.ca).

READ: *Full disclosure, beginning on p. 16.*

Commissioner testifies before Federal Standing Committee on Access to Information, Privacy and Ethics (ETHI)

In May 2018, Commissioner McEvoy appeared before the ETHI Committee to discuss the breach of personal information involving Cambridge Analytica and Facebook. In his remarks, he urged committee members to seek out legislative remedies that would help assure Canadians about the privacy of their data and the integrity of our democratic and electoral processes. He also stressed the importance of Canada's political parties taking measures themselves to restore confidence in Canada's democracy.

READ: *Statement to Standing Committee on Access to Information, Privacy, and Ethics* (oipc.bc.ca).

Commissioner launches educational campaign for BC's private sector

Commissioner McEvoy launched a new initiative called PrivacyRight in February 2019 to help private organizations that collect, use, or disclose personal information from employees, customers, clients, members, and patients understand their obligations under PIPA. The free online program covers topics such as the basic obligations of PIPA, the importance of effective privacy management programs, how to write a privacy policy, responding to access requests, and more. New tools will be published monthly throughout 2019 on the OIPC website.

VISIT: oipc.bc.ca/PrivacyRight

HIGHLIGHTS

OIPC audits City of White Rock's freedom of information program

The "duty to assist" applicants is an essential component of FIPPA that requires public bodies to make every reasonable effort to assist each applicant openly, accurately, completely, and without delay. In this report, the OIPC Audit & Compliance team assessed whether the City of White Rock (the City) was meeting its duty to assist applicants. Specifically, auditors reviewed the City's approach to processing freedom of information (FOI) requests by recurrent applicants. The audit found both strengths and weaknesses in the City's FOI program. Commissioner McEvoy made three recommendations for full compliance with FIPPA, including that the City fully document all FOI requests from the original request to the closing of the file; forward requests to departments to search for records as soon as possible; and respond to all FOI requests without delay and within legislated timelines. The City has implemented all of the recommendations.

READ: *City of White Rock Duty to Assist* (oipc.bc.ca).

OIPC releases lesson plans for students

In partnership with the Office of the Privacy Commissioner of Canada, Canadian provincial and territorial regulators, and MediaSmarts (a Canadian not-for-profit organization), the OIPC published and distributed lesson plans for BC students in both official languages. Three of the four plans were designed for Grades 6 to 9, while the fourth plan targets high school students from Grades 9 to 12. The lesson plans incorporate videos, class discussions, and exercises to introduce students to privacy principles, such as online privacy, the concept of personal privacy, and personal information regulations

VISIT: oipc.bc.ca/resources/lesson-plans/

International GPEN privacy sweep highlights need for improved privacy practices

The OIPC, together with colleagues from around the world, surveyed more than 600 organizations in 18 countries in the sixth annual Global Privacy Enforcement Network (GPEN) sweep. This year's investigations examined how well respondents have implemented accountability policies and procedures for handling personal information. A total of 356 responses were received from organizations across a variety of sectors. Results highlighted a need for organizations around the world to improve their privacy practices. In BC, PIPA requires organizations to develop policies and procedures to meet their obligations under the Act. These requirements are founded on the principle of accountability and are consistent with the measures used in this year's sweep.

INFO: Global Privacy Enforcement Network (privacyenforcement.net).

Legislative Officers urge reform of BC legislative assembly administrative functions

In February 2019, Commissioner McEvoy, Ombudsperson Jay Chalke, and Merit Commissioner Fiona Spencer wrote a joint letter to the Legislative Assembly Management Committee urging the adoption of a modern transparency and accountability framework for the administrative aspects of the legislative assembly. They called for these changes to be built into the audit being conducted by the Auditor General of BC. Together, the officers also called for legislative amendments to the respective Acts that govern their roles, which would provide greater oversight of the legislative assembly's administration, including revisions to FIPPA, so that the Act also applies to the legislative assembly.

