Office of the Information and Privacy Commissioner for British Columbia

ANNUAL REPORT 2020-21

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:

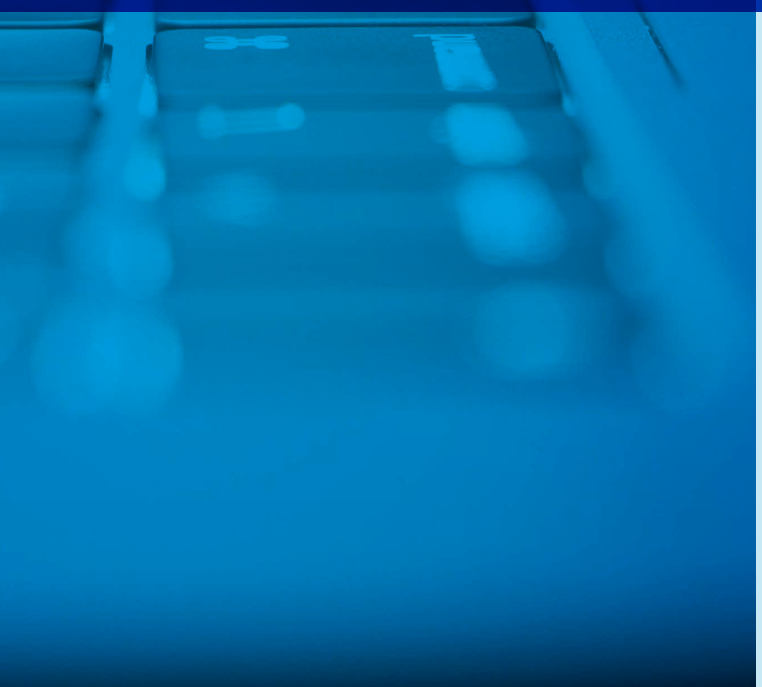
- The ***Freedom of Information and Protection of Privacy Act*** (FIPPA), which applies to over 2,900 public bodies, including ministries, local governments, schools, crown corporations, hospitals, municipal police forces, and more; and
- The ***Personal Information Protection Act*** (PIPA), which applies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

OUR CORE VALUES

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

TABLE OF CONTENTS



OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

September 2021

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

Dear Honourable Speaker,

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

This report covers the period from April 1, 2020 to March 31, 2021.

Yours sincerely,

Michael McEvoy
Information and Privacy Commissioner and Registrar of Lobbyists for British Columbia.

COMMISSIONER'S MESSAGE

I am pleased to present the 2020-21 annual report for the Office of the Information and Privacy Commissioner for British Columbia.

During the last fiscal year, the spread of COVID-19 continued to strongly impact both our internal operations and our mandate to protect the personal information of citizens and their right to access information. The dramatic increase in online services utilized by public bodies, private organizations, and individuals accelerated these impacts.

It was therefore hardly surprising that our office responded to many inquiries, complaints, and applications about how our privacy and access statutes apply during the COVID-19 pandemic.

The rapid spread of the virus also challenged the access to information operations of some public bodies, as their move to remote work initially made it more difficult to gather hard copy records. Considering these extraordinary circumstances, in March 2020, I provided public bodies additional time of up to 30 days to process access to information requests, with a requirement to report the extensions to my office.

This extension only applied to requests received between March 1, 2020 and May 15, 2020 — after that time, public bodies were expected to adjust to a new normal which included the ability to use the time extension mechanisms available under FIPPA, if appropriate.

A few months later, I released my report card on the timeliness of provincial government responses to access to information requests. The report, my office's sixth examination of government timeliness, covered a three-year period from April 1, 2017, to March 31, 2020. While government's response times have generally improved since the previous report was released in 2017, there were thousands of cases where government extended the time it took to answer access requests without any lawful basis under FIPPA. As I observed in the report, nothing less than a shift in government's mindset is required to enable that to happen.

Other matters tackled by my office this year included the alarming increase in privacy breaches and cybercrimes. Together with our colleagues at the Ontario Information and Privacy Commissioner's Office, we continued our investigation into the LifeLabs cyberattack, which affected millions of people, mostly in British Columbia and Ontario. While the report has not yet been published pending court processes, all of the orders we issued against LifeLabs have been addressed by the company.

The growing use of artificial intelligence and facial recognition technologies was also a matter of focus by my office. Facial recognition technology (FRT) figured prominently in a joint investigation of Clearview AI, a company that scrapes facial images from a myriad of places for law enforcement purposes. Together with our colleagues from Quebec, Alberta, and the federal

privacy commissioner's office, we found that Clearview AI collected highly sensitive biometric information without the knowledge or consent of individuals for inappropriate purposes. Clearview AI agreed to stop offering its services in Canada for a period of two years but objected to ceasing the collection of images of individuals in Canada and to deleting the ones they already collected.

Another joint investigation, this time with the Privacy Commissioner of Canada and the Information and Privacy Commissioner of Alberta, touched on the commercial use of surveillance without a person's consent. The mall developer Cadillac Fairview used facial recognition via a small camera embedded in their mall directories without customers' consent to generate additional personal information about individuals, such as estimated age and gender. More detailed information about the reports mentioned can be found in the Features section of this report.

Beyond significant investigation work, the COVID-19 outbreak has also required my office to provide guidance and advice to a wide array of interests, from businesses and school educators to public bodies and the general public. We have offered our expertise on matters ranging from how retail establishments should collect and use their patron's personal information to how educators should deploy new technological learning tools for kids; from how seniors shopping online, often for the first time, should protect themselves to what businesses can do to make sure work from home doesn't expose the sensitive information of clients and customers.

Contact tracing related to the virus also put matters of privacy protection squarely before my office. These and related issues, like vaccine certification, are in many instances linked to national and international considerations. For this reason, we continue to be deeply engaged in discussions with regulatory colleagues, nationally and internationally. Together with our federal, provincial, and territorial counterparts, we released a joint resolution and statement on the issue of contact tracing apps.

The need for national and international regulatory cooperation highlighted the importance of my office's continued leadership role as Secretariat for the Asia Pacific Privacy Authorities (APPA). We have served in this capacity since 2016, coordinating the activities of the 19-member organization. Together, we share information about common investigatory matters and exchange ideas about emerging privacy issues, new technologies, the management of privacy enquiries and complaints, and the pressing need in many jurisdictions for legislative reform.

The importance of reforming the *Personal Information Protection Act* (PIPA) and the *Freedom of Information and Protection of Privacy Act* (FIPPA, which govern the access and privacy rights of citizens, public bodies, and private organizations, has been the subject of past messages. The impact of COVID-19 has only sharpened the imperative for this legislative overhaul.

Steps were taken on the road to reform for BC's private sector privacy legislation in 2019 with the work of the Special Committee to Review the Personal Information Protection Act. These efforts were put on pause during the provincial election in September 2020 and resumed when a new Special Committee was appointed in late 2020.

The metaphorical reform train is now back on track. It is my hope that PIPA will soon be strengthened, so the personal information of British Columbians is better protected. With the FIPPA Special Committee now struck as well, we are hopeful that necessary amendments to BC's public sector privacy legislation will also be forthcoming. Reforming these Acts is fundamentally critical to preserving and enhancing our privacy and access to information rights.

