Office of the Information and Privacy Commissioner for British Columbia

ANNUAL REPORT 2019-2020

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

WHO WE ARE

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

- The ***Freedom of Information and Protection of Privacy Act*** (FIPPA), which applies to over 2,900 "public bodies," including ministries, local governments, schools, crown corporations, hospitals, municipal police forces, and more; and
- The ***Personal Information Protection Act*** (PIPA), which applies to any private sector organization 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.

OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

TABLE OF CONTENTS

August 2020

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, 2019 to March 31, 2020.

Yours sincerely,

Michael McEvoy
Information and Privacy Commissioner for British Columbia

COMMISSIONER'S MESSAGE

I am pleased to present the 2019-20 annual report for the Office of the Information and Privacy Commissioner for British Columbia.

Past reports have highlighted the incredible pace of technological change and its impact on privacy and information rights in BC. During this past fiscal reporting year, my office has witnessed an exponential surge in this trajectory.

The impacts of the COVID-19 pandemic have amplified society's digital universe: from BC businesses and public bodies expanding online services and employees working from home to educators delivering remote learning to students. With more of our everyday transactions taking place online, we need a digital and information infrastructure in place that we can trust.

The rules regulating the conduct of organizations and public bodies must be sufficiently robust, so that the public can confidently navigate and participate in our modern economy and government systems. But BC's access to information and protection of privacy legislations, at one time state of the art, are no longer fit for purpose.

So much has changed since the province's two pieces of privacy legislation were first introduced. For example, when the *Freedom of Information and Protection of Privacy Act* was enacted nearly 30 years ago, privacy breaches affected relatively small groups of individuals and were most often the outcome of things like misplaced files and briefcases. In our digital age, a privacy breach can occur with a click of a mouse and can affect tens of thousands, even millions of individuals.

Additionally, organizations and public bodies are collecting and storing vast amounts of our personal information – often to create profiles of us with the amassed data. Profiling can predict future behaviour, to help marketers sell us something, but it could just as easily be used to deny an insurance product or assess eligibility for a government program.

We are at an inflection point with these technological, societal, and economic changes. To keep pace, we must reform BC's privacy and access to information laws.

Our investigations over the last year further underscore the need for change. Take, for example, the Facebook/ Cambridge Analytica scandal of 2018. This privacy breach affected 622,000 users in Canada, including 92,000 in British Columbia. As news of the breach spread around the world, people began to realize how readily their personal information could be misappropriated and misused. My office opened an investigation into the actions of the social media giant with the Office of the Privacy Commissioner of Canada (OPC). Our joint inquiry found major shortcomings in the company's privacy practices and concluded that Facebook contravened BC and Canadian privacy laws.

In a related joint investigation with the OPC, Federal Commissioner Daniel Therrien and I found that Victoria-based tech firm AggregateIQ (AIQ) violated BC and Canadian privacy laws when it used the personal information of millions of people — including sensitive data such as psychological profiles — to "microtarget" them for political campaign ads in Canada, the United States, and the United Kingdom.

In other jurisdictions, such behaviour might be subject to significant sanctions, like fines. Here in BC, this is not the case. Imposing a fine was not an option with either company because our private sector privacy law does not provide such deterrence.

At least, not yet.

BC`s Special Committee to Review the *Personal Information Protection Act* meets every six years to discuss reforms to the Act. This is one of those years. It is my hope that mandatory breach notification will be introduced as a result of the review, so people know when their personal information has been breached. BC is virtually alone in North America as a jurisdiction without mandatory breach notification laws. Significant penalties would also serve as a disincentive for bad actors and an incentive for companies to invest in proper privacy and security for their clients, customers, and patients.

With a modern privacy law, businesses can reassure customers, and each other, that privacy rights are being meaningfully protected. This is especially important when organizations handle highly sensitive personal health information. In December 2019, the lab testing company LifeLabs revealed that its computer system had suffered a cyberattack involving the personal health information of millions of Canadians. This massive breach is the subject of our joint investigation with the Ontario Information and Privacy Commissioner's Office.

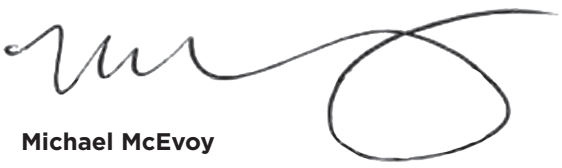
These high profile breaches not only adversely impact the people whose personal information is compromised; they also erode citizens' trust in the ability of organizations and public bodies to protect their data. Legislative reform that allows regulators to impose financial penalties on companies that violate people's privacy rights would go a long way towards restoring that trust.

In addition to joint investigations and other undertakings with Canadian colleagues, I'm also proud of our office's leading role with international privacy organizations. International collaboration is a necessity in an age when data knows no boundaries — and it has been especially urgent during this global pandemic. Throughout 2019-20, we continued our leadership role as Secretariat for the Asia Pacific Privacy Authorities (APPA). My office has served in this capacity since 2016, organizing twice-yearly forums for the 19-member organization and serving as a platform to share information about common investigatory matters as well as exchanging ideas about emerging privacy issues, new technologies, and the management of privacy enquiries and complaints. Our office's role in APPA is especially relevant, given that so many of BC's trade relationships are within the Asia Pacific region. I remain grateful to the Finance and Governance Committee for continuing to support this initiative.

The statistics provided within this report detail the significant volume of access and privacy matters that we continue to investigate, mediate, and adjudicate. However, it also remains an important part of our work to provide guidance, outreach, and education for organizations, public bodies, and the public at large. This has been especially so during the COVID-19 pandemic. We have given guidance on everything from tips for public bodies and organzations setting up remote work locations to helping food and drink establishments with the "what" and "how" to collect personal information for potential exposure notification of customers. I'm also especially proud of my office's private sector educational program, PrivacyRight, that ran throughout 2019-20 to help organizations large and small understand their privacy obligations.

BC's access and privacy laws serve two purposes: they promote access to information to individuals and citizens and they ensure personal information is properly secured and protected. During this past fiscal year, a number of our high-profile investigations dealt with privacy issues. At the same time, our office continues to resolve hundreds of matters between citizens and public bodies, through which they seek information and, in many instances, to hold government accountable for their actions. In the coming year, my office will release our report card on just how well government is doing in their response to those access requests.

I would like to close by acknowledging my staff, who continue to provide uninterrupted service to British Columbians during these uncertain times. The public is extremely well served by the dedication, expertise, and high ethical standards that each member of the OIPC team brings to their work. I am deeply appreciative of their efforts over the past year.



Michael McEvoy
Information and Privacy Commissioner for British Columbia

OUR TEAM

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

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; investigates access and privacy complaints; comments on the implications of new programs, policies, and technologies on access and privacy rights; collaborates with national and international regulators; and engages in public education and outreach activities.

