Office of the Information and
Privacy Commissioner of Alberta

ANNUAL REPORT
2020-21

Office of the Information and
Privacy Commissioner of Alberta

Office of the Information and
Privacy Commissioner of Alberta
410, 9925 - 109 Street, NW
Edmonton, AB T5K 2J8

Phone: 780.422.6860
Toll Free: 1.888.878.4044
Fax: 780.422.5682
Email: generalinfo@oipc.ab.ca
Twitter: @ABoipc

www.oipc.ab.ca

NOVEMBER 2021

Office of the Information and
Privacy Commissioner of Alberta

November 2021

Honourable Nathan Cooper
Speaker of the Legislative Assembly
325 Legislature Building
10800 - 97 Avenue
Edmonton, AB T5K 2B6

Dear Mr. Speaker:

I am honoured to present to the Legislative Assembly the Annual Report of the Office of the Information and Privacy Commissioner for the period April 1, 2020 to March 31, 2021.

This report is provided in accordance with section 63(1) of the *Freedom of Information and Protection of Privacy Act,* section 95(1) of the *Health Information Act* and section 44(1) of the *Personal Information Protection Act.*

Sincerely,

Original signed by
Jill Clayton
Information and Privacy Commissioner

Table of Contents

Commissioner's Message

This past year was a year like no other for access to information and protection of privacy in Alberta as the COVID-19 pandemic raised new challenges for regulated stakeholders and my office.

Work from home mandates significantly affected Alberta's access to information system. Public body staff had difficulties retrieving records, challenging their ability to respond to access requests within legislated timeframes under the *Freedom of Information and Protection of Privacy Act* (FOIP Act). My office also noticed an increase in the time it took for public body staff to respond to our requests for information during our review of public body responses to access requests.

Health custodians were adopting new technology solutions *en masse* for the provision of health care when it was not possible to see patients in person. My office received notice of over 150 implementations of new virtual care technologies within weeks of the global pandemic declaration, and hundreds of privacy impact assessments (PIAs) were submitted on these projects throughout 2020-21.

Private sector businesses fully leveraged cloud-based services and other digital communications technologies to work from home, but doing so brought additional privacy and security considerations. Work from home realities resulted in my office seeing an increase in reports of breaches related to transporting documents or devices between homes and offices, and an increase in reports of misdirected emails.

To respond to the new challenges faced by regulated entities, our office produced guidance to assist them in understanding how access and privacy laws applied in a public health emergency. We also consulted with our regulator colleagues across Canada and globally to share information, speak with a united voice on important topics and learn from each other's experiences.

While new processes and technologies added challenges, some realities for my office continued, including an ever-increasing caseload. We saw a 14% increase in cases opened in 2020-21, from 3,658 to 4,166.

Despite work from home challenges presented by the pandemic, I am pleased to report that we closed 18% more cases in 2020-21. I am incredibly proud of my colleagues for this accomplishment. As an office, we pivoted on a dime to work from home and everyone rose to the challenge. I cannot thank my staff enough.

As we continue work from home arrangements, it is clear that we will not revert to the way things were in the office. In its way, the pandemic accelerated changes that were likely in any event and it will be exciting to see what takes hold, and what other opportunities arise.

For me, however, I will be watching these changes from a new perspective. My second five-year term as Information and Privacy Commissioner of Alberta ends on January 31, 2022, and I am not seeking reappointment. Nevertheless, I will be keenly observing progress on the following topics in Alberta.

PRIVACY AND TECHNOLOGY

Over 17 years with the OIPC, including 10 as Commissioner, there has been one constant: The privacy challenges presented by new technologies.

We are fortunate in Alberta to have privacy laws that are grounded in near universal principles. As such, these laws provide a useful, objective and flexible framework to support robust assessment of new technologies to help ensure they realize their promise, while still protecting individual privacy. Some of these new technologies, however, are straining our existing legislative models beyond their limits.