I would like to close by acknowledging the immensely talented OIPC staff. Each brings a deep sense of commitment and purpose to the work they do; never better exemplified than through the delivery of uninterrupted service to British Columbians during these uncertain times.

The public is extremely well served by their dedication, expertise, and high ethical standards. I deeply appreciated their efforts of the past year.

Michael McEvoy
Information and Privacy Commissioner for British Columbia

OIPC 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.*

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 under FIPPA and PIPA 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 determine whether to open a file, 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, make decisions on complaint files, 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 an inquiry. Adjudicators assess the evidence and arguments and issue final and legally binding decisions. Orders are subject to judicial 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, provide guidance, and make educational presentations.

Audit & systemic review

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

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 41 people worked at the Office of the Information and Privacy Commissioner in 2020- 21. An additional 20 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.

During the 2020-21 fiscal year, the OIPC implemented six actions recommended by the office's Diversity and Inclusion Group (DIG) , most of which have now been integrated into our regular office practices. These include establishing a harassment policy; incorporating Indigenous Relations Behavioural Competencies into job postings; creating an orientation document for new hires, which includes information about actions taken in this area; supporting staff who wish to take training about diversity and inclusiveness as part of their learning plans; updating our signature blocks to include acknowledgement of Indigenous territory with an option to incorporate gender pronouns; and including territorial acknowledgements in OIPC speeches and presentations.

OIPC staff also take pride in and have long supported community causes. This includes the Provincial Employees Community Services Fund (PECSF), as well as other local charities. OIPC staff are proud to have received two awards for the 2020 PECSF campaign: Highest Staff Participation Rate and Highest Average Donation for a small entity.

OUR WORK IN THE TIME OF COVID

STARTING IN MARCH 2020 AND CONTINUING INTO 2021, MOST OIPC STAFF FOUND THEMSELVES IN THE SAME POSITION AS MANY OTHER BRITISH COLUMBIANS — WORKING FROM HOME. WHAT REMAINED UNCHANGED, HOWEVER, WAS THE HIGH DEMAND FOR THE OIPC'S SERVICES.

The COVID-19 pandemic set into motion a series of rapid changes in all of our lives, both personally and professionally. It curtailed our physical interactions and accelerated our virtual ones, as we turned to online platforms and websites to see friends, families, and even doctors. Students of all ages learned in online classrooms, while teachers adjusted lesson plans to adapt to the new virtual environment. Meanwhile retailers, from grocers to furniture outlets, ramped up their online purchase systems.

Starting in March 2020 and continuing into 2021, most OIPC staff found themselves in the same position as many other British Columbians — working from home. What remained unchanged, however, was the high demand for the OIPC's services.

While the number of files coming into the office didn't slow down in 2020-21, there was a shift in the *types* of files the OIPC received. For example, OIPC staff saw an increase in breach reports, requests for information, privacy impact assessments, and requests for inquiry compared to the previous fiscal year. This came as no surprise as British Columbians had to rely on new online tools to conduct business, and individuals and organizations alike tried to understand how new Public Health Officer measures and orders affected them. Time extensions, complaints, and requests for review remained steady.[1]

It was also clear at the outset of the pandemic that the access to information operations of many public bodies would be significantly affected. For that reason, Information and Privacy Commissioner Michael McEvoy made a proactive decision on March 18, 2020 that recognized both the challenges public bodies faced in reorganizing themselves due to COVID-19 and the continuing need for transparency. The decision granted a 30-day time extension to public bodies to respond to freedom of information requests received between March 1, 2020 and April 30, 2020. On April 22, 2020 the Commissioner extended that order to requests received between May 1 and May 15, 2020 in order to give public bodies time to arrange their operations to meet the provisions of the statutes.[2] In both decisions, pubic bodies were required to report the extensions to the OIPC.

The provincial government also exercised extraordinary authority in modifying data residency requirements for the personal information of British Columbians held by the province's public bodies. The temporary measure was invoked through a series of Ministerial Orders.

"I regarded the temporary provisions as tailored and reasonable, given the immediacy of the challenges public bodies found themselves in," said Commissioner McEvoy.

Government's special orders broadened the authorized communication tools that could be used by health care and education personnel, among others, to technologies hosted outside Canada. This enabled communication and collaboration through those technologies for the purpose of continuing service delivery during the public health emergency. "To the government's credit, they moved early to consult with my office, detailing how they intended to draw the orders in a narrow fashion," says Commissioner McEvoy. The present order is set to expire on December 31, 2021.

[1] See a year by year comparison in the Year in Numbers summary on page 24 of this report.

[2] The number of time extensions taken under this decision can be found in the Year in Numbers summary on page 24 of this report.

One area that the Ministerial Orders directly impacted was education and, in particular, K-12 education. The order permits the use of a wider range of technology tools for distance learning in cases where students are not able to connect physically in a classroom. The OIPC worked with school districts and the BC Teachers' Federation to ensure e-learning could happen in a privacy protective way.

As the pandemic progressed through 2020, governments turned to digital technologies to develop tools to deal with the pandemic, such as contact tracing apps and vaccination rollout.

In May 2020, Commissioner McEvoy joined his federal, provincial, and territorial colleagues to issue a joint statement calling on governments to ensure that COVID-19 contact tracing applications respect key privacy principles. "There may be a place for contact tracing apps as the province determines next steps in addressing the COVID-19 crisis. If the government goes down this road, what most British Columbians would expect is that any initiative would be voluntary, would collect the minimum amount of personal information necessary and, critically, whatever personal information is collected would only be used for the purpose of fighting COVID-19," said Commissioner McEvoy. Ultimately, the BC government decided to focus resources on traditional contact tracing methods versus using a digital contact tracing app.

The matter of knowing where transmission of the virus was occurring in BC came before the OIPC in September, 2020, when the Nuu-chah-nulth Tribal Council, Heiltsuk Nation, and Tsilhqot'in National Government submitted a s. 25 complaint that the Ministry of Health and several other public bodies failed to disclose specific information relating to cases of COVID-19 in neighbouring communities.

At inquiry, the Commissioner considered whether the Ministry of Health and certain other public bodies failed to comply with s. 25 of FIPPA by withholding information about presumptive or confirmed COVID-19 cases proximate to the Nations' rural Indigenous Communities. Section 25(1)(a) of FIPPA requires a public body to, "without delay, disclose to the public, to an affected group of people or to an applicant…information about a risk of significant harm to the environment or to the health or safety of the public or a group of people."

Commissioner McEvoy determined that the *Public Health Act* did not override this responsibility. However, he also determined that while COVID-19 creates a risk of significant harm to the public, sufficient information was already available on COVID-19 cases to enable the public, and the complainant governments, to take steps to avoid or mitigate the risks connected with COVID-19.

Throughout 2020-21, the OIPC continued collaboration efforts with provincial, federal, and global regulators on the challenges stemming from the COVID-19 pandemic. In September, members of the Asia Pacific Privacy Authorities (APPA) held a special session to discuss privacy issues in member jurisdictions related to the pandemic and data protection efforts to tackle these challenges.