READ: oipc.bc.ca/public-comments/2274

HIGHLIGHTS

OIPC order authorizes access request after transfer of former Crown agency's assets

The Ministry of Advanced Education, Skills & Training tried unsuccessfully to use an OIPC order pertaining to a crown corporation whose mandate it had taken over to disregard a new access request from an applicant. The Private Career Training Institutions Agency (PCTIA) was a crown agency that had regulated privately run career training institutions in British Columbia. In early 2016, the OIPC issued Order F16-24 authorizing PCTIA to disregard certain access requests from an applicant because they were frivolous or vexatious under s. 43 of FIPPA. PCTIA was later dissolved and its mandate taken over by the Ministry. The Ministry relied on Order F16-24 to deny a subsequent access request from the applicant, claiming that the order was an asset that had been transferred to it from the crown corporation. The adjudicator found that the Order was not an asset and ordered the Ministry to respond to the applicant's access request.

DOWNLOAD: *Order F18-25* (oipc.bc.ca).

OIPC intervenes in Province's Supreme Court of Canada legal action against Philip Morris International

The OIPC intervened on behalf of the privacy rights of British Columbians in a legal action by the Province against Philip Morris International at the Supreme Court of Canada to recover health care costs for treating tobacco-related illnesses. The tobacco manufacturer sought production of databases of health care information of British Columbians that the Province intended to use to prove causation and damages. On July 13, 2018, the Court published its decision in *British Columbia v. Philip Morris International, Inc.* that the province of BC will not be compelled to provide the personal health records of millions of British Columbians to Philip Morris.

OIPC releases guidance for private sector cannabis retailers

Prior to the legalization of recreational cannabis in October 2018, the OIPC released a guidance document to ensure retailers and purchasers understand their rights and obligations under PIPA. The guidance stresses that, in general, retailers should only collect the information necessary to complete a transaction. For example, it is not necessary to keep a copy of an individual's driver's license to verify age for purchase; simply viewing the information is sufficient. Privacy policies, staff training, and appropriate safeguards should be implemented to protect collected personal information. The guidance also cautions consumers that their personal information is being used and secured by retailers.

DOWNLOAD: *Protecting personal information: Cannabis transactions* (oipc.bc.ca).

Canadian regulators release joint resolution for privacy regulation and oversight of political parties

Political parties access and use the sensitive and personal information of nearly all Canadians, but they are only subject to privacy legislation in British Columbia. In a joint resolution, Commissioner McEvoy joined Canada's Information and Privacy Ombudspersons and Commissioners as they called on their respective governments to also pass legislation requiring political parties to comply with globally recognized privacy principles, provide Canadians with access to the personal information they hold about them, and allow for independent oversight to verify and enforce privacy compliance. The joint resolution was agreed upon at the annual meeting of federal, provincial, and territorial Information and Privacy Ombudspersons and Commissioners in September 2018.

READ: *Securing Trust and Privacy in Canada's Electoral Process* (oipc.bc.ca).

HIGHLIGHTS

OIPC order underscores importance of duty to assist

A journalist requested copies of an employee's emails in the Office of the Premier for a 12-hour period in April 2017. The Office of the Premier disclosed three pages of records and said it was not obliged under s. 6(1) (duty to assist an applicant) of FIPPA to search the employee's Recover Deleted Items folder for any other responsive records. The adjudicator found that the Office of the Premier should have searched this folder first and that it had not complied with its duty under s. 6(1). At the time of the inquiry, the requested emails were no longer in the employee's Recover Deleted Items folder because the system had automatically deleted them from that folder and saved them to a backup server. The adjudicator further found that, in view of the complexity, effort, and cost involved, the Office of the Premier was not obliged to restore the emails from the backup in order to respond to the journalist's access request.

DOWNLOAD: *Order F19-04* (oipc.bc.ca).

Order finds clinic manager not authorized to use complainant's personal information

A patient who attended a medical clinic run by the Vancouver Coastal Health Authority (VCHA) complained that the clinic's manager reviewed her medical files because he was curious after reading about her in the news. The adjudicator determined the clinic manager looked at the complainant's files because he was curious about what they might indicate about the complainant's relationship with her employer, and the clinic's relationship with her employer. The adjudicator found this was a use of the complainant's personal information that was inconsistent with the purpose for which VCHA obtained or compiled the information, and as a result it was contrary to s. 32(a) of FIPPA.

DOWNLOAD: *Order F18-27* (oipc.bc.ca).