Virtual Care

The most significant development on our office's oversight role has been the almost overnight deployment of virtual care apps by health custodians. Patients and health care providers have welcomed these technology solutions during the pandemic. Having now reviewed numerous PIAs for different products, however, my office sees some concerning trends.

In the past, technology solutions for the health sector recognized the special nature of health information. Custodians thoughtfully deliberated to ensure compliance with the unique accountability framework established by Alberta's *Health Information Act* (HIA). The rapid deployment of virtual care apps and other technology solutions, however, has resulted in some custodians overlooking HIA's rigorous risk mitigation and safeguarding provisions meant to protect Albertans' health information. The potential outcomes include loss of control by custodians and patients, and commercialization of health care practices and individuals' health information.

Facial Recognition Technology (FRT)

My office's 2019-20 Annual Report highlighted the ubiquitous use of facial recognition technologies (FRT) and resulting global reaction, including investigations, studies, bans or moratoria on use of the technology.

In 2020-21, my office, along with colleagues in BC, Quebec and federally, jointly released our investigation report into Clearview AI. The investigation found Clearview AI scraped billions of images of people from across the internet and offered its database to law enforcement and businesses in order to match photographs of unknown people for identification purposes. We found that Clearview's practices represented mass surveillance and were a violation of Canada's privacy laws.

Similarly, a joint investigation of Cadillac Fairview found the use of FRT to be non-compliant with privacy laws.

These investigations are just the tip of the iceberg. Use of FRT is increasing, raising important questions about whether the technology is appropriate in certain settings. One of the important questions is whether our existing privacy laws are up to the task of regulating this technology. I expect FRT to continue to be a prominent and vexing challenge for privacy regulators for years to come.

Artificial Intelligence and Machine Learning

Like FRT, advances in computing capabilities have contributed to many new, unique and sometimes troubling uses of artificial intelligence (AI) and machine learning for automated decision-making.

Regulating the design, use and deployment of AI poses many challenges for privacy authorities. Certain uses of AI technologies require massive amounts of personal information to operate effectively. At the same time, what personal information is being used and why decisions are being made often seem to take place in a "black box", raising questions about transparency and ethics, including potential discrimination and bias. Another challenge is that there can be insufficient oversight by regulators, in part due to claims that these technologies use "de-identified data" such that privacy laws may not apply.

Similar to the challenges posed by FRT, the question remains as to whether existing privacy laws are fit for the purpose of regulating AI and machine learning when there are implications for individuals' rights. It may be that this technology demands a new and innovative legislative approach.

ACCESS TO INFORMATION

Over the past 10 years as Commissioner, there have been many ups and downs for Alberta's access to information system.

Back in 2012-13, there seemed to be new energy and focus on access to information. The Government of Alberta (GoA) committed to a review of the FOIP Act, new transparency programs for disclosing expenses and compensation were implemented, and there was resourcing and support for open government initiatives.

This is in contrast to 2015-16 when I reported that, "Access to information in Alberta is fast approaching a crisis situation." No amendments resulted from the GoA's 2013 review of the FOIP Act, hopes that open government programs would result in a reduction of access requests did not come to fruition, and we saw concerning case trends, such as a significant increase in access requests that resulted in no response from public bodies (also known as "deemed refusals"). My office also experienced public bodies refusing to provide records to my office for reviews and an increase in court challenges.

The situation continued to deteriorate. In February 2017, we released investigation reports that focused attention on delays in responding to access to information requests by three GoA departments. The reports found common themes: A significant increase in the number and complexity of access requests received by public bodies, process issues, and a lack of staffing and resources. In particular, the reports noted that GoA senior leadership needed to convey a clear commitment to access and openness. In other words, a culture change was required to improve the system.

Since then, the provincial government has taken steps to address the problem, including centralizing the processing of access requests and, more recently, upgrading the information system used to manage and administer access to information.