Case review

Case review officers help individuals file complaints relating to access and privacy 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 assist in early resolution of complaints and grant or deny public bodies' 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 legally binding decisions. Orders are subject to review by the BC Supreme Court.

Policy

Policy analysts research and analyze current and emerging access and privacy issues, 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 the compliance of organizations and public bodies with BC's privacy and access laws, conducts systemic investigations, 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 dedicated staff committed to service

A team of 42 people worked at the Office of the Information and Privacy Commissioner in 2019-20. An additional 18 Corporate Shared Services staff 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.

We celebrate our staff's commitment to public service with an OIPC long service program. These awards are presented annually at five-year increments. For the 2019-20 fiscal year, we distributed Long Service certificates to two individuals: one received a five-year certificate and one received a 25-year certificate for their service to the people of British Columbia through our office.

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 2019 PECSF campaign: Highest Participation Rate and Highest Average Donation for a small entity.

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.

HIGHLIGHTS

OIPC and federal privacy commissioner find Facebook, Inc. violated Canadian and BC privacy laws

Commissioner McEvoy and Privacy Commissioner of Canada Daniel Therrien's investigation into Facebook found major shortcomings in the company's privacy practices and concluded that Facebook contravened Canadian and British Columbian privacy laws. The investigation focused on the social media giant's global privacy breach that affected 622,000 Canadian users of Facebook between November 2013 and December 2015, including 92,000 users in British Columbia. The company disputed the commissioners' findings and refused to implement recommendations to address deficiencies. The Office of the Privacy Commissioner of Canada has taken Facebook to Federal Court, seeking an order to force the company to correct its privacy practices. The report and subsequent legal action highlight critical weaknesses within the current Canadian privacy protection framework and underscore an urgent need for stronger privacy laws.

READ: *Breach of trust, p. 14*

DOWNLOAD: *Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia* (oipc.bc.ca).

OIPC and federal privacy commissioners find AggregateIQ Data Services Ltd. microtargeted citizens without consent

Victoria-based tech firm AggregateIQ Data Services Ltd. (AIQ) violated BC and Canadian privacy laws when it used the personal information of millions of people — including sensitive data such as psychological profiles — to "microtarget" them for political campaign ads in Canada, the United States and the United Kingdom. This was the main finding of a joint investigation by Commissioner McEvoy and federal Privacy Commissioner Daniel Therrien. The investigation into AIQ's compliance with BC's *Personal Information Protection Act* (PIPA) and Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) highlighted the firm's failure to obtain consent for the use and disclosure of people's personal information when delivering microtargeted ads. Commissioners McEvoy and Therrien also concluded that AIQ failed to properly protect the personal information in its custody. AIQ agreed to address these issues and to follow all of the Commissioners' recommendations.

READ: *A question of consent, p. 16.*

DOWNLOAD: *Investigation report P19-03 Pipeda-035913 AggregateIQ Data Services Ltd.* (oipc.bc.ca).

HIGHLIGHTS

OIPC order establishes jurisdiction under PIPA for federal riding association operating in BC

An applicant made a complaint under PIPA about the use of their personal information by a federal electoral district association: the Courtenay-Alberni Riding Association of the federal New Democratic Party of Canada. The organization argued that PIPA did not apply to federally registered political entities because the federal *Personal Information Protection and Electronic Documents Act*, the *Canada Elections Act* and other federal statutes prevail over BC's PIPA. The Commissioner found on constitutional grounds that PIPA does apply to the organization's collection, use or disclosure of the complainants' personal information. He ordered a further hearing in this inquiry, to consider the merits of the complainants' allegations (P20-02).

DOWNLOAD: *Order P19-02* (oipc.bc.ca).

Review of private medical clinics finds privacy safeguards lacking

Medical clinics handle some of our most sensitive personal information, making robust privacy management a legal and ethical necessity. An OIPC review of 22 medical clinics throughout British Columbia found, however, that many are falling behind when it comes to protecting personal information and meeting their legal obligations under PIPA. The report identified common gaps in clinics' privacy management programs and provided 16 recommendations on how medical clinics can improve their practices.

READ: *Prescription: Privacy protection p. 20*

DOWNLOAD: *Audit and Compliance Report P19 01: Compliance Review of Medical Clinics* (oipc.bc.ca).

OIPC podcast helps stratas get PrivacyRight

There are many privacy concerns for strata councils, from sensitive issues discussed at council meetings and in strata correspondence to rules governing surveillance and challenges of safeguarding personal information in the digital age. This podcast was developed as part of the OIPC`s PrivacyRight education program in response to a growing number of calls, queries, and complaints related to privacy rights and obligations at strata complexes. The OIPC spoke to those who deal with these issues on a daily basis, including the heads of the Condominium Homeowners Association, the Vancouver Island Strata Owners Association, and a property management firm. Commissioner McEvoy helped clarify stratas' obligations under BC's privacy laws and outlined how the OIPC can help.

DOWNLOAD: *Podcast helps stratas protect personal information and avoid privacy pitfalls* (oipc.bc.ca).

LISTEN: *PrivacyRight podcast 3 – Strata privacy: Rights, cameras and taking action* (anchor.fm)

Canadian regulators release joint resolution urging need for legislative reforms

While new technologies offer potential benefits to society, they can also potentially impact fundamental democratic principles and human rights, including privacy, access to information, freedom of expression, and electoral processes. With security breaches often affecting millions of users, the public is becoming more and more concerned about the use and exploitation of their personal information. In a joint resolution, Commissioner McEvoy joined Canada's information and privacy commissioners and ombudspersons to call on their respective governments to modernize privacy legislation to better protect Canadians.

DOWNLOAD: *Effective Privacy and Access to Information Legislation in a Data Driven Society* (oipc.bc.ca).

HIGHLIGHTS

Commissioner releases remote work guidance for public bodies and organizations

The sudden shift to remote work for many British Columbians brought on by the COVID-19 outbreak resulted in pressing concerns around privacy and the protection of personal information. The OIPC issued tips and resources for public bodies and organizations when setting up remote workspaces for their employees. The guidance, which was broadly distributed through media outlets and the OIPC website, provides a timely reminder that care must be taken to protect personal information when it leaves the worksite.

DOWNLOAD: *Tips for public bodies and organizations setting up remote workspaces* (oipc.bc.ca).