OIPC continues role as Secretariat for Asia Pacific Privacy Authorities

The OIPC's leadership role as Secretariat for the Asia Pacific Privacy Authorities (APPA) continued throughout 2018-19. APPA's 19 members from 13 countries convene to form partnerships and exchange ideas about privacy regulation, new technologies, and the management of privacy enquiries and complaints. The OIPC joined APPA in 2010 and has served as Secretariat since July 2016, organizing twice-yearly APPA forums and chairing eight APPA Governance Committee meetings annually.

VISIT: appaforum.org

OIPC publishes letter to the City of Nanaimo re: Privacy Breach Investigation F17-72024

The City of Nanaimo has implemented several measures to improve personal information protection in response to recommendations stemming from an OIPC privacy breach investigation. In August 2018, the Commissioner found that the City had disclosed documents containing personal information without authorization under FIPPA in three separate incidents. In a letter to the City about the investigation into the disclosures, the Commissioner made recommendations on how the City could improve their personal information protection practices, underscoring that City council and officers of the City should lead by example by demonstrating commitment and support for effective privacy management. The City has designated a staff member responsible for privacy, developed a privacy management program, instituted privacy training, and adopted a privacy policy that will apply to the collection, use, and disclosure of the personal information they hold.

Commissioner ends monitoring of monthly government privacy breach reporting

Following a recommendation from the OIPC's January 2015 audit report, *An Examination of BC Government's Privacy Breach Management*, government's Privacy Compliance and Training Branch (PCTB) initiated monthly reporting of privacy breaches to the OIPC. After four years of monitoring reports from the PCTB, the Commissioner determined that the percentage of personal information breaches that could reasonably be expected to cause harm to the individual and/or involved a large number of individuals that were not reported to the OIPC was consistently low, averaging less than one percent. As a result, Commissioner McEvoy ended his request for monthly reporting by PCTB in December 2018.

FULL DISCLOSURE

AN OIPC INVESTIGATION REPORT FOUND THAT BC'S POLITICAL PARTIES SHOULD BE MORE TRANSPARENT ABOUT HOW MUCH PERSONAL INFORMATION THEY COLLECT, AND WHY.

Lawn signs and political ads typically signal the approach of an election in British Columbia. But less visible activities can also be at play, including the access and use of sensitive personal information about voters by political parties. Over the past two years, the public's attention has been heightened about the misuse of personal information for political campaigning. Cambridge Analytica's manipulation of Facebook data to psychologically profile US voters is one example that sent shockwaves around the world.

British Columbia is the only Canadian province that regulates the privacy practices of political parties. Commissioner Michael McEvoy and his counterparts have called on legislators across the country to ensure that Canadian law at all levels carries meaningful privacy obligations for political parties. The OIPC received complaints about how BC's three main political parties treated the personal information they collected. Under the authority of BC's *Personal Information Protection Act* (PIPA) Commissioner McEvoy decided to open an investigation to examine the kinds of personal information BC's three main political parties were collecting from the province's 3.3 million registered voters—and what they were doing with it.

"While a functioning democracy necessitates that political parties understand the aspirations of voters in order to effectively communicate with them, there are rules in place in BC about how far parties can go in collecting, using, and disclosing the personal information of individuals," says Commissioner McEvoy.

"These two interests are not inherently at odds when a political party clearly explains to a voter why they are collecting their personal information and how they intend to use it."

In the OIPC investigation, however, the Commissioner found that political parties aren't doing enough to explain to individuals how much personal information they collect — and why.

"Some of the issues arising from the collection of information came from observations made and recorded about a person by a canvasser going door-to-door. Other examples included 'scraping' personal information from social media platforms and disclosing donor lists, birthdates, and other data to Facebook. To be absolutely clear, political parties may be allowed to collect and use this kind of information. However, in most circumstances, the political party would need to get that individual's consent," says Commissioner McEvoy.

The report also examined how political parties retain and protect the personal information they collect. Although all three political parties develop and publish privacy policies, investigators found a number of deficiencies with retention and audit practices that prevent full compliance with PIPA.

The OIPC found all of the political parties had inadequate privacy training and indefinite retention of the information. "This, combined with the vast amount of sensitive personal information collected, leaves political parties, and by default voters, vulnerable. Political parties must ensure the same effort goes into protecting personal information as is put into collecting it," says Commissioner McEvoy.