It is too soon to know whether these changes are sufficient. The centralization was barely underway before the pandemic upended our work lives, and new technology is often not the silver bullet that we want it to be when system pressures arise.

Stats in my office show that system challenges persist. We continue to see increases in the number of time extension requests made to my office, with GoA departments often citing staff shortages, unfilled vacancies, and large and complicated requests as the reasons for requesting a time extension to respond to access requests. Despite the valiant and dedicated efforts of FOIP staff, it appears impossible to keep up with demands given system design and resourcing.

As we move towards a post-pandemic world, it would be worthwhile for government – or an independent regulator, for that matter – to review the implementation and impacts of centralization with a view to determining if it has achieved its objectives, and to consider if FOIP processes and resourcing are adequate to meet demands.

LEGISLATIVE REFORM

In the 2019-20 Annual Report, I said that all thee of Alberta's access and privacy laws were due for modernization, in part to address some of the challenges I have described above. I said I would be writing to the Ministers responsible for Alberta's access and privacy laws to ask that they turn their attention to these matters.

Shortly thereafter, the government introduced Bill 46, which proposed significant amendments to Alberta's HIA. Unfortunately, amendments were introduced without the benefit of meaningful consultation with my office and, in my view, failed to address some of the most pressing issues of today, while increasing risk to Albertans' privacy. I was disappointed at the missed opportunity, and said so publicly.

That said, I am optimistic about the government's efforts for possible reform of the FOIP Act and *Personal Information Protection Act* (PIPA).

In November 2020, I wrote to the Minister of Service Alberta setting out my office's priority recommendations for amending these laws. To date, I am encouraged by the meaningful consultation that my colleagues and I have had with the Minister and ministry staff, and with the GoA's efforts to engage with the public and other stakeholders.

With respect to the FOIP Act and PIPA, the issues being discussed are modern and relevant, including privacy management programs, automated decision-making and enhanced enforcement. A respectful, meaningful, transparent and accountable engagement process will go a long way to ensuring Alberta achieves the right balance in modernizing these important laws.

Over the ensuing years, I will be following access and privacy issues in Alberta with much interest as they unfold under the direction of a new Commissioner.

For now though, I will say it has been a great honour and privilege to serve two terms as the Information and Privacy Commissioner of Alberta. This is in large part due to my exceptional colleagues, and I thank them for their efforts, especially over the last year during such a challenging time.

Jill Clayton
Information and Privacy Commissioner

Passing of Robert C. Clark

The Commissioner issued the following statement on July 13, 2020:

> Alberta has lost a great community builder and leader with the recent passing of Robert C. Clark, Alberta's first Information and Privacy Commissioner.
>
> Bob was appointed to the role of Information and Privacy Commissioner on May 31, 1995, and led the development of the Office of the Information and Privacy Commissioner in its formative years.
>
> He saw the office through the expansion of the application of the *Freedom of Information and Protection of Privacy Act* from government ministries in 1995, to school jurisdictions and health care bodies in 1998, and to post-secondary institutions and local government bodies in 1999. During his last year as Commissioner, the Health Information Act was added to his list of oversight responsibilities.
>
> Bob exemplified the leadership he was already known for in political and community circles in developing the OIPC. He recognized from the start that he was not just a regulator. He was also an educator and an advocate for the principles of access to information and privacy, and he was willing to engage politicians, interest groups and stakeholders in those discussions.
>
> At the same time, Bob appreciated that the FOIP Act was complex and that if it was going to be successful, it had to be workable for the smaller, less resourced public bodies. Although he was no longer Commissioner when the *Personal Information Protection Act* was enacted in 2004, his common sense, real life approach can be seen in the drafting of that Act, which considers the interests of small- to medium-sized businesses.
>
> Governments can enact freedom of information legislation but unless there is a champion – an advocate for the principles – the legislation languishes and is merely symbolic. Although Bob resigned as Information and Privacy Commissioner in 2001, he left an indelible imprint on the access and privacy world in Alberta. His legacy lives on today.
>
> My condolences and best wishes go to Bob's family and friends during this difficult time.