In December 2020 members of the 54th APPA Forum also discussed the privacy implications of the COVID-19 pandemic as well as how any government actions need to appropriately balance the need for governments to protect their communities and the harms associated with risking the protection of personal information.

The OIPC issued an array of COVID-related guidance and advice in 2020-21 for businesses, school educators, and the general public. This included guidance on how retail establishments should collect and use their patrons' personal information, how educators should deploy new technological learning tools for kids, how seniors shopping online, often for the first time, should protect themselves, and what businesses can do to make sure work from home doesn't expose the sensitive information of clients and customers.[3]

As of March 31, 2021, the COVID-19 pandemic and the challenges it poses to access to information and privacy are ongoing. The Commissioner will once again report on these challenges in the 2021-22 annual report.

One guiding principle will remain constant as the OIPC continues to work with the government and the public on these issues: BC's legislation is designed to facilitate the sharing of personal information necessary to ensure the public's health and safety. Protection of personal information does not pose a barrier to this. ●

ADDITIONAL READING

Decision of the Commissioner: Extension of time for public bodies to respond to access requests

Statement from BC's Information and Privacy Commissioner on freedom of information during the COVID-19 pandemic

Privacy guardians issue joint statement on COVID-19 contact tracing applications

Privacy tips for seniors: Protect your personal information

Making privacy a priority amid the 'new normal': Data Privacy Day Commissioner statement

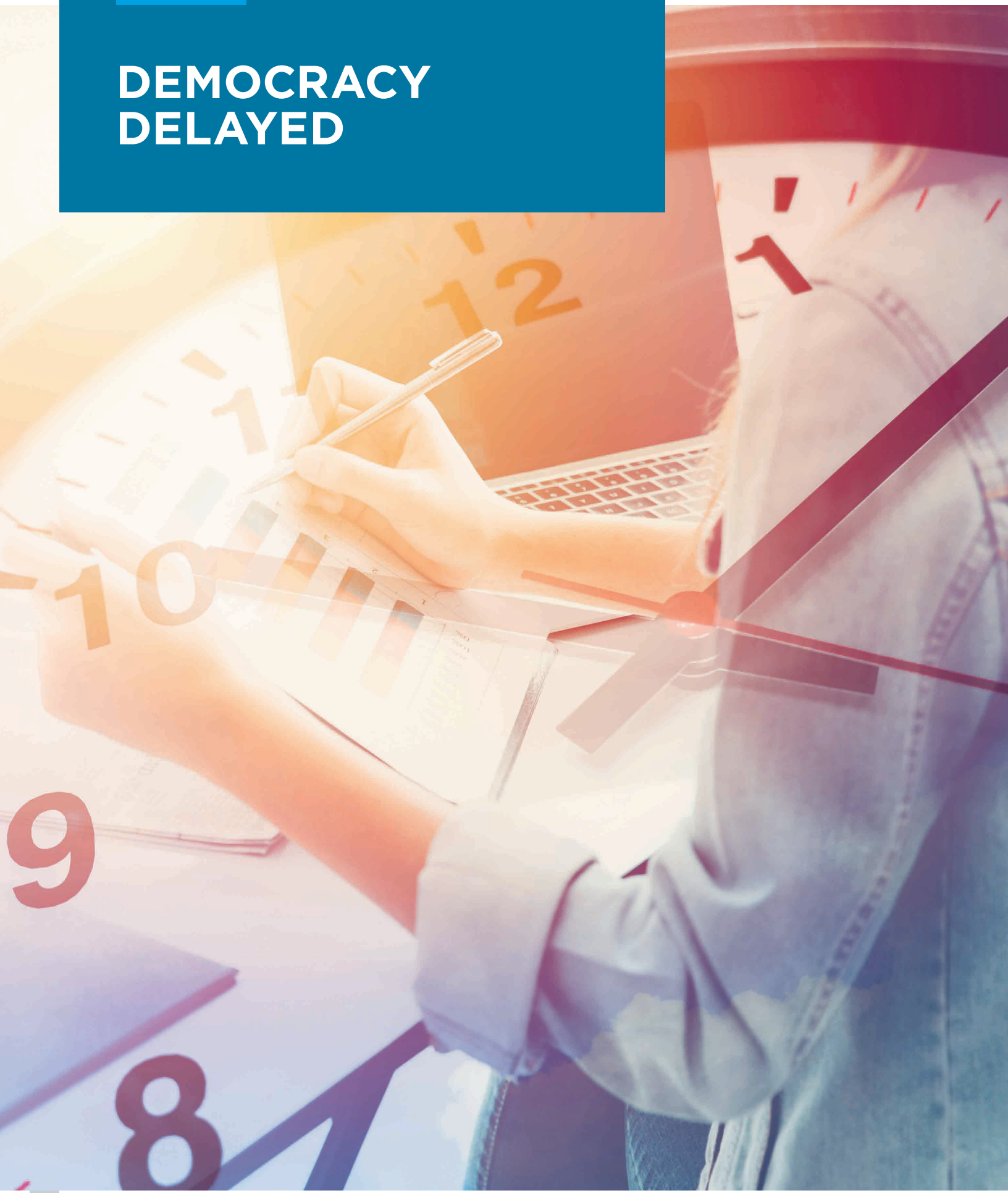
Collecting personal information at food and drink establishments, gatherings, and events during COVID-19

FIPPA and online learning during the COVID-19 pandemic

Commissioner rejects argument government's emergency powers override public interest disclosure provision; determines s. 25 of FIPPA does not require Ministry of Health to disclose requested COVID-19 information

[3] For a full list of OIPC guidance documents, check out Resources on page 35

DEMOCRACY DELAYED



TIMELINESS UNDERPINS MEANINGFUL ACCESS TO GOVERNMENT INFORMATION. TOO OFTEN, HOWEVER, GOVERNMENT RESPONSES TO ACCESS REQUESTS OCCUR WELL BEYOND FIPPA'S TIMELINES.

The right to access government records is enshrined in the province's *Freedom of Information and Protection of Privacy Act* (FIPPA) to promote accountable government. When our access to information system is working well, any applicant — subject to certain exceptions — should be able to request and access records about themselves or those that detail how government decisions are made.

Timeliness underpins meaningful access to government information. Too often, however, government responses to access requests occur well beyond FIPPA's timelines without any authority to do so. The OIPC's September 2020 Special Report, Now is the time: A report card on government's access to information timeliness — April 1, 2017 — March 31, 2020, shines a light on this issue. In thousands of cases over a three-year period, government extended the time it took to respond to access to information requests without a lawful basis.

In this, the OIPC's sixth review of government timeliness, analysts examined information provided by the Ministry of Citizens' Services Information Access Operations (IAO). The IAO processes access requests received by core government, including the Office of the Premier. Analysts examined three key measures: the percentage of requests responded to within FIPPA timelines, the average number of business days spent processing requests and the average number of business days a response was delayed beyond FIPPA timelines.

FIPPA mandates that government should respond to access requests within 30 business days. Government can extend by an additional 30 days in defined circumstances. Any further extensions require OIPC approval. Yet in some 4,000 cases during the period covered in the report, government took longer than 60 days to respond to access requests without seeking OIPC permission to do so.