The report recognizes the rapid advancement of technological tools to profile and micro-target voters and the risks these developments could pose for BC's citizens and its democratic system of governance. Its findings and recommendations aim to protect citizens by improving the privacy management practices of all parties in the province, whether represented in the legislature or not. It is important that these findings and recommendations are not viewed in isolation. British Columbia's Chief Electoral Officer has the wide-ranging responsibility for the conduct and administration of provincial election matters.

"A number of the issues raised in this report are best accomplished by coordination between our two offices," concludes Commissioner McEvoy. "BC's Chief Electoral Officer is of the same view, and I look forward to working with his office." ■

DOWNLOAD: Investigation Report P19-01: *Full Disclosure: Political parties, campaign data, and voter consent.*

GETTING PrivacyRight

OIPC LAUNCHES EDUCATIONAL PROGRAM TO HELP BC ORGANIZATIONS BETTER PROTECT PERSONAL INFORMATION.

Hundreds of thousands of organizations in British Columbia collect, use, or disclose people's personal information. That personal information is one of an organization's most valuable assets. Protecting it is not only a legal obligation, it's simply good business. It's about trust.

In early 2019, the OIPC launched its largest-ever public education program in response to a growing number of requests from organizations who wanted to do more to protect personal information. In some cases, organizations weren't even sure where to begin.

PrivacyRight aims to demystify privacy management and help organizations understand their obligations under the *Personal Information Protection Act* (PIPA). The program consists of a comprehensive suite of tools that span a range of digital platforms, including animated webinars, videos, guidance documents, and a fictionalized podcast based on real files seen by our office.

PrivacyRight takes a fun, engaging approach to show that effective privacy management doesn't need to be a complex matter. Monthly releases throughout 2019 will offer practical, step-by-step guidance on everything from basic obligations under PIPA to writing a privacy policy, issues around consent and notification, ensuring effective security safeguards, and more.

Taken as a whole, the suite of PrivacyRight tools offer businesses a way to "privacy-proof" their operations—to address potential pitfalls before a breach occurs, and take effective action if it does. They also empower consumers to better understand their privacy rights and the actions they can take when they're unsure about how much information an organization can legally request or how their data is being used.

The PrivacyRight materials were designed for the small business community. Information about the program is included in welcome materials sent to people registering businesses in British Columbia. Monthly PrivacyRight updates are also spotlighted in the Better Business Bureau of BC's Accredited Business Newsletter, which is sent to more than 4,400 members.

"We're committed to expanding the reach of PrivacyRight content," says Commissioner McEvoy. "And we're serious about supporting organizations throughout British Columbia in their efforts to safeguard the personal information they hold and the trust they work so hard to build." ■

VISIT: To view PrivacyRight materials and sign up for updates, visit: https://www.oipc.bc.ca/privacyright/

PRIVACY GUARDIANS

THE OIPC'S COLLABORATION WITH NATIONAL AND INTERNATIONAL REGULATORS IS CRITICALLY IMPORTANT IN THE DIGITAL AGE.

Isolation is not an option when it comes to effective data privacy protection in the digital age. The Facebook-Cambridge Analytica scandal drove home that reality, with its reverberations felt around the world, including here in British Columbia. The challenges that come with complex international data flows demand a concerted effort among regulators entrusted to protect citizens' personal information.

Over the past year, the OIPC has played a significant role in assisting coordinated Canadian and international actions. "Collaborating with other privacy guardians is of fundamental importance if we are to properly serve and protect the interests of British Columbians," says Information and Privacy Commissioner Michael McEvoy. "And that means taking action — pushing forward the regulatory changes we need in response to challenges to people's privacy that will only intensify."

The OIPC has worked closely with the Commissioners of Alberta and Canada on joint investigations since 2004. Most recently, the OIPC and Privacy Commissioner of Canada launched joint investigations into Facebook and AggregateIQ, casting an important spotlight on issues that impact the everyday lives of Canadians and all people navigating social media.