OIPC continues vital collaboration with international regulators

International collaboration is a necessity in an age when data knows no borders — and especially urgent during a global pandemic like COVID-19. The OIPC continued its leadership role as Secretariat for the Asia Pacific Privacy Authorities (APPA) throughout 2019-20. The office has served in this capacity since 2016, organizing twice-yearly forums where 19 APPA members from 13 countries gather to form partnerships and exchange ideas about privacy regulations, new technologies, the management of privacy enquiries and complaints, and emerging privacy issues. In addition, the OIPC continues to participate with regulators from around the world who are members of the Global Privacy Enforcement Network (GPEN) and also organizes and chairs regional conference calls. Together, the 70 members conduct privacy "sweeps" and take part in advocacy, enforcement, and communications efforts.

OIPC releases privacy impact assessment template and guidance

Businesses must build safeguards to protect privacy into every initiative that will involve the collection, use, or disclosure of personal information. On Data Privacy Day, January 28, 2020, Commissioner McEvoy launched the OIPC's privacy impact assessment (PIA) template and related guidance to help businesses gain a comprehensive understanding of the privacy implications of all aspects of their planned initiatives, so they can meet their legal requirements under the *Personal Information Protection Act*. The PIA template and related guidance help businesses ask the right questions and chart the flow of personal information within their organization.

DOWNLOAD: *PIA guidance, PIA Template* (oipc.bc.ca).

Guidance offers advice to retailers about privacy protection

The OIPC guidance document *Privacy-proofing your retail business* addresses some of the most frequently asked questions when it comes to private organizations' legal obligations to protect personal information. Launched as part of the OIPC's PrivacyRight education campaign, the guidance aims to help retail businesses understand their obligations under PIPA and outlines best practices.

DOWNLOAD: *Privacy-proofing your retail business: FAQ and tips for protecting customers' personal information*

OIPC issues guidance on personal information disclosures in emergencies

A common misconception is that BC's privacy laws can delay or prevent the sharing of information that could potentially save someone's life in an emergency situation. The OIPC guidance document *Disclosure of personal information of individuals in crisis* makes clear, however, that BC's privacy laws are designed to facilitate the responsible disclosure of personal information in these cases. The guidance provides information for public bodies and private sector organizations on the circumstances under which the legislation allows them to disclose an individual's personal information in emergency situations.

DOWNLOAD: *Disclosure of personal information of individuals in crisis* (oipc.bc.ca).

HIGHLIGHTS

Duty to document allegation highlights flaw in FIPPA

The former Minister of Citizens' Services was the subject of allegations that she had failed in her duty to document important government decisions. The OIPC did not have oversight of the matter. The *Information Management Act* designates the Minister as the authority responsible for ensuring her own ministry's compliance with its duty to document. In a statement, Commissioner McEvoy said that this falls short of the independent oversight required to ensure public trust and accountability and called for reforms to FIPPA to give the OIPC oversight of the duty to document. The Commissioner also underscored that while FIPPA does not explicitly prohibit the use of personal communication tools for public business, it is a poor practice and a threat to the proper documentation of government decisions.

DOWNLOAD: *Statement from BC Information and Privacy Commissioner regarding independent oversight over government's duty to document and use of personal communication tools* (oipc.bc.ca).

Order rejects government's attempt to block opposition access requests

Access to information rights are a pillar of accountable government, and FIPPA gives the public the right to access any record in the custody or under the control of a public body subject only to specified exceptions. In this case, the Official Opposition had made 615 requests for access to the emails of government ministers and employees who were using their personal emails to conduct government business. The BC Government and the Office of the Premier requested authorization to disregard the access requests. The adjudicator rejected the government's contention that the requests were "frivolous and vexatious," under s. 43(2)(b) of FIPPA, noting that the Opposition had a legitimate reason for making them. The adjudicator said that the use of personal email accounts for government business has the potential to undermine the public's ability to hold a public body to account since it makes it harder for public bodies to search for and produce the requested records, and employees may be unwilling to produce records from their personal accounts or allow access to their accounts for that purpose.

DOWNLOAD: *Order F19-34* (oipc.bc.ca).

Order confirms Ministry of Finance's right to collect SINs for Speculation Tax

British Columbians have the right to ask questions when new government initiatives require their personal information. They also have the right to file complaints with the OIPC when they believe that collection, use and disclosure is unlawful. The OIPC received two complaints about the requirement that residential property owners provide their social insurance number (SIN) on the declaration form for the Province's newly introduced Speculation and Vacancy Tax. The OIPC also received correspondence from the public expressing concerns about the requirement to provide other types of personal information on the declaration form, such as name, date of birth, address and email. Following an inquiry, the adjudicator issued an order stating that FIPPA authorized the Ministry of Finance to collect, use and disclose the SIN and other personal information on the declaration form and that it was necessary to do so to administer the *Speculation and Vacancy Tax Act*.

DOWNLOAD: *Order F19-37* (oipc.bc.ca).

Commissioner grants 30-day time extension for public bodies due to COVID-19 crisis

The COVID-19 pandemic forced public bodies to quickly implement measures to protect the public's health, such as physical distancing. Responding to this unprecedented situation, the Commissioner issued a decision on March 18, 2020, granting a 30-day time extension to public bodies to respond to freedom of information requests received between March 1, 2020 and April 30, 2020. In the decision, he stated that he considered the action fair and reasonable, recognizing the challenges public bodies faced in reorganizing themselves in the face of the COVID-19 public health emergency and the continuing need for accountability and transparency.

DOWNLOAD: *Decision of the Commissioner: Extension of time for public bodies to respond to access requests* (oipc.bc.ca).

BREACH OF TRUST

JOINT INVESTIGATION INTO FACEBOOK HIGHLIGHTS URGENT NEED FOR REFORMS TO BC'S *PERSONAL INFORMATION PROTECTION ACT*.

Facebook is currently the world's largest social media platform, a powerful digital space where approximately 2.6 billion monthly users share an immense amount of personal information. In 2017, a massive privacy breach involving the social media giant would forever change our understanding of how people's personal information can be exploited online.