Mr. Clark had a long and storied career in public service, including as MLA, government minister, leader of the official opposition and ethics commissioner. He was also widely recognized for his contributions to his community, particularly junior hockey and post-secondary education. Premier Jason Kenney also recognized Mr. Clark's contributions to Alberta in a statement on July 10, 2020.

ABOUT
THE OFFICE

Mandate

The Information and Privacy Commissioner is an Officer of the Legislature. The Commissioner reports directly to the Legislative Assembly of Alberta and is independent of the government.

Through the Office of the Information and Privacy Commissioner (OIPC), the Commissioner performs the legislative and regulatory responsibilities set out in Alberta's three access and privacy laws.

Freedom of Information and Protection of Privacy Act

The *Freedom of Information and Protection of Privacy Act* (FOIP Act) applies to more than 1,000 public bodies, including provincial government departments, agencies, boards and commissions, municipalities, Métis settlements, drainage districts, irrigation districts, housing management bodies, school boards, post-secondary institutions, public libraries, police services, police commissions and health authorities.

The FOIP Act provides a right of access to any record in the custody or under the control of a public body, subject to limited and specific exceptions. The Act also gives individuals the right to access their own personal information held by public bodies and to request corrections to their own personal information. The Act protects privacy by setting out the circumstances in which a public body may collect, use or disclose personal information.

Health Information Act

The *Health Information Act* (HIA) applies to health custodians, including Alberta Health, Alberta Health Services, Covenant Health, nursing homes, physicians, registered nurses, pharmacists, optometrists, opticians, chiropractors, podiatrists, midwives, dentists, denturists and dental hygienists.

HIA also applies to "affiliates" who perform a service for custodians, such as employees, contractors, students and volunteers. Custodians are responsible for the information collected, used and disclosed by their affiliates.

HIA allows health services providers to exchange health information to provide care and to manage the health system.

HIA protects patients' privacy by regulating how health information may be collected, used and disclosed, and by establishing the duty for custodians to take reasonable steps to protect the confidentiality and security of health information. The Act also gives individuals the right to access their own health information, to request corrections, and to have custodians consider their wishes regarding how much of their health information is disclosed or made accessible through the provincial electronic health record information system (that is, Alberta Netcare).

Personal Information Protection Act

The *Personal Information Protection Act* (PIPA)applies to provincially regulated private sector organizations, including businesses, corporations, associations, trade unions, private schools, private colleges, partnerships, professional regulatory organizations and any individual acting in a commercial capacity.

PIPA protects the privacy of clients, customers, employees and volunteers by establishing the rules for the collection, use and disclosure of personal information by organizations.

PIPA seeks to balance the right of the individual to have their personal information protected with the need of organizations to collect, use or disclose personal information for reasonable purposes. The Act also gives individuals the right to access their own personal information held by organizations and to request corrections.

COMMISSIONER'S POWERS, DUTIES AND FUNCTIONS

The Commissioner oversees and enforces the administration of the Acts to ensure their purposes are achieved.

The Commissioner's powers, duties and functions include:

- Providing independent review and resolution on requests for review of responses to access to information requests and privacy complaints related to the collection, use and disclosure of personal and health information
- Investigating any matters relating to the application of the Acts, whether or not a review is requested
- Conducting inquiries to decide questions of fact and law and issuing binding orders
- Reviewing privacy breach reports submitted by private sector organizations and health custodians as required under PIPA and HIA, and when voluntarily submitted by public bodies
- Reviewing and commenting on privacy impact assessments submitted to the Commissioner
- Receiving comments from the public concerning the administration of the Acts
- Educating the public about the Acts, their rights under the Acts, and access and privacy issues in general
- Engaging in or commissioning research into any matter affecting the achievement of the purposes of the Acts
- Commenting on the access and privacy implications of existing or proposed legislative schemes and programs
- Giving advice and recommendations of general application respecting the rights or obligations of stakeholders under the Acts
- Commenting on the privacy and security implications of using or disclosing personal and health information for record linkages or for the purpose of performing data matching