The OIPC also joins its national and provincial counterparts in taking collective action on issues related to access and privacy. In September 2018, for example, the regulators signed a joint letter urging legislators across Canada to bring political parties under privacy legislation. BC is a leader in this regard, as the province's *Personal Information Protection Act* is the only privacy legislation in the country that covers political parties' collection of personal information.

The OIPC is also active on the global stage, playing a key role in two key international privacy associations: the Asia Pacific Privacy Authorities (APPA) and the Global Privacy Enforcement Network (GPEN).

APPA serves as the primary forum for privacy and data protection authorities in the Asia-Pacific, a significant trading region for BC businesses. Founded in 1992 and comprising 19 members from 13 countries, APPA is a vital platform for cooperation and enforcement actions in the region. The OIPC has led APPA's Secretariat and Governance Committee since 2016. This collaboration and collective action enables the OIPC to better address challenges that result when British Columbians' data is shared across borders.

GPEN was founded in 2010 to facilitate cross-border cooperation in the enforcement of privacy laws. GPEN today has 69 members and achieves its goals through advocacy, enforcement, and communications efforts.

GPEN's annual Privacy Sweeps provide a snapshot of emerging privacy issues. Most recently, GPEN regulators, including the OIPC, asked more than 600 organizations in 18 countries about how they handled personal information, highlighting a clear need for improvement.

"By engaging in a broad conversation about privacy and access, the OIPC is better able to meet the challenges facing us with rapidly changing technology," says Commissioner McEvoy. ■

YEAR IN NUMBERS

TABLE 1. Year in Numbers Summary of all FIPPA and PIPA files received in 2018-2019

FILE TYPE	Received 18/19	Closed 18/19	Received 17/18	Closed 17/18
Privacy breach notification (includes monthly government breach reviews)	205	209	186	195
Privacy complaints	332	322	273	260
Access to information				
Access complaints	406	443	439	379
Requests for review of decisions to withhold information	458	521	506	389
Deemed refusal	199	176	160	167
Applications to disregard requests as frivolous or vexatious	13	12	7	10
Time extensions				
Requests by public bodies and private organizations	3,854	3,859	1,638	1,633
Requests by applicants seeking a review	21	24	34	31
Reconsideration of OIPC decisions	51	37	60	53
Public interest notification (s.25)	20	18	16	17
Information requested/received				
Requests for information and correspondence received	5,481	5,483	4,669	4,666
Non-jurisdictional issue	13	13	23	21
No reviewable issue	118	105	97	93
Media inquiries	135	127	166	160
FOI requests for OIPC records	18	18	15	15
Adjudications of OIPC decisions	4	2	0	0
OIPC initiatives				
Audit and Compliance	4	4	3	3
Investigations	17	16	15*	8*
Legislative reviews	42	50	20	18
Projects	19	23	27	22
Policy or issue consultation	392	417	206	189
Police Act IIO reports	44	43	21	22
Privacy impact assessments	94	95	48	42
Public education and outreach				
Speaking engagements	48	37	42	40
Meetings with public bodies and private organizations	73	64	33	29
Other (s. 56, internal reviews, and research agreement complaint)	87	92	87	91
TOTAL	**12,148**	**12,210**	**8,791**	**8,553**

* **NOTE:** The numbers above have been adjusted because, prior to fiscal 2018-19, Audit and Compliance investigations were accounted for under Investigations.

TABLE 2. Orders issued in 2018-2019

Total orders	59

TABLE 3. Breakdown of access complaints received in 2018-2019 (FIPPA and PIPA)

Duty required by Act	104
Time extension by public body	23
Adequate search	211
Fees	59
No notification issued	9
Total	**406**

NOTE:

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

TABLE 4. Breakdown of privacy complaints received in 2018-2019 (FIPPA and PIPA)

Accuracy	10
Collection	110
Use	14
Disclosure	114
Retention	12
Correction	48
Protection	24
Total	**332**

NOTE:

Complaints allege:

Accuracy: Where personal information in the custody or control of a public body is inaccurate or incomplete.
Collection: The unauthorized collection of information.
Correction: Refusal to correct or annotate information in a record.
Disclosure: Unauthorized disclosure by a public body or private organization.
Retention: Failure to retain information for the time required.
Use: Unauthorized use by the public body or private organization.
Protection: Failure to implement reasonable security measures.