"This represents a blight on the access system that damages the integrity of BC's access to information law," said Information and Privacy Commissioner Michael McEvoy. "The timeline provisions in FIPPA are not suggestions — they are legal obligations."

The Commissioner noted a general improvement in government's response times since the previous timeliness report, released in September 2017. He also commended the public servants who have been working hard to meet a significantly higher number of access requests during this time.

However, he said, a total disregard for legislated timelines in far too many cases, means "this is far from an unqualified success."

"There is significant work to be done to keep FIPPA from falling into disrepute," said Commissioner McEvoy. "Nothing less than a shift in government's mindset towards timely response to access to information requests will enable that work to succeed. Violating legislated timeline provisions should no longer be tacitly accepted as 'business as usual'."

The report notes the challenges public servants face when processing access requests, including the soaring number of requests. There has also been an increase in requests that involve a large number of records or those that require time-consuming searches. Both can affect response time.

Recommendations in the report to address these challenges include proactively disclosing records, expanding presumptive sign-off policies, and exploring automation for the processing of records.

Implementing these recommendations may reduce the growing number of time extension requests filed by government without authority. Regardless of the demand, the onus is on government to operate within the parameters set out in FIPPA, Commissioner McEvoy said. "The fact is that the public service must have the resources necessary to keep pace with demand and to comply with the law." ●

DOWNLOAD: *Now is the time: A report card on government's access to information timeliness — April 1, 2017–March 31, 2020* (oipc.bc.ca)

CANDID CAMERA

A JOINT INVESTIGATION REVEALED THAT CADILLAC FAIRVIEW USED FACIAL RECOGNITION SOFTWARE WITHOUT CUSTOMER KNOWLEDGE OR CONSENT, COLLECTING AND STORING APPROXIMATELY 5 MILLION NUMERICAL REPRESENTATIONS OF PEOPLE'S FACES.

No-one who pauses to view an information kiosk in a shopping mall would reasonably expect their image to be captured and analyzed by facial recognition software. However, a joint investigation, undertaken by the OIPC with the Privacy Commissioners of Canada and Alberta found that Cadillac Fairview, one of North America`s largest commercial real estate companies, did just that.

The investigation revealed that the company used facial recognition software without customer knowledge or consent, collecting and storing approximately 5 million numerical representations of people's faces.

Customer images were captured through the use of small embedded cameras inside their shopping mall information kiosks in several Canadian locations, including Richmond Centre and Pacific Centre in BC.

The goal of the software, according to Cadillac Fairview, was to analyze the age and gender of shoppers to provide targeted advertising, not to identify individuals. Cadillac Fairview maintained that shoppers were made aware of the activity via decals it had placed on shopping mall entry doors that referred to their privacy policy – a measure the commissioners determined was insufficient.

Cadillac Fairview claimed it was not collecting personal information because the images were only briefly analyzed then deleted. While investigators confirmed images were deleted, they discovered that sensitive biometric information from the images was being stored in a centralized database by a third party.

Cadillac Fairview said that it was unaware of this database, highlighting an additional risk of potential use by unauthorized parties or, should a data breach occur, by malicious actors.

The conclusion reached by commissioners about cameras in mall directories was straight-forward: "Pictures of individuals were taken and analyzed in a manner that required notice and consent," said Michael McEvoy, Information and Privacy Commissioner for BC.

In response to the investigation, Cadillac Fairview removed the cameras from its digital directory kiosks and says it has no current plans to reinstall the technology. The company has also deleted all information associated with the facial recognition technology that was not required for legal purposes, and confirmed it will not retain or use such data for any other purpose. This includes the more than 5 million biometric representations of individual shoppers' faces as well as the images stored by the third party.

Together, the privacy commissioners recommended that if Cadillac Fairview were to use such technology in the future, it should take steps to obtain express, meaningful consent, before capturing and analyzing the biometric facial images of shoppers. ●

READ: *Report of findings: Joint investigation of the Cadillac Fairview Corporation Ltd. by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia* (oipc.bc.ca)

BILLIONS OF FACES, NO CONSENT

CLEARVIEW AI, AN AMERICAN FACIAL RECOGNITION COMPANY, SCRAPED THE IMAGES OF BILLIONS OF PEOPLE FROM ONLINE SOURCES (INCLUDING SOCIAL MEDIA) FOR USE IN FACIAL RECOGNITION SOFTWARE THAT WAS MARKETED TO LAW ENFORCEMENT AGENCIES AND PRIVATE ORGANIZATIONS ACROSS NORTH AMERICA

Hundreds of millions of people post photos online every day. From sharing special moments to the mundane, photos are often central to the online experience, particularly on social media. Few would expect those images to be surreptitiously used to train an artificial intelligence algorithm that would, in effect, place them in a massive, perpetual police lineup.

Effectively, that is what happened in the case of Clearview AI, an American facial recognition company that scraped the images of billions of people from online sources (including social media) for use in facial recognition software that was marketed to law enforcement agencies and private organizations across North America. Subscribers could use Clearview AI's facial recognition app to match photographs of unknown people with the company's database of images and the corresponding links to where the images were found online.

In an investigation report published on February 3, 2021, Michael McEvoy, Information and Privacy Commissioner for BC, along with commissioners from the Office of the Privacy Commissioner of Canada (OPC), the Commission d'accès à l'information du Québec, and the Office of the Information and Privacy Commissioner of Alberta, found Clearview AI's practices to be unlawful. "They are tantamount to the mass surveillance of Canadians and a widescale violation of their privacy rights," said Commissioner McEvoy.

The report notes that the company did not attempt to obtain consent from — or even notify — those captured in the database, the majority of whom have never and will never be implicated in any crime.

"Our investigation revealed a vast amount of personal information collected without people's knowledge or consent," said Commissioner McEvoy. "It is unacceptable and deeply troubling that a company would create a giant database of our biometric data and sell it for profit without recognizing its invasive nature."

The investigation was launched in February 2020 following numerous media reports raising concerns about the company's collection and use of personal information without consent.

In July 2020, Clearview AI announced that it had temporarily stopped offering its facial recognition service in Canada in response to the investigation. The regulators' investigation continues however, because of Clearview AI's failure to delete the information it had collected and agree to cease collecting personal information of individuals in Canada.

Among other defences, the company argued that its lack of a "real and substantial connection" to Canada meant that it did not fall under Canadian privacy laws. It rejected even the premise that the mass collection of people's biometric information without their consent violated reasonable expectations of privacy believing that consent was not required because the information was "publicly" available.

The regulators rejected these assertions., The company's connection with Canadians was manifest having collected millions of images of individuals in Canada and actively marketed its services to Canadian law enforcement agencies. The Commissioners reminded Clearview AI that information from sources such as social media or professional profiles, collected from public websites and then used for an unrelated purpose, does not fall under the "publicly available" exceptions provided for by the law. The report also noted the potential risks to individuals whose images were included in the database, both in terms of misidentification and exposure to potential data breaches.