VISION

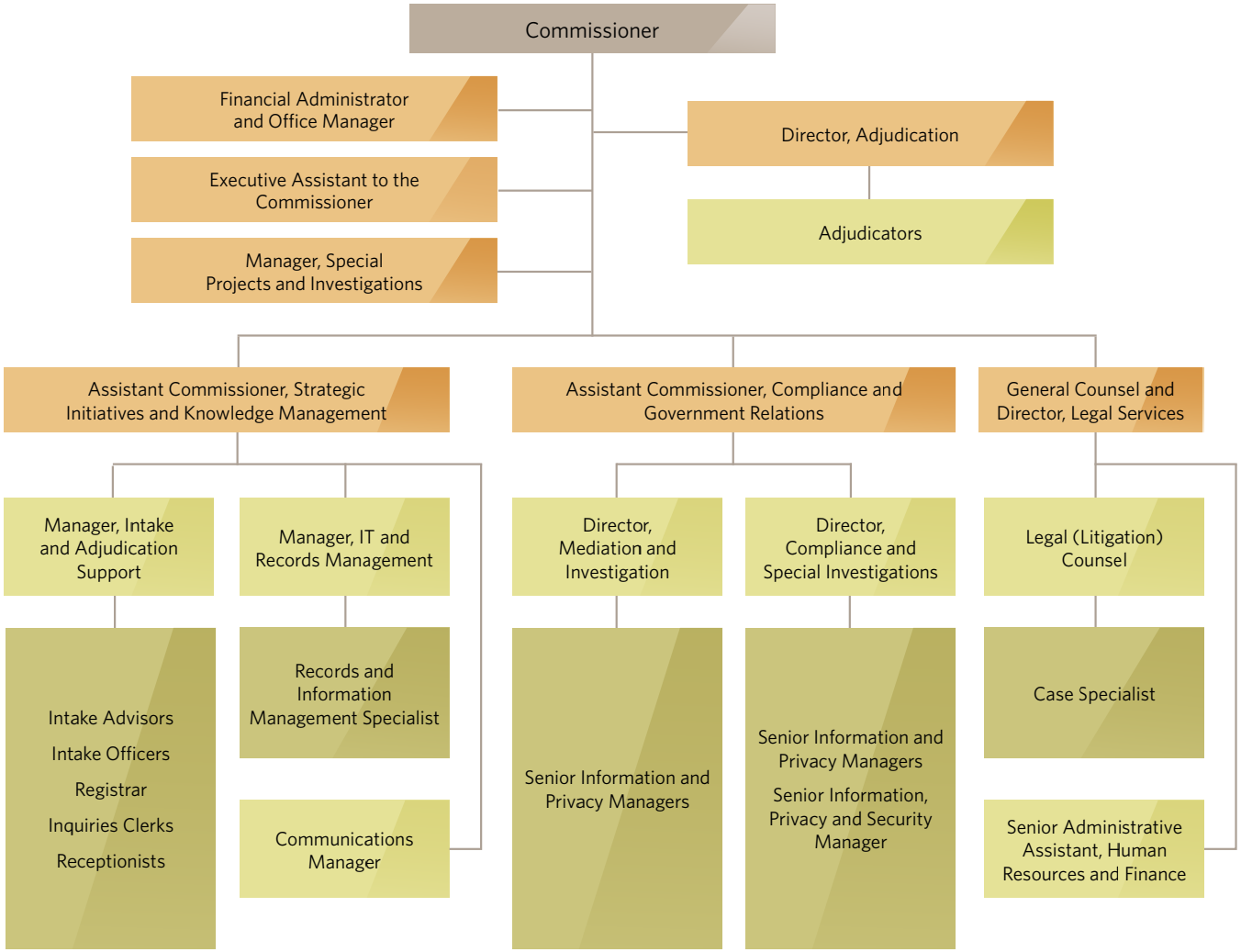
A society that values and respects access to information and personal privacy.