YEAR IN NUMBERS

TABLE 5. Number of FIPPA complaints and requests for review received in 2018-19 by public body

Public Body	Complaints received	Requests for review received	Total
Insurance Corporation of British Columbia	31	34	**65**
Ministry of Finance	23	35	**58**
City of Vancouver	19	32	**51**
Vancouver Island Health Authority	27	20	**47**
University of British Columbia	11	28	**39**
Ministry of Children and Family Development	14	21	**35**
WorkSafe BC	21	10	**31**
Vancouver Police Department	10	19	**29**
Ministry of the Attorney General	5	24	**29**
Ministry of Forests, Land, Natural Resource Operations and Rural Development	10	17	**27**
Top 10 totals	**171**	**240**	**411**
All other public bodies	346	360	**706**
Total	**517**	**600**	**1117**

NOTE:

The number of requests for review and complaints against a public body does not necessarily indicate non-compliance. It may instead 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 lawsuits.

TABLE 6. Number of PIPA complaints and requests for review received in 2018-19 by sector

Sector	Complaints received	Requests for review received	Total
Services	78	10	88
Health	44	16	60
Real estate	20	5	25
Professional science and development	13	2	15
Finance/insurance	8	5	13
Administrative support	12	0	12
Retail trade	7	4	11
Accommodation	5	3	8
Construction	7	1	8
Education	6	1	7
Top 10 total	**200**	**47**	247
Other	21	10	31
Total	**221**	**57**	**278**

TABLE 7. Outcome of access complaints resolved in 2018-19, FIPPA

Type	Investigation	No investigation	Hearing or report	Total
Adequate search	57	131	3	**191**
Duty	46	50	2	**98**
Fees	34	21	3	**58**
Time extension by public body	20	4	0	**24**
S 25 not applied	7	6	0	**13**
TOTAL	**164**	**212**	**8**	**384**

NOTE:

Investigation: Includes files that were mediated, not substantiated, partially substantiated, and substantiated.
No investigation: Includes files referred back to public body, withdrawn, or files the OIPC declined to investigate.
Hearing or report: Refers to files that proceeded to inquiry and/or a report was issued.

TABLE 8. Outcome of access complaints resolved in 2018-19, PIPA

Type	Investigation	No investigation	Hearing or report	Total
Adequate search	11	18	0	**29**
Duty	12	11	0	**23**
Fees	4	3	0	**7**
Extension by organization	0	0	0	**0**
TOTAL	**27**	**32**	**0**	**59**

NOTE:

Adequate search: Failure to conduct an adequate search for records.
Duty: Failure to fulfill any duty required except adequate search.
Fees: Unauthorized or excessive fees assessed by the public body or private organization.
Time extension: Unauthorized time extension taken by public body or private organization.

TABLE 9. Outcome of privacy complaints resolved in 2018-19, FIPPA

Type	Investigation	No investigation	Hearing or report	Total
Accuracy	0	7	0	**7**
Collection	11	28	1	**40**
Correction	9	22	0	**31**
Disclosure	23	27	0	**50**
Retention	6	2	0	**8**
Use	3	4	0	**7**
Protection	4	11	0	**15**
Total	**56**	**101**	**1**	**158**

NOTE:

Accuracy: Where personal information in the custody or control of a public body is inaccurate or incomplete.
Collection: The unauthorized collection of information.
Correction: Refusal to correct or annotate information in a record.
Disclosure: Unauthorized disclosure by a public body or private organization.
Retention: Failure to retain information for the time required.
Use: Unauthorized use by the public body or private organization.
Protection: Failure to implement reasonable security measures.

TABLE 10. Outcome of privacy complaints resolved in 2018-19, PIPA

Type	Investigation	No investigation	Hearing or report	Total
Accuracy	1	2	0	**3**
Collection	20	47	3	**70**
Correction	5	10	0	**15**
Disclosure	24	30	0	**54**
Retention	6	2	0	**8**
Use	1	5	0	**6**
Protection	3	5	0	**8**
TOTAL	**60**	**101**	**3**	**164**

NOTE:

Accuracy: Where personal information in the custody or control of a public body is inaccurate or incomplete.
Collection: The unauthorized collection of information.
Correction: Refusal to correct or annotate information in a record.
Disclosure: Unauthorized disclosure by a public body or private organization.
Retention: Failure to retain information for the time required.
Use: Unauthorized use by the public body or private organization.
Protection: Failure to implement reasonable security measures.