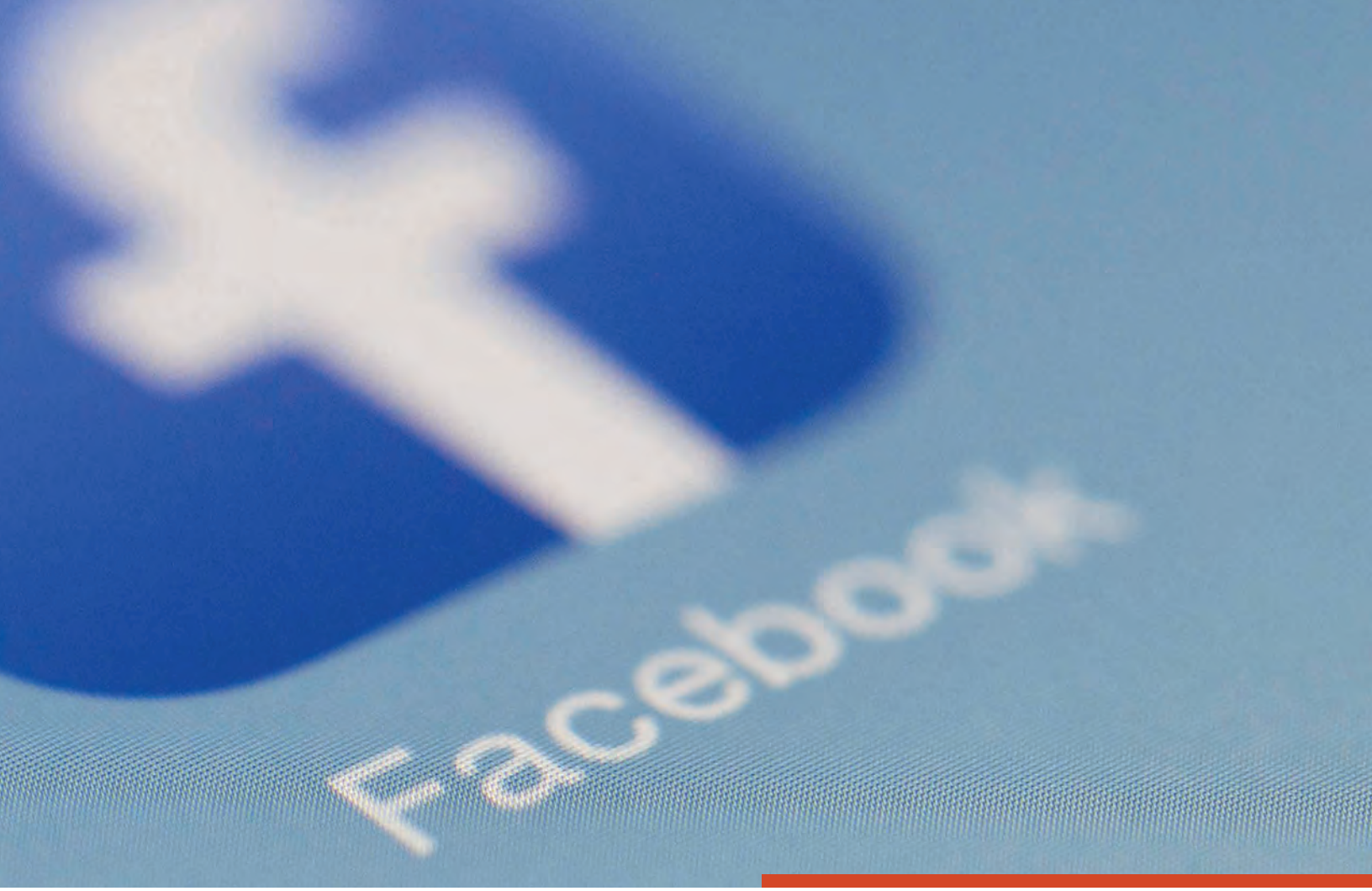
The breach occurred when Facebook allowed an organization to use a third-party application called "This is Your Digital Life" to access users' personal information. Some of that data was then shared with other organizations, including the UK-based Cambridge Analytica, which was involved in US political campaigns.

The app, which encouraged users to complete a personality quiz, collected information about the users who had installed it as well as their Facebook "friends." Some 300,000 Facebook users worldwide used the app, leading to the potential disclosure of the personal information of approximately 87 million users, including more than 600,000 Canadians and up to 100,000 British Columbians.

The OIPC opened a joint investigation into Facebook, Inc. with the Office of the Privacy Commissioner of Canada (OPC) in April 2018. "Given the BC and Canadian connection to this scandal, it quickly became clear that coordinated regulatory action would be required," said BC Information and Privacy Commissioner Michael McEvoy.

In addition to the unauthorized access and lack of meaningful consent from the "friends of friends," the joint investigation found that Facebook failed to exercise proper oversight over the privacy practices of apps on its platform. The company relied instead on the apps to protect against unauthorized access to user information.

"Facebook's monitoring of compliance with those app companies was wholly inadequate," said Commissioner McEvoy. "A basic tenet of privacy laws is that organizations are responsible for the personal information under their control. But Facebook did little to ensure its users' data was properly protected. Instead, the company attempted to shift that responsibility to the apps on its platform and to the users themselves."



DOWNLOAD: *Report of Findings: Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia.* (oipc.bc.ca)

Among other recommendations, the Commissioners called on Facebook to properly audit all apps that collect their users' data. Facebook rejected the OIPC's findings and recommendations, a response that underscored another serious roadblock.

"As regulators in British Columbia and Canada, we have a limited number of tools to protect the privacy rights of our citizens," said Commissioner McEvoy. "Without the ability to levy significant and meaningful fines, I cannot meet the challenges these companies pose to the public interest.

"Facebook has spent more than a decade pledging its commitment to protecting people's privacy. However, when it comes to concrete actions that will fix these transgressions, they demonstrate disregard."

The OPC has taken Facebook to Federal Court, seeking an order to force the company to correct its privacy practices. The OIPC, meanwhile, continues to reserve its right under the *Personal Information Protection Act* (PIPA) to consider future actions against the company.

In the report, Commissioner McEvoy urgently called upon the BC government to update PIPA to better protect the public.

"With the ability to levy significant fines for non-compliance with the law, we will be better able to hold companies like Facebook fully accountable," he said.

A QUESTION OF CONSENT

INVESTIGATION FINDS VICTORIA-BASED FIRM AGGREGATEIQ DATA SERVICES LTD. DELIVERED MICROTARGETED POLITICAL ADS TO CITIZENS WITHOUT ENSURING CONSENT.

The Facebook/Cambridge Analytica story may have had its origins in the United Kingdom and the United States, but Victoria, BC-based AggregateIQ Data Services Ltd (AIQ) also found itself caught up in the global scandal. Information and Privacy Commissioner for BC Michael McEvoy and Privacy Commissioner of Canada Daniel Therrien decided to open a joint investigation into AIQ following media reports about the company's involvement in the 2016 Brexit referendum and their ties to political consulting firm Cambridge Analytica and its parent company, SCL Elections Ltd (SCL). These reports revealed that AIQ worked with SCL on various U.S. political campaigns between 2014 and 2016.

Investigators discovered that SCL provided AIQ with personal information, including psychographic profiles, ethnicity and religion, political donation history, birthdates, email addresses, magazine subscriptions, association memberships, inferred incomes, home ownership information, and vehicle ownership details. AIQ confirmed that SCL was able to use the information to segment individuals into narrow groups for microtargeted advertising campaigns on Facebook.