MISSION

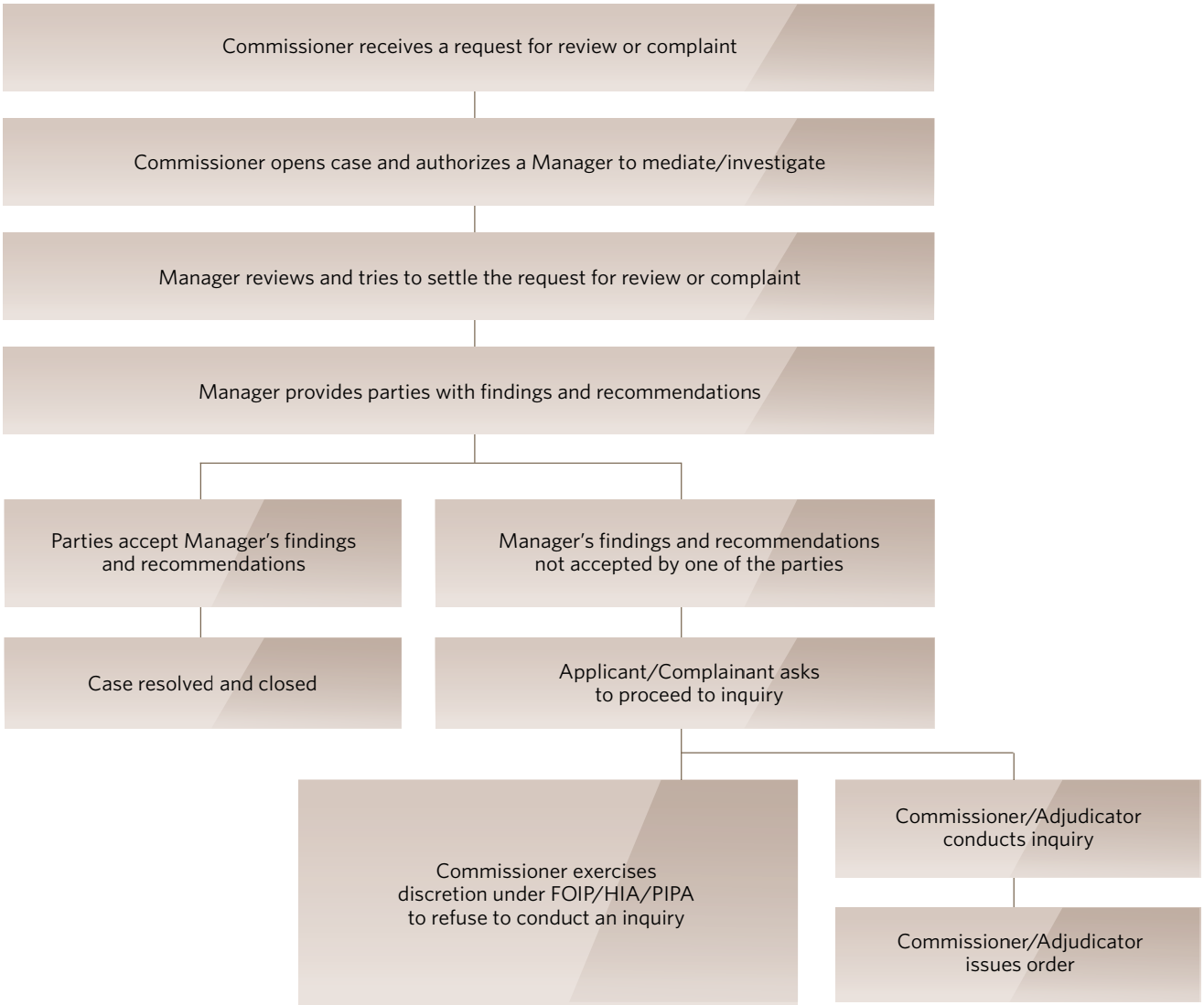
Our work toward supporting our vision includes:

- Advocating for the access and privacy rights of Albertans
- Ensuring public bodies, health custodians and private sector organizations uphold the access and privacy rights contained in the laws of Alberta
- Providing fair, independent and impartial reviews in a timely and efficient manner

Organizational Structure



Request for Review and Complaint Process



OIPC as a Public Body

FOIP REQUESTS TO THE OIPC

As a public body under the FOIP Act, the OIPC receives access requests on occasion. In 2020-21, the OIPC received two general information requests under the FOIP Act. The OIPC responded to both requests within 30 days.

Individuals who disagree with the access request response received from the OIPC can request a review of the OIPC's decision. An External Adjudicator is appointed by order in council to determine whether the OIPC properly responded to the access request, such as properly excluding records subject to the access request.

On January 5, 2021, an External Adjudicator issued Adjudication Order #12. The External Adjudicator ordered the OIPC to make contact information on independent contractors and consultants available to the applicant. Before releasing the information, the OIPC was directed to first inform the affected third parties of the request for their information, in order for them to be heard. Adjudication Order #12 is available at www.oipc.ab.ca.

Two other outstanding requests for review for which an External Adjudicator had been appointed were withdrawn by the applicant before the reviews could be heard.

As of March 31, 2021, there was one outstanding request for review for which an External Adjudicator had been appointed, but the review had not yet been heard. There was also one outstanding request for review awaiting the appointment of an External Adjudicator.

OIPC PRIVACY MATTERS

In 2020-21, the OIPC conducted six investigations into internal incidents involving potential privacy breaches.

Incident 1

A staff member inadvertently auto-filled the name of an individual outside the OIPC in an email. The staff member intended to forward the correspondence to a colleague. The correspondence contained personal information of a complainant. There was a real risk of signification harm, and the OIPC notified the complainant.

Incident 2

The OIPC inadvertently attached an unrelated email to an email sent to a privacy officer of a clinic. The unrelated email did not contain any personal or health information. The privacy officer had forwarded the email to one other individual in the clinic, who had not read the email. Both the privacy officer and the other individual deleted the email. There was no real risk of significant harm, and no notification was required.

Incident 3

The OIPC mistakenly attached an unrelated individual's request for review submission to a third party's request for review acknowledgement package. The third party who received the unrelated individual's submission in error notified the OIPC and returned the submission to the OIPC. There was no real risk of significant harm, and no notification was required.

Incident 4

An applicant's request for review submission was lost or misplaced internally within the OIPC. That determination was made on the basis that no one outside the OIPC had reported receiving records in error, which is usually the case when records have inadvertently been sent outside the OIPC. Nevertheless, given the nature of the personal information contained in the submission, there was a real risk of significant harm, and the applicant was notified about the loss.

Incident 5

Two staff members called in to a conference call. While waiting for additional participants to join, the two staff members discussed a matter related to another staff member. Unknown to the call moderator, a third staff member had joined the call and overheard a portion of the discussion. There was no real risk of significant harm as no identifiable personal information was disclosed during the call and the subject individual cannot be readily identified from the conversation. Further, the information at issue cannot be used to cause significant harm.

Incident 6

A staff member inadvertently auto-filled the name of an individual outside the OIPC in emails. The staff member intended to forward correspondence to a colleague. The correspondence contained personal information about a complainant and an attachment contained the complainant's name. The individual realized the correspondence was not for her, did not open the attachment, deleted the emails and confirmed those actions by email to the staff member. There was no real risk of significant harm, and no notification was required.