TABLE 11. Outcome of requests for review resolved in 2018-19, FIPPA

Type	Mediated/resolved	Declined to investigate/ discontinue	Hearing/ consent order/ other	Total
Accuracy		1		**1**
Deemed refusal	127	6	9	**142**
Deny	76	8	34	**118**
Notwithstanding	0	0	0	**0**
Partial access	243	7	63	**313**
Refusal to confirm or deny	8	0	1	**9**
Scope	9	1	5	**15**
Third party	34	0	12	**46**
S. 25 Review	0	0	0	**0**
Total	**497**	**23**	**124**	**644**

NOTE:

Mediated/resolved: Includes files that were mediated, withdrawn, referred to public body, consent order, or other decision by Commissioner.

YEAR IN NUMBERS

TABLE 12. Outcome of requests for review resolved in 2018-19 PIPA

Type	Mediated/ resolved	Declined to investigate/ discontinue	Hearing/ consent order/ other	Total
Deemed refusal (no response within 30 days)	30	4	0	**34**
Deny access (all records denied)	8	1	0	**9**
Notwithstanding (other Act prevails)	0	0	0	**0**
Partial access (some records provided)	6	1	3	**10**
Refusal to confirm or deny (the existence of records)	0	0	0	**0**
Scope (PIPA does not apply)	0	0	0	**0**
Totals	**44**	**6**	**3**	**53**

NOTE:

Mediated/resolved: Includes files that were mediated, withdrawn, referred to public body, consent order, or other decision by Commissioner.

TABLE 13. Outcome of all complaints resolved by the OIPC (FIPPA and PIPA) in 2018-2019

Investigations	No investigations	Declined to investigate/ discontinued	Hearing or report	Total
307	60	386	12	**765**

NOTE:

Investigation: Includes files that were mediated, not substantiated, partially substantiated, and substantiated.
No investigation: Includes files referred back to public body, withdrawn, or files the OIPC declined to investigate.
Hearing or report: Refers to files that proceeded to inquiry and/or a report was issued.

TABLE 14. Outcome of all requests for review resolved by the OIPC (FIPPA and PIPA) in 2018-2019

Mediated/ resolved without hearing	Hearing or report	Declined to investigate/ discontinued	Total
541	127	29	**697**

NOTE:

Investigation: Includes files that were mediated, not substantiated, partially substantiated, and substantiated.
No investigation: Includes files referred back to public body, withdrawn, or files the OIPC declined to investigate.
Hearing or report: Refers to files that proceeded to inquiry and/or a report was issued.

How to make a freedom of information request

In British Columbia, access to information and privacy rights are governed by the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). These laws are enforced by BC's Information and Privacy Commissioner.

FIPPA gives you the right to access records held by public bodies, including your own personal information. PIPA applies to private sector organizations and gives you the right to access your own personal information.

OUR PROCESSES

How to make a complaint

If you need help resolving a privacy complaint, or are not getting access to records you believe should be disclosed, you can submit a complaint to the Office of the Information and Privacy Commissioner for BC.

STEP 1 | ATTEMPT TO RESOLVE THE COMPLAINT

First, work directly with the public body or organization to try to resolve the complaint. Submit your complaint in writing, providing as much detail as possible, including how they did not comply with FIPPA or PIPA. Allow the public body or organization 30 days to respond.

STEP 2 | PREPARE YOUR COMPLAINT

If Step 1 is unsuccessful, you can complain to our office. Determine whether you are making a **privacy complaint** or an **access complaint**. Visit **oipc.bc.ca** for additional information about how to prepare your submission based on the type of complaint.

STEP 3 | SUBMIT YOUR COMPLAINT

Send us a concise description of the circumstances that led to your complaint. If you are making an **access complaint**, provide a copy of your original request and any response you received. If you are making a **privacy complaint**, include all correspondence and documentation.