Clearview AI's practices illustrate a wider threat to individuals' privacy posed by the proliferation of facial recognition and other types of artificial intelligence. Commissioner McEvoy emphasized the urgent need for law reform to address these challenges early on: "The results of our work also point to the need to strengthen our privacy laws to properly protect the public from the growing threat of these technologies to their personal information rights." ●

READ: *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information and Privacy Commissioner of Alberta* (oipc.bc.ca)

HIGHLIGHTS

LifeLabs breach affected millions of Canadians

We give some of our most sensitive information to medical laboratories for testing, with the expectation that this information will be securely protected. Yet a joint investigation by the Information and Privacy Commissioners of BC and Ontario found that LifeLabs, a major Canadian laboratory testing company, had a significant breach in 2019 when it failed to protect the personal health information of millions of Canadians. The investigation revealed that the company's failure to implement reasonable safeguards to protect personal health information violated BC and Ontario privacy laws. Both offices ordered LifeLabs to implement a number of measures to address the company's shortcomings. However, publication of the report was put on hold due to LifeLabs' claims that information it provided to the commissioners was privileged or otherwise confidential. The commissioners rejected these claims, and the matter is proceeding in court.

PIPA Review underway with Special Committee

Every six years, the Special Committee to Review the Personal Information Protection Act undertakes a statutory review of BC's private sector privacy legislation. The committee holds public hearings and accepts written submissions to inform the recommendations they make to government in a written report. Commissioner McEvoy made three presentations to the special committee in 2020-21, recommending long overdue and critically important enhancements to PIPA, such as mandatory breach notification, administrative monetary penalties, and modernizing consent requirements. He noted that PIPA was drafted almost 20 years ago under very different conditions from those under which we live today. The OIPC's recommendations to government focus on legislative amendments that will make BC a leader in Canada and help the province keep pace globally with the rapidly expanding digital economy, in harmony with other jurisdictions. While government is ultimately responsible for implementing the special committee's recommendations, Commissioner McEvoy said that it is his hope that government chooses to modernize PIPA without delay.

Commissioner determines s. 25 of FIPPA does not require Ministry of Health to disclose requested COVID-19 information

In September 2020 the OIPC received a s. 25 complaint from the Nuu-chah-nulth Tribal Council, Heiltsuk Nation, and Tsilhqot'in National Government that the Ministry of Health and several other public bodies failed to disclose specified information relating to cases of COVID-19 in neighbouring communities. Section 25(1)(a) of FIPPA requires a public body to, "without delay, disclose to the public, to an affected group of people or to an applicant… information about a risk of significant harm to the environment or to the health or safety of the public or a group of people."

Commissioner McEvoy determined that the *Public Health Act* did not override the Ministry's responsibility under s. 25. However, he held that while COVID-19 creates a risk of significant harm to the public, there was sufficient information already available on COVID-19 to enable the public, and the three indigenous governments, to take steps to avoid or mitigate the risks connected with COVID-19.

OIPC continues critical collaboration with international regulators

The OIPC continued its leadership role as Secretariat for the Asia Pacific Privacy Authorities (APPA) in 2020-21. In this role, which the office has held since 2016, the OIPC coordinates the activities of the 19-member organization and organizes twice-annual forums. APPA members share information about common investigatory matters and exchange ideas about emerging privacy issues, new technologies, the management of privacy enquiries and complaints, and the pressing need in many jurisdictions for legislative reform.

The OIPC also continued its leadership role in the Global Privacy Enforcement Network (GPEN), coordinating and hosting monthly presentations via teleconference. Along with the GPEN's 69 members, the OIPC also conducts privacy "sweeps" and takes part in advocacy, enforcement, and communications efforts.

Commissioner finds public bodies need to act to categorize and proactively disclose records

Section 71 of the *Freedom of Information and Protection of Privacy Act* (FIPPA) requires public bodies to create categories of records that are available without an access to information request. To determine if and how public bodies are complying with this requirement, the OIPC surveyed 30 public bodies and asked them to provide a list of established categories of records, and examples of records within those categories.

Investigation Report 20-01: Section 71: Categories of records available without a request found that while some public bodies comply with their obligations under FIPPA, many need to do more to meet their legal obligations.

The report emphasized that public bodies should create categories of records that are meaningful under FIPPA, a statute that was designed to promote transparency and public sector accountability. These categories must be established in a way that enables staff and the public to know which records can be routinely released.

The report offered three recommendations for all public bodies in British Columbia:

- All public bodies should establish additional categories of records;
- Categories of records should be published and easily accessible to everyone; and
- Government should update its Open Information and Open Data Policy to include guidance and tools to help ministries identify and establish categories of records.

YEAR IN REVIEW

April 1, 2020-March 31, 2021

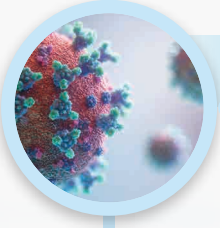
April 2020

01 First day of reporting period.

08 OIPC issues FIPPA and online learning during the COVID-19 pandemic guidance document.

22 Commissioner increases the period in which the head of each public body in BC is permitted to extend the time provided under FIPPA to respond to a freedom of information request for requests received between May 1 and May 15, 2020.

28 Commissioner delivers speech on the OIPC's work to the Select Standing Committee on Finance and Government Services.



May 2020

07 Commissioner and other Canadian regulators issue a statement calling on government to ensure COVID-19 contact tracing applications respect privacy.

June 2020

02 Commissioner McEvoy provides a general briefing to the Special Committee to Review the *Personal Information Protection Act*.

02 - 04 The OIPC joins regulators from around the Asia-Pacific region for the 53rd APPA Forum, hosted virtually by Personal Data Protection Commissioner of Singapore.

11 The OIPC releases Section 71: Categories of records available without a request report and calls for public bodies to categorize and communicate proactively disclosed records.

15 OIPC issues Privacy tips for seniors: Protect your personal information brochure with the Office of the Senior's Advocate on World Elder Abuse Awareness Day.

15 Select Standing Committee on Finance and Government Services releases Interim Report on Statutory Offices

25 OIPC and Ontario Information and Privacy Commissioner issue a media release about their findings that LifeLabs failed to protect the personal health information of millions of Canadians in 2019 breach.

29 OIPC BC, Office of the Privacy Commissioner of Canada (OPC), La Commission d'accès à l'information du Québec (CAI) and the OIPC Alberta launch a joint investigation into Tim Hortons app over geolocation tracking concerns.

July 2020

31 The OIPC releases Collecting personal information at food and drink establishments, gatherings, and events during COVID-19 guidance document..

August 2020

27 The OIPC publishes 2019-20 Annual Report.

September 2020

01 Commissioner calls for changes to address routine violations of access to information timelines in Now is the time: A report card on government's access to information timeliness – April 1, 2017 – March 31, 2020 report.

16 Commissioner presents submission to the Special Committee to Review the *Personal Information Protection Act* (supplemental submission follows on February 23).

28 Right to Know Week begins. Commissioner issues statement emphasizing importance of access rights, particularly amid challenges such as the COVID-19 pandemic, and joins virtual Commissioners' Panel hosted by the Public Service Information Community Connection (PSICC).

30 Commissioner presents to the BC Freedom of Information and Privacy Association InfoSummit.

October 2020

13 - 15 OIPC joins the virtual Global Privacy Assembly's Annual Meeting.