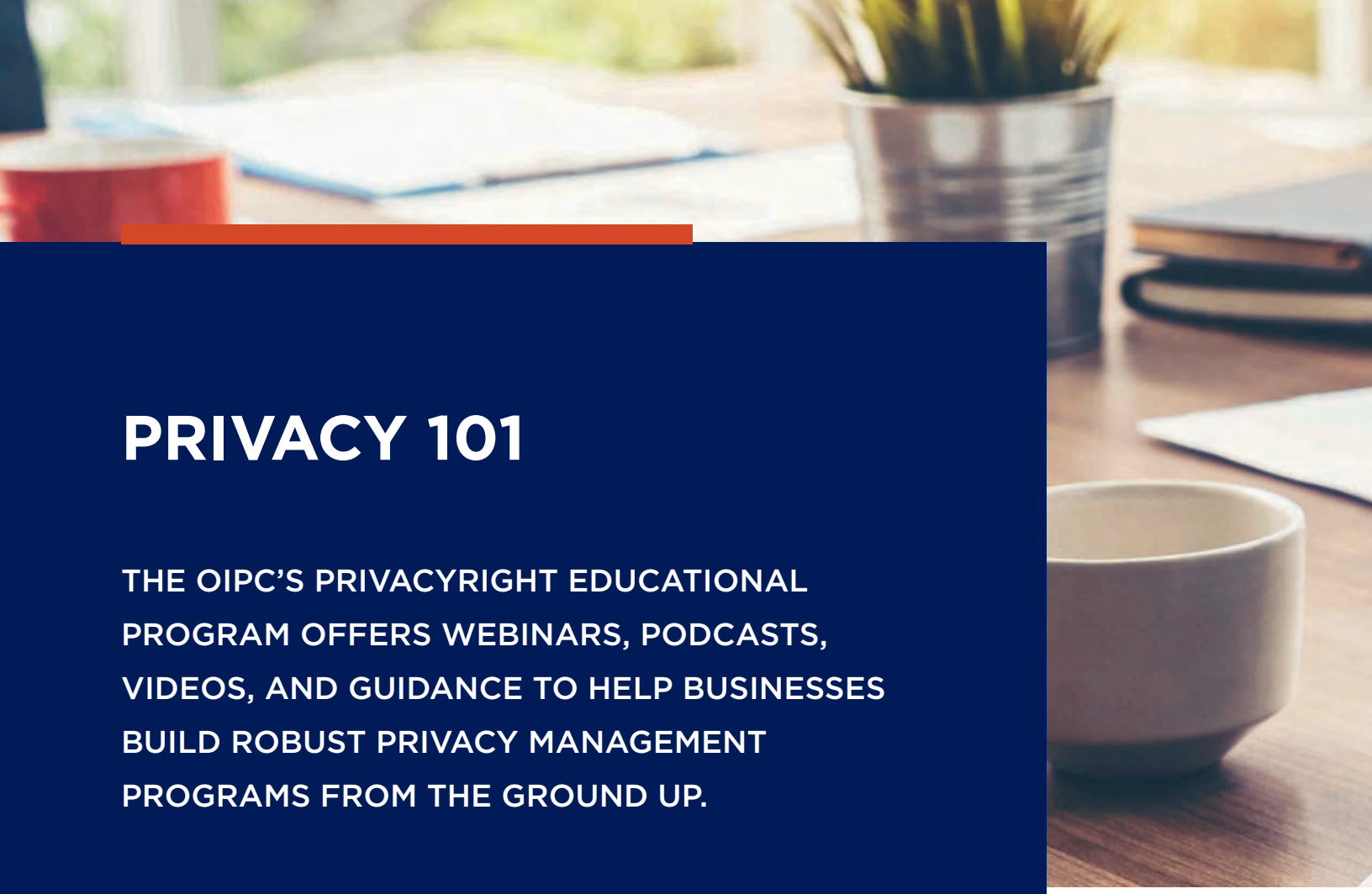
AIQ used individuals' names and email addresses to deliver ads for SCL and other clients using the social network's "custom audience" feature, which allows advertisers to show ads to a list of contacts that Facebook matches on its platform. It also leveraged Facebook's "lookalike" audience feature, which allows advertisers to target broader groups of Facebook users with similar characteristics.

DOWNLOAD: *Investigation Report P19-03 PIPEDA-035913 AggregateIQ Data Services Ltd.* (oipc.bc.ca)

The investigation found that AIQ failed to meet its obligations under Canadian privacy laws when it used and disclosed the personal information of millions of voters in British Columbia, the United States, and the United Kingdom. Specifically, the company did not take reasonable steps to ensure that consent obtained by its international clients was valid for its practices in Canada.

"It is imperative that the activities of tech companies operating across borders respect privacy obligations in all jurisdictions in which they operate," said Commissioner McEvoy. "That's especially the case when it comes to handling sensitive information like the psychological profiles described in this investigation report."

In response to the investigation, AIQ committed to taking a number of measures to improve its security measures. Both commissioners were satisfied with those steps and confirmed that AIQ has implemented their recommendations.



PRIVACY 101

THE OIPC'S PRIVACYRIGHT EDUCATIONAL PROGRAM OFFERS WEBINARS, PODCASTS, VIDEOS, AND GUIDANCE TO HELP BUSINESSES BUILD ROBUST PRIVACY MANAGEMENT PROGRAMS FROM THE GROUND UP.

Businesses that fail to protect personal information in their custody are not only breaking the law, they're also risking their most valuable asset: people's trust.

And yet for many organizations in BC, this crucial consideration is often overlooked in the face of other daily demands — until, that is, a breach occurs and privacy dominates the conversation. There are also many business owners who want to do their best to protect personal information, but simply don't know where to start when it comes to building a privacy management program.

Enter PrivacyRight. The OIPC's most expansive educational program to date, PrivacyRight offers private sector organizations straightforward guidance about their obligations under the *Personal Information Protection Act* (PIPA). The province's private sector privacy legislation applies to any private organization that collects, uses and discloses the personal information of British Columbians, including businesses and corporations, unions, political parties and not-for-profit organizations.

"Our message to BC organizations is clear: privacy compliance is not only their legal obligation, it is also good for business," said Information and Privacy Commissioner Michael McEvoy.

Launched in March 2019, on the 15th anniversary of PIPA's enactment, PrivacyRight is a multi-platform campaign, designed to guide organizations through all aspects of building a privacy management program, from creating a privacy policy through to monitoring compliance.

The nine PrivacyRight webinars offer a step-by-step approach to privacy management, detailing an organization's obligations under PIPA and providing guidance on each component of a robust privacy management program. The animated webinars are short, informative, and accessible and can be used either independently or as a part of an organization's broader privacy training.