STEP 4 | WHAT HAPPENS NEXT

If your complaint is accepted, we will assign it to an investigator, who will review the evidence and mediate the dispute by making a finding and recommendations. If mediation is unsuccessful, your file may proceed to **inquiry** for adjudication, which will result in a legally binding order.

How to make a request for review

If you submitted a freedom of information request and believe that you have been improperly denied access to information, you can ask us to review the decision.

STEP 1 | WHAT YOU CAN DO

You can make a **request for review** if you do not receive a response within 30 business days, were denied access to records, or disagree with a redaction. You have 30 business days to request a review.

STEP 2 | WHAT YOU NEED

Include a copy of your original access request, the response, any correspondence that shows that you tried to resolve the matter, plus your written request for a review of the decision. Include the reasons you believe the decision did not comply with FIPPA or PIPA.

STEP 3 | WHAT HAPPENS NEXT

If you were denied access, we will work with the public body or organization to get you a response. With other requests, we may assign an investigator to examine the records in dispute and the public body or organization's rationale for denying you access to them.

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 500,000 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 the Registrar of Lobbyists and oversees and enforces 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.

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:

2018-19	Operating	Capital
Appropriation	$6,252,000	$45,000
Total operating expenses	$6,160,271	-
Capital acquisitions	-	$30,762
Unused appropriation	$91,729	$14,238

2017-18	Operating	Capital
Appropriation	$6,064,000	$45,000
Total operating expenses	$5,912,198	-
Capital acquisitions	-	$28,109
Unused appropriation	$151,802	$16,891

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).

2018-19	Closing cost	Closing accumulated amortization	Net book value (March 31/19)
Computer hardware and software	$338,661	-296,370	$42,291
Tenant improvements	$552,302	-$552,302	-
Furniture and equipment	$98,400	-$90,213	$8,187
Total tangible capital assets	$989,363	-$938,717	$50,646

2017-18	Closing cost	Closing accumulated amortization	Net book value (March 31/18)
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
Total tangible capital assets	$958,600	-$910,946	$47,654.58

OUTREACH

Commissioner McEvoy launches the Office's PrivacyRight education program for BC organizations at a Greater Victoria Chamber of Commerce event on March 7, 2019.

Commissioner McEvoy and OIPC staff are frequent speakers and participants at events and conferences throughout BC, across Canada, and around the world.

The OIPC is mandated under FIPPA and PIPA to carry out public education.

The following are examples of some of these speaking engagements and conferences during the 2018-19 fiscal year:

- BC Aware Day Conference, Vancouver
- BC FIPA InfoSummit, Vancouver
- Canadian Bar Association, Privacy and Access Section, Vancouver
- Canadian College of Health Leaders, Victoria
- Canadian Information Processing Society, Victoria
- Greater Victoria Chamber of Commerce, Victoria
- IAPP Canada Privacy Symposium, Toronto
- IAPP Global Privacy Summit, Washington DC
- Municipal Finance Authority of BC, Victoria
- Social Media Camp, Victoria
- Standing Committee on Access to Information, Privacy and Ethics, Ottawa, ON
- Thompson Rivers University Privacy Conference, Kamloops
- 20th Annual Privacy and Security Conference, Victoria
- University of Alberta Access and Privacy Conference, Edmonton

RESOURCES

Getting started

- Access to data for health research
- BC physician privacy toolkit
- Guide to OIPC processes (FIPPA and PIPA)
- Guide to PIPA for business and organizations
- Guide to FIPPA for individuals
- Developing a privacy policy under PIPA
- Early notice and PIA procedures for public bodies
- Privacy Management Program self assessment
- Access (General)
- Guidelines for conducting adequate search investigations (FIPPA)
- How do I request records?
- How do I request a review?
- Instructions for written inquiries
- 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 information

Privacy (General)

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

Comprehensive privacy management

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

Privacy breaches

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

PrivacyRight

- Your basic obligations under PIPA: PrivacyRight Webinar 1
- 10 steps to develop a privacy management program: PrivacyRight Webinar 2
- How to write a privacy policy: PrivacyRight Webinar 2b

Technology and social media

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

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

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 B.C.: 1.800.663.7867

Email: info@oipc.bc.ca

@BCInfoPrivacy

oipc.bc.ca