29 OIPC BC, OPC and OIPC Alberta issue investigation report finding that Cadillac Fairview collected 5 million shoppers' images without consent.

29 Commissioner presents to the Federal Provincial and Territorial Privacy and Access Subcommittee.

30 The OIPC issues Securing personal information: A self-assessment for public bodies and organizations guidance document.

November 2020

25 Commissioner announces review of BC's licensed private sector liquor and cannabis retailers.

27 Commissioner delivers a speech to the Canadian Bar Association, British Columbia (CBABC).

December 2020

08 - 10 The OIPC joins the 54th APPA Forum, hosted virtually by the Office of the Victorian Information Commissioner based in Melbourne, Australia.

17 Commissioner issues Order F20-57, finding that the Ministry of Health did not need to disclose records requested under S. 25 of FIPPA by three First Nations.

January 2021

25 Commissioner submits OIPC's Budget and Service Plan 2021/22-2023/24 to the Select Standing Committee on Finance and Government Services.

February 2021

02 Commissioner joins counterparts from Ontario and Alberta on a panel about legislative reform as part of 2021 Data Privacy Week panel hosted by the Public Service Information Community Connection (PSICC).

03 OIPC BC, OPC, CAI Quebec and OIPC Alberta issue investigation report finding Clearview AI clearly violated Canadians' privacy rights.

05 Commissioner delivers keynote address, Privacy, profit and the pandemic: Where we go from here, to the Victoria Privacy and Security Conference.

March 2021

03 The OIPC issues Common or integrated programs or activities guidance document.

31 End of reporting period.

SUMMARY OF COMPLIANCE:
OIPC investigation and special reports 2020-21

INVESTIGATION/SPECIAL REPORT/AUDIT	SUMMARY/STATUS
JUNE 11, 2020 ***Investigation Report 20-01:*** ***Section 71: Categories of records available without a request***	This investigation surveyed 30 public bodies to determine compliance with FIPPA's s. 71 requirement to establish categories of records available without an access to information request. The investigation found that the approach public bodies took to this section of the Act was inconsistent. The report provided three recommendations, all of which have been implemented to the OIPC's satisfaction.
JUNE 25, 2020 ***Joint Investigation into LifeLabs Data Breach*** **Information and Privacy Commissioner of Ontario PHIPA Decision 122** **Information and Privacy Commissioner for British Columbia Investigation Report 20-02**	This joint investigation examined a cyberattack on LifeLabs' computer systems that affected millions of Canadians. The report has not yet been published pending court processes relating to LifeLabs' claim that some of the information in the report is privileged or confidential. The Commissioners issued five orders to LifeLabs. All orders have been implemented to the IPC and OIPC's satisfaction.
SEPTEMBER 2, 2020 **Special Report** ***Now is the time: A report card on government's access to information timeliness April 1, 2017-March 31, 2021***	This is the fifth special report in a series on the timeliness of government's management of access to information requests. While response times improved since the OIPC's last report in 2017, government failed to comply with FIPPA's legislated timelines in thousands of cases. All four recommendations in the report have been implemented.

INVESTIGATION/SPECIAL REPORT/AUDIT	SUMMARY/STATUS
OCTOBER 29, 2020 ***Investigation Report 20-03:*** ***Report of Findings: Joint investigation of The Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia***	This joint investigation examined whether Cadillac Fairview collected and used personal information, including sensitive biometric information, without valid consent. The report found that Cadillac Fairview used facial recognition without customers' consent to generate additional personal information about individuals, such as estimated age and gender. All four recommendations have been implemented.
FEBRUARY 3, 2021 ***Investigation Report 21-01:*** ***Report of findings: Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta***	This joint investigation looked into the practices of Clearview AI, an American facial recognition company. Its technology allowed law enforcement and commercial organizations to match photographs of unknown people against the company's databank of more than 3 billion images of Canadians, including children. The Commissioners found that Clearview AI collected highly sensitive biometric information without the knowledge or consent of individuals for inappropriate purposes. The report made three recommendations, one of which was to cease operations in Canada. Clearview AI agreed to stop offering its services in Canada for a period of two years. However, the company objected to implementing the remaining two recommendations to cease collecting images of individuals in Canada and to delete the ones they have already collected.". Should Clearview AI maintain its refusal, the commissioners will pursue other actions available under their respective Acts to bring Clearview AI into compliance with Canadian laws.

YEAR IN NUMBERS

TABLE 1. Year in Numbers Summary of all FIPPA and PIPA files received in 2020-21

FILE TYPE	Received 20/21	Closed 20/21	Received 19/20	Closed 19/20
Privacy breach notification	238	236	209	209
Privacy complaints	227	232	274	292
Access complaints	386	367	382	433
Requests for review				
Requests for review of decisions to withhold information	415	463	477	489
Deemed Refusal	177	163	184	194
Applications to disregard requests as frivolous or vexatious	14	15	9	7
Time extensions				
Requests by public bodies and private organizations	4,029	4,039	6,591	6,585
Requests by applicants seeking a review	27	31	32	30
Time Extensions reported under Commissioner's Decision	1,856	1,856		
Public interest notification (s.25)	17	17	12	16
Request for reconsideration				
Requests for reconsideration of OIPC decisions	65	53	55	55
Information requested/received				
Requests for information and correspondence received	5,364	5,370	4,528	4,525
Non-jurisdictional issue	14	13	14	15
No reviewable issue	78	80	113	130
Request for Contact Information (research)	0	0	0	0
Media inquiries	149	163	137	128
FOI requests for OIPC records	14	14	18	18
Adjudications of OIPC decisions	0	0	0 *	0 *
Commissioner initiated reports				
Privacy Reports		3		3
Access Reports		2		0
Policy or issue consultation	380	382	407	434
Legislative reviews	14	14	47	49
Police Act IIO reports	48	48	64	65
Privacy impact assessments	97	101	69	85
Public education and outreach				
Speaking engagements	40	40	42	46
Meetings with public bodies and private organizations	24	22	36	44
Other (section 56 and internal reviews)	281	279	301	305
TOTAL	**13,954**	**14,003**	**14,001**	**14,157**

*these numbers have been corrected since the last reporting period.

TABLE 2. Breakdown of access complaints received in 2020-21 (FIPPA and PIPA)	
Duty required by Act	58
Time extension by public body	21
Adequate search	226
Fees	55
No notification issued	24
Total	**384**

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 3. Breakdown of privacy complaints received in 2020-21 (FIPPA and PIPA)	
Accuracy	0
Collection	53
Use	15
Disclosure	99
Retention	9
Correction	24
Protection	22
Total	**222**

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.