VISIT: *The full PrivacyRight program is available here: https://www.oipc.bc.ca/privacyright/*

The four-part PrivacyRight "pop-up" video series puts some of the main principles discussed in the webinars into an everyday context. The series shows how even a routine occurrence, like a visit to the dentist's office, can involve a substantial amount of personal information.

The PrivacyRight podcasts delve into some of the most pressing privacy issues facing private organizations and the public in BC. The first two episodes are fictionalized stories in the style of popular investigative news podcasts. The first explores the pitfalls of employers conducting social media background checks on applicants, while the second focuses on the privacy implications of Canada's legalization of cannabis, particularly for those crossing into the United States. The third episode is an in-depth discussion of privacy issues at strata complexes, featuring interviews with prominent voices in strata matters, as well with Commissioner Michael McEvoy.

Overall, the PrivacyRight program comprises nine webinars, four videos, three podcasts, six new or updated guidance documents, 10 blogs and 10 newsletters.

PrivacyRight updates were distributed to more than 4,400 Better Business Bureau of BC members who receive the organization's *Accredited Business Newsletter*. The program was also included in welcome materials sent to thousands of people registering businesses in BC. In addition, promotional slides for PrivacyRight were featured at ServiceBC locations throughout the province.

"The PrivacyRight program can help organizations get on track with their privacy management programs and make privacy a priority before a breach forces the issue," said Commissioner McEvoy. ●

PRESCRIPTION: PRIVACY PROTECTION

AN OIPC REVIEW FINDS BC MEDICAL CLINICS NEED TO DO MORE TO SAFEGUARD PATIENTS' PERSONAL INFORMATION.

A privacy breach at a medical clinic could have disastrous consequences for patients, from damaged relationships and humiliation to financial loss and more. That's why medical clinics have both a legal and ethical obligation to prevent breaches and protect the personal information in their custody.

A review published by the OIPC in September 2019 found that far too many clinics are failing to meet that obligation.

As private organizations that collect, use and disclose personal information, clinics are legally obligated to abide by the *Personal Information Protection Act* (PIPA). *Audit and Compliance Report P19 01: Compliance Review of Medical Clinics* examined whether 22 medical clinics in BC were meeting their obligations under PIPA. A sample of clinics with five or more licensed physicians on staff in Burnaby, Kelowna, Richmond, Vancouver and Victoria was selected for the report.

Auditors examined clinics' privacy management programs and privacy policies as well as their collection and protection of personal information. Auditors analyzed clinics' websites; conducted interviews with medical directors, privacy officers, and others; and reviewed policies, staff training manuals, and other documents.

The results are concerning in a sector where even minor gaps in privacy protections can have serious ramifications. While some clinics were performing well, none of those reviewed received a "perfect score." Several clinics had serious gaps in their privacy management programs: lacking a privacy officer; inadequate funding and resources for privacy; and a failure to ensure that privacy safeguards kept pace with technological developments.

Information and Privacy Commissioner Michael McEvoy recognizes there are intense and increasing demands on medical professionals; however, he noted that respecting and protecting patients' private information remains "critically important."

"Clinics hold large amounts of some of the most sensitive personal information out there. They are also among the most frequent subjects of complaints and breach reports to my office related to the private sector," he said. "I hope that this report will underscore the need for clinics to address gaps in how they protect this sensitive information and my office's willingness to assist them in doing so."

To that end, the report concluded with 16 recommendations aimed at helping clinics address the gaps in their privacy practices. The recommendations included a call for clinics to build robust privacy management programs, from creating a personal information inventory and developing privacy policies to establishing a protocol for when breaches happen and monitoring compliance with privacy policies.

The report also called on clinics to make privacy practices a priority by ensuring adequate funds for privacy management, designating a privacy officer, and providing training for everyone accessing personal information.

OIPC auditors also recommended that clinics take added precautions if collecting information online and ensure adequate notification for patients. This has since become a particularly pressing concern given the rapid expansion in online medical services brought on by COVID-19.

DOWNLOAD: *Audit and Compliance Report P19 01: Compliance Review of Medical Clinics*

BC Physician Privacy Toolkit: A guide for physicians in private practice

PrivacyRight resources

While the OIPC's Physician Privacy Toolkit and PrivacyRight program can help clinics improve their privacy management programs, legislative reform is also crucial to protect patients.

Commissioner McEvoy noted at the time of the report's release that including mandatory breach notification in PIPA would help ensure that victims of breaches know at an early stage that their information has been compromised.

Administrative monetary penalties would also serve as an effective deterrent. The OIPC has repeatedly called for a uniform set of rules around the protection of personal information in health care. These measures would help give the privacy practices of BC's medical clinics a clean bill of health.

YEAR IN NUMBERS

TABLE 1. Summary of all FIPPA and PIPA files received in 2019-20

FILE TYPE	Received 19/20	Closed 19/20	Received 18/19	Closed 18/19
Privacy breach notification	209	209	194	198
Government monthly breach reviews	0	0	11	11
Privacy complaints (See Tables 2, 8, 9)	274	292	332	322
Access complaints (See Tables 3, 6, 7)	382	433	406	443
Requests for review				
Requests for review of decisions to withhold information	477	489	458	521
Deemed refusal	184	194	199	176
Applications to disregard requests as frivolous or vexatious	9	7	13	12
Time extensions				
Requests by public bodies and private organizations	6,591	6,585	3,854	3,859
Requests by applicants seeking a review	32	30	21	24
Public interest notification (s.25)	12	16	20	18
Requests for reconsideration of OIPC decisions	55	55	51	37
Information requested/received				
Requests for information and correspondence received	4,528	4,525	5,481	5,483
Non-jurisdictional issue	14	15	13	13
No reviewable issue	113	130	118	105
Media enquiries	137	128	135	127
FOI requests for OIPC records	18	18	18	18
Adjudications of OIPC decisions	3	3	4	2
OIPC initiatives				
Audit and Compliance	2	3	4	5
Investigations	12	14	17	16
Legislative reviews	47	49	42	50
Projects	6	5	19	23
Policy or issue consultation	407	434	392	417
Police Act IIO reports	64	65	44	43
Privacy impact assessments	69	85	94	95
Public education and outreach				
Speaking engagements	42	46	48	37
Meetings with public bodies and private organizations	36	44	73	64
Other (section 56, internal reviews, and research agreement complaint)	301	305	86	92
TOTAL	**14,024**	**14,179**	**12,148**	**12,211**

TABLE 2. Breakdown of privacy complaints received in 2019-20 (FIPPA and PIPA)	
Accuracy	1
Collection	69
Use	2
Disclosure	136
Retention	5
Correction	25
Protection	36
Total	**274**

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 3. Breakdown of access complaints received in 2019-20 (FIPPA and PIPA)	
Duty required by Act	48
Time extension by public body	37
Adequate search	242
Fees	46
No notification issued	9
Total	**382**

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.

YEAR IN NUMBERS

TABLE 4. Number of FIPPA complaints and requests for review received in 2019-20 by public body

Public body	Complaints received	Requests for review received	Total
Ministry of Children and Family Development	38	46	**84**
Insurance Corporation of British Columbia	23	37	**60**
Vancouver Island Health Authority	26	31	**57**
City of Vancouver	25	22	**47**
Vancouver Police Department	10	32	**42**
Ministry of Attorney General	16	26	**42**
University of British Columbia	7	30	**37**
Ministry of Health	17	13	**30**
Ministry of Public Safety & Solicitor General	11	16	**27**
Ministry of Finance	10	14	**24**
Top 10 total	**183**	**267**	**450**
All other public bodies	285	318	**603**
Total	**468**	**585**	**1,053**

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 the 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 5. Number of PIPA complaints and requests for review received in 2019-20 by sector

Sector	Complaints received	Requests for review received	Total
Services	63	12	75
Health	29	28	57
Real estate	21	4	25
Professional science & development	12	5	17
Administrative support	11	6	17
Retail trade	13	2	15
Finance/insurance	10	4	14
Arts/entertainment	4	5	9
Accommodation	5	2	7
Education	3	2	5
Wholesale trade	3	2	5
Top 10 total	**174**	**72**	**246**
Other	14	4	18
Total	**188**	**76**	**264**

NOTE (TABLES 6 -13):

Investigation: Files that were mediated, not substantiated, partially substantiated, and substantiated.
Declined to investigate/discontinued: Files referred back to public body, withdrawn, or files the OIPC declined to investigate (for example, those that were frivolous, vexatious, or not made in good faith).
Hearing or report: Files that proceeded to inquiry and/or a report was issued.

TABLE 6. Outcome of access complaints resolved in 2019-20, FIPPA

Type	Investigation	Declined to investigate/ discontinued	Hearing or report	Total
Adequate search	81	128	1	**210**
Duty	34	20	21	**75**
Fees	42	14	0	**56**
Time extension by public body	30	2	1	**33**
S 25 not applied	4	6	0	**10**
TOTAL	**191**	**170**	**23**	**384**

TABLE 7. Outcome of access complaints resolved in 2019-20, PIPA

Type	Investigation	Declined to investigate/ discontinued	Hearing or report	Total
Adequate search	16	18	0	**34**
Duty	4	3	0	**7**
Fees	5	1	2	**8**
TOTAL	**25**	**22**	**2**	**49**

YEAR IN NUMBERS

TABLE 8. Outcome of privacy complaints resolved in 2019-20, FIPPA

Type	Investigation	Declined to investigate/ discontinued	Hearing or report	Total
Accuracy	1	1	0	2
Collection	8	11	0	19
Correction	10	9	0	19
Disclosure	35	45	0	80
Retention	0	2	0	2
Use	1	0	0	1
Protection	7	16	0	23
TOTAL	**62**	**84**	**0**	**146**

TABLE 9. Outcome of privacy complaints resolved in 2019-20, PIPA

Type	Investigation	Declined to investigate/ discontinued	Hearing or report	Total
Collection	29	18	4	51
Correction	3	7	0	10
Disclosure	36	21	4	61
Retention	3	3	0	6
Use	2	1	0	3
Protection	10	5	0	15
TOTAL	**83**	**55**	**8**	**146**

TABLE 10. Outcome of requests for review resolved in 2019-20, FIPPA

Type	Mediated	Declined to investigate/ discontinued	Hearing/consent order/other	Total
Deemed refusal	128	13	9	**150**
Deny	65	1	27	**93**
Notwithstanding	3	0	1	**4**
Partial access	226	18	64	**308**
Refusal to confirm or deny	5	0	5	**10**
Scope	7	0	1	**8**
Third party	27	0	12	**39**
Total	**461**	**32**	**119**	**612**

TABLE 11. Outcome of requests for review resolved in 2019-20 PIPA

Type	Mediated	Declined to investigate/ discontinued	Hearing or report	Total
Deemed refusal	41	3	0	**44**
Deny access	8	2	3	**13**
Partial access	9	1	3	**13**
Scope	1	0	0	**1**
Totals	**59**	**6**	**6**	**71**

TABLE 12. Outcome of all complaints resolved by the OIPC (FIPPA and PIPA) in 2019-20

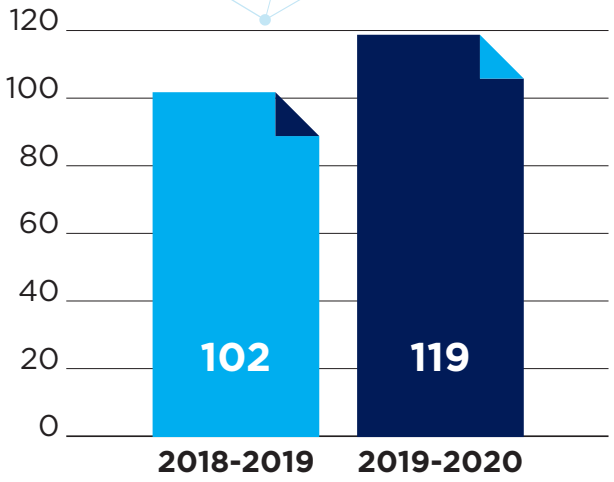
Investigations	No investigations	Declined to investigate/ discontinued	Hearing or report	Total
361	296	35	33	**725**

TABLE 13. Outcome of all requests for review resolved by the OIPC (FIPPA and PIPA) in 2019-20

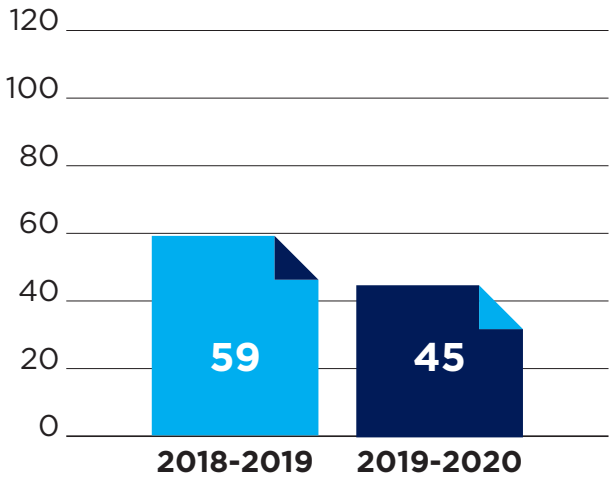
Mediated	Hearing or report	Declined to investigate/ discontinued	Total
520	125	38	**683**