YEAR IN NUMBERS

TABLE 4. Number of FIPPA complaints and requests for review received in 2020-21 by public body

Public body	Complaints received	Requests for review received	Total
Ministry of Health	42	20	**62**
Provincial Health Services Authority	22	26	**48**
Island Health	24	19	**43**
Insurance Corporation of British Columbia	20	22	**42**
City of Vancouver	21	17	**38**
Vancouver Police Department	7	29	**36**
Vancouver Coastal Authority	9	26	**35**
Ministry of Children and Family Development	7	26	**33**
Ministry of Finance	15	17	**32**
Fraser Health	3	18	**21**
Top 10 totals	**170**	**220**	**390**
All other public bodies	264	305	**569**
Total	**434**	**525**	**959**

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 2020-21 by sector

Sector	Complaints received	Requests for review received	Total
Services	61	12	**73**
Health	28	14	**42**
Professional science & technology	18	12	**30**
Real Estate	19	5	**24**
Retail/Trade	13	6	**19**
Finance/Insurance	10	4	**14**
Administrative support	6	2	**8**
Accommodation	7	0	**7**
Education	5	2	**7**
Info/Cultural	4	1	**5**
Top 10 total	**174**	**64**	**238**
Other	5	3	**8**
Total	**179**	**67**	**246**

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 2020-21, FIPPA

Type	Investigation	Declined to investigate/ discontinued	Hearing or report	Total
Adequate Search	105	97	4	**206**
Duty	24	12	0	**36**
Fees	25	17	2	**44**
Time extension by public body	19	3	0	**22**
S 25 Not Applied	6	11	1	**18**
TOTAL	**179**	**140**	**7**	**326**

TABLE 7. Outcome of access complaints resolved in 2020-21, PIPA

Type	Investigation	Declined to investigate/ discontinued	Hearing or report	Total
Adequate Search	17	11	0	**28**
Duty	4	5	0	**9**
Fees	2	0	0	**2**
Time Extension by Organization	2	0	0	**2**
TOTAL	**25**	**16**	**0**	**41**

YEAR IN NUMBERS

TABLE 8. Outcome of privacy complaints resolved in 2020-21, FIPPA

Type	Investigation	No investigation	Hearing or report	Total
Collection	12	7	0	19
Correction	8	6	0	14
Disclosure	36	11	2	49
Retention	3	1	0	4
Use	1	2	0	3
Protection	6	4	0	10
TOTAL	**66**	**31**	**2**	**99**

TABLE 9. Outcome of privacy complaints resolved in 2020-21, PIPA

Type	Investigation	No investigation	Hearing or report	Total
Collection	26	13	3	42
Correction	4	6	0	10
Disclosure	37	14	3	54
Retention	4	1	0	5
Use	6	1	0	7
Protection	5	10	0	15
TOTAL	**82**	**45**	**6**	**133**

TABLE 10. Outcome of requests for review resolved in 2020-21, FIPPA

Type	Mediated	Declined to investigate/ discontinued	Hearing/consent order/other	Total
Deemed refusal	116	2	14	**132**
Deny	56	3	25	**84**
Notwithstanding	1	0	1	**2**
Partial Access	206	4	73	**283**
Refusal to confirm or deny	6	0	6	**12**
Scope	6	0	9	**15**
Third Party	25	0	10	**35**
Total	**416**	**9**	**138**	**563**

TABLE 11. Outcome of requests for review resolved in 2020-21 PIPA

Type	Mediated/Resolved	Declined to investigate/ discontinued	Hearing or report	Total
Deemed refusal	29	2	0	**31**
Deny Access	12	0	4	**16**
Partial Access	12	0	4	**16**
Totals	**53**	**2**	**8**	**63**

TABLE 12. Outcome of all complaints resolved by the OIPC (FIPPA and PIPA) in 2020-21

Investigations	No investigations	Declined to investigate/ discontinued	Hearing or report	Total
352	200	32	15	**599**

TABLE 13. Outcome of all requests for review resolved by the OIPC (FIPPA and PIPA) in 2020-21

Mediated	Hearing or report	Declined to investigate/ discontinued	Total
469	146	11	626

ADJUDICATION

The number of inquiry requests to the OIPC increased from 119 in 2019-20 to 155 in 2020-21. In total, adjudicators issued 68 orders, an increase from 45 in the previous fiscal year.

One issue that adjudicators faced in 2020-21 focused on s. 6(2) of FIPPA, which requires the head of a public body to make every reasonable effort to assist applicants and to respond without delay. As part of this requirement, the "head of a public body must create a record for an applicant if (a) the record can be created from a machine readable record … and (b) creating the record would not unreasonably interfere with the operations of a public body."

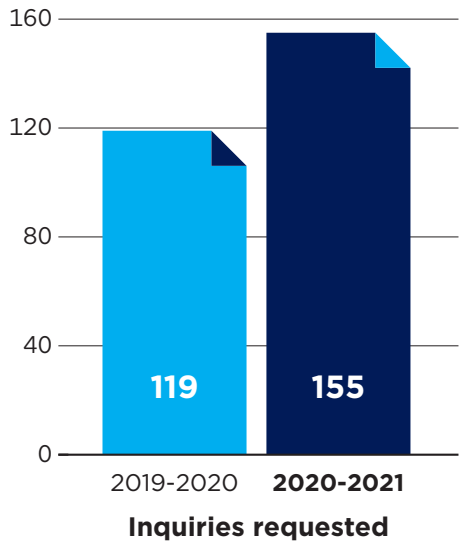
An adjudicator explored this section of FIPPA in F21-07, when a complainant was denied a response to access requests to all BC government ministries and the Office of the Premier for lists of certain file and folder names on specific electronic devices.

In a joint submission, the public bodies stated that any method to create the requested records would unreasonably interfere with their operations, as a program would need to be developed to do so. However, aside from the number of hours it would take to develop such a program, the public bodies did not provide estimates showing how costly a program would be or other budgetary considerations involved.

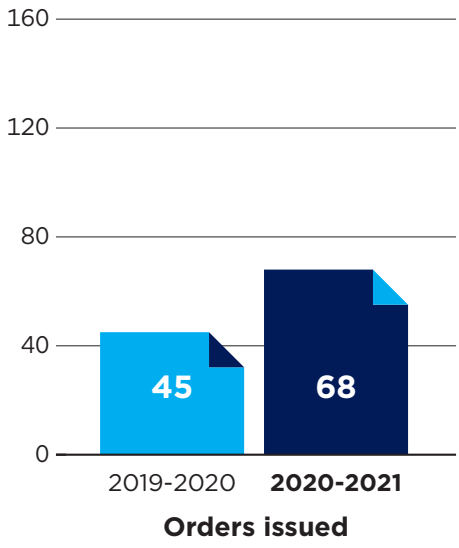
The adjudicator determined that the public bodies were required to create the records, as the requested records could be created from a machine readable record using the public bodies' normal computer hardware, software and technical expertise and it would not unreasonably interfere with the public bodies' operations.

The adjudication team also saw an increase in orders that dealt with s. 43 of FIPPA, or the power to authorize a public body to disregard requests that are repetitive, frivolous or vexatious. In three of six requests, adjudicators granted permission to the public bodies to disregard the requests because the requests were vexatious, repetitive or systematics.