YEAR IN NUMBERS

ADJUDICATION: Inquiries requested and orders issued

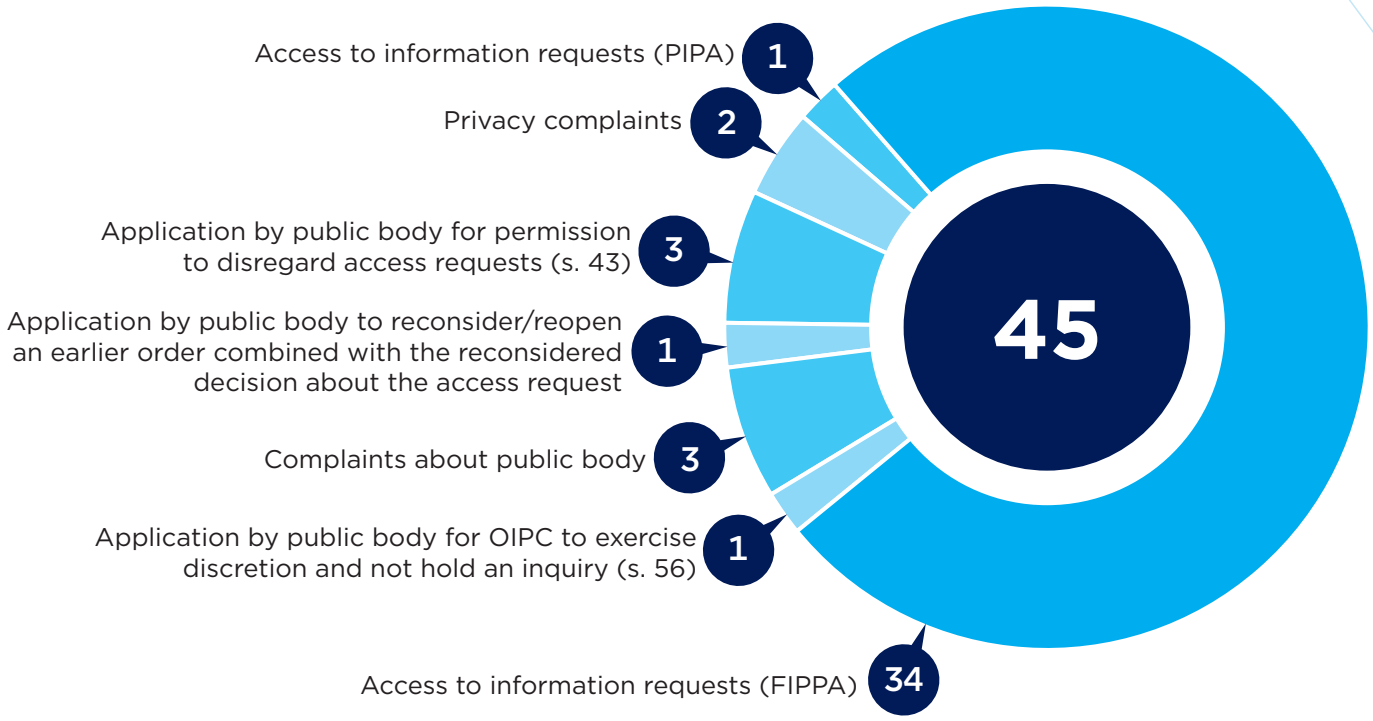


Inquiries requested



Orders issued

ADJUDICATION: Types of FIPPA and PIPA inquiries



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 the Registrar of Lobbyists and oversees and enforces the *Lobbyists Transparency Act* (LTA).

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

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

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

2019-20	Operating	Capital
Appropriation	$6,702,000	$543,944
Total operating expenses	$6,612,019	-
Capital acquisitions	-	$543,944
Unused appropriation	$89,981	$0

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

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).

2019-20	Closing cost	Closing accumulated amortization	Net book value (March 31/20)
Computer hardware and software	$873,728	-$325,298	$548,430
Tenant improvements	$552,302	-$552,302	$0
Furniture and equipment	$107,277	-$95,915	$11,362
Total tangible capital assets	**$1,533,307**	**-$973,515**	**$559,792**

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**

Commissioner McEvoy delivers a keynote address at the 21st Annual Privacy and Security Conference in Victoria, February 7, 2020.

OUTREACH

COMMISSIONER MCEVOY AND OIPC STAFF ARE FREQUENT SPEAKERS AND PARTICIPANTS AT EVENTS AND CONFERENCES THROUGHOUT BC — AND BEYOND.

Here are some of the events that featured OIPC speakers and presenters during the 2019-20 fiscal year:

- 10th Annual Access Privacy Conference, Toronto
- Big Data Surveillance Conference, Victoria
- Canadian Bar Association Privacy Law Conference, Vancouver
- Canadian College of Health Leaders, Victoria
- Conference of Canadian Election Officials, Saint Andrews, New Brunswick
- IAPP Canada Privacy Symposium, Toronto, Ontario
- IAPP Global Privacy Summit, Washington
- LandlordBC Annual General Meeting, Victoria
- 20th Meeting of Federal, Provincial and Territorial Ministers, Charlottetown, PEI
- MISA (Municipal Information Systems Association) Conference, Niagara Falls, Ontario
- Privacy and Data Governance Congress (Privacy and Access Council of Canada), Calgary
- 21st Annual Privacy and Security Conference Privacy & Security: Bringing Digital Into Focus, Victoria
- Thompson Rivers University Privacy and Security Conference 2020, Kamloops
- 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
- Developing a privacy policy under PIPA
- Early notice and PIA procedures for public bodies
- Privacy management program self assessment
- Privacy impact assessments for the private sector

Access (general)

- Guidance 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 records

Privacy (general)

- Direct-to-consumer genetic testing and privacy
- Employee privacy rights
- Guide to using overt video surveillance
- Identity theft resources
- Information sharing agreements
- Obtaining meaningful consent
- Privacy proofing your retail business
- Private sector landlords and tenants
- Protecting personal information: cannabis transactions
- Protecting personal information away from the office
- Disclosure of personal information of individuals in crisis
- Responding to PIPA privacy complaints

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

Technology and social media

- Guidance for the use of body-worn cameras by law enforcement authorities
- Guidelines for online consent
- Guidelines for social media background checks
- Mobile devices: tips for security & privacy
- Public sector surveillance guidelines
- Use of personal email accounts for public business
- Tips for public bodies and organizations setting up remote workspace

OFFICE OF THE
INFORMATION & PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

For more information about BC's access and privacy laws, visit **oipc.bc.ca**

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