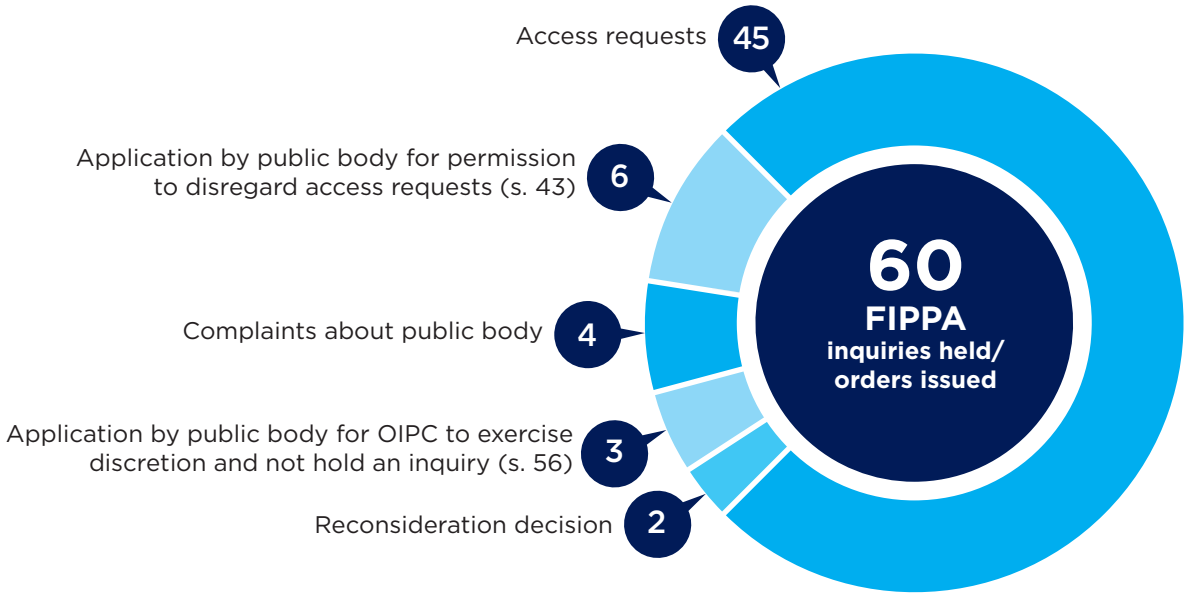
*See pg. 19 for a summary of Order F20-57, Ministry of Health, that addressed a s. 25 complaint from the Nuu-chah-nulth Tribal Council, Heiltsuk Nation, and Tsilhqot'in National Government.

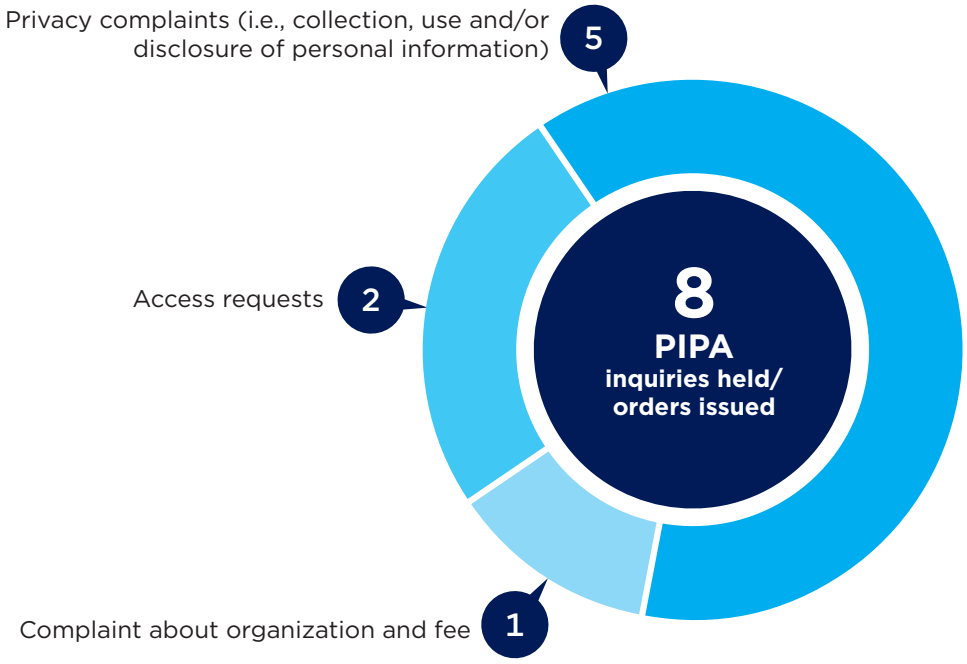


Inquiries requested



Orders issued


Access requests 45
Application by public body for permission to disregard access requests (s. 43) 6
Complaints about public body 4
Application by public body for OIPC to exercise discretion and not hold an inquiry (s. 56) 3
Reconsideration decision 2
60
FIPPA
inquiries held/
orders issued


Privacy complaints (i.e., collection, use and/or disclosure of personal information) 5
Access requests 2
Complaint about organization and fee 1
8
PIPA
inquiries held/
orders issued

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 bodies 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*.

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:

2020-21	Operating	Capital
Appropriation	$6,942,000	$543,944
Total operating expenses	$6,941,724	-
Capital acquisitions	-	$27,595
Unused appropriation	$276	$1,405

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

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).

2020-21	Closing cost	Closing accumulated amortization	Net book value (March 31/21)
Computer hardware and software	$675,601	($224,338)	$451,264
Tenant improvements	$0	$0	$0
Furniture and equipment	$30,313	($22,387)	$7,925
Total tangible capital assets	**$705,914**	**($246,725)**	**$459,189**

Note: A large number of capital assets were retired in FY 2021

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

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

The Office of the Information and Privacy Commissioner and the Office of the Registrar of Lobbyists have not had any investigations or disclosures under PIDA between April 1, 2020 and March 31, 2021.

OUTREACH

Commissioner McEvoy and OIPC staff are frequent speakers and participants at events and conferences throughout British Columbia and beyond.

Here are some of the events that featured OIPC speakers and presenters during the 2020-21 fiscal year:

22nd Annual Privacy and Security Conference
BC FIPA InfoSummit
BC Privacy Professionals
BC Teachers Federation
Better Business Bureau
Camosun College
Canadian Bar Association Privacy Law Section
Ending Violence Association
FPT Privacy and Access Subcommittee
GRC World Forum
Health Info Management
Identity North
Landlord BC
Oak Bay Probus Club
Oak Centre Child & Youth Advocacy Centre
Regional District of Okanagan Similkameen
Sedona Conference DPA Roundtable
Transition House
UBC iSchool
University of Victoria
Verney Conference Management: Right to Know Week Commissioners Panel

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)

- Collecting personal information at food and drink establishments, gatherings, and events during COVID-19
- Direct-to-consumer genetic testing and privacy
- Disclosure of personal information of individuals in crisis
- Employee privacy rights
- FIPPA and online learning during the COVID-19 pandemic
- Guide to using overt video surveillance
- Guide for organizations collecting personal information online
- Identity theft resources
- Information sharing agreements
- Instructions for Written Inquiries
- Obtaining meaningful consent
- Privacy proofing your retail business
- Privacy tips for seniors: Protect your personal information
- Private sector landlords and tenants
- Protecting personal information: cannabis transactions
- Protecting personal information away from the office
- Responding to PIPA privacy complaints
- Securing personal information: A self-assessment for public bodies and organizations

Comprehensive privacy management

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

Privacy breaches

- 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 workspaces

oipc
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