PROACTIVE TRAVEL AND EXPENSES DISCLOSURE

The OIPC continues to disclose the vehicle, travel and hosting expenses of the Commissioner, and the travel and hosting expenses of the Assistant Commissioners and Directors on a bi-monthly basis. The disclosures are available at www.oipc.ab.ca.

PUBLIC SECTOR COMPENSATION TRANSPARENCY ACT

The *Public Sector Compensation Transparency Act* requires public sector bodies, including the OIPC, to publicly disclose compensation and severance provided to an employee if it is more than $125,000 in a calendar year, as adjusted according to the Act. For the 2019 calendar year, the threshold was adjusted to $132,924. In addition, other non-monetary employer-paid benefits and pension must be reported.

This disclosure is made annually by June 30 and is available at www.oipc.ab.ca.

PUBLIC INTEREST DISCLOSURE (WHISTLEBLOWER PROTECTION) ACT

There were no disclosures received by the OIPC's designated officer under the *Public Interest Disclosure Act* in 2020-21.

Financial Overview

For the 2020-21 fiscal year, the total approved budget for the OIPC was $7,256,000. The total cost of operating expenses and capital purchases was $7,214,884. The OIPC returned $41,116 (0.57% of the total approved budget) to the Legislative Assembly.

TOTAL ACTUAL COSTS COMPARED TO BUDGET

	VOTED BUDGET	ACTUAL	DIFFERENCE
Operating Expenses*	$ 7,256,000	$ 7,059,127	$ 196,873
Capital Purchases	-	155,757	(155,757)
Total	$ 7,256,000	$ 7,214,884	$ 41,116

*Amortization is not included

Salaries, wages, and employee benefits make up approximately 85% of the OIPC's operating expenses budget. In 2020-21, payroll related costs and legal fees were under budget. Supplies and services and capital purchases were over budget.

TOTAL ACTUAL COSTS COMPARED TO PRIOR YEAR

	2020-2021	2019-2020	DIFFERENCE
Operating Expenses	$ 7,059,127	$ 6,779,170	$ 279,957
Capital Purchases	155,757	56,009	99,748
Total	$ 7,214,884	$ 6,835,179	$ 379,705

Total costs for operating expenses and capital purchases increased by $379,705 from the prior year.

TRENDS & ISSUES

COVID-19 Pandemic

CONTACT TRACING

Governments, privacy regulators, technology companies, healthcare professionals, academics and the public were engaged in discussions about contact-tracing apps in the early months of the pandemic. Many people thought digital contact tracing and exposure notifications would be pivotal in transitioning back to normal after months of public health restrictions.

In May 2020, the Government of Alberta became the first jurisdiction in Canada to launch a contact-tracing app. A PIA on the ABTraceTogether app was submitted by Alberta Health to the OIPC as required under section 63 of HIA. Given the global attention on contact-tracing apps, the Commissioner prioritized the OIPC's review of the app and in the interests of transparency published a PIA review report on the app in July 2020 (see Regulation and Enforcement section of this report).[1]

A few months later, the Government of Canada released its digital exposure notification app. The COVID Alert app took a slightly different approach in design and function. Instead of integrating with public health contact-tracing systems and staff, like ABTraceTogether, the federal app notifies potential contacts of a person diagnosed with COVID-19 through Bluetooth "handshakes", without human intervention. Nine provinces and territories opted to use COVID Alert. Alberta did not adopt COVID Alert.

The Office of the Privacy Commissioner of Canada and the Information and Privacy Commissioner of Ontario reviewed the COVID Alert app jointly. COVID Alert was first released in Ontario. The two offices compared COVID Alert against a set of principles that federal, provincial and territorial privacy commissioners issued with respect to contact-tracing apps.[2] In July 2020, the two offices found COVID Alert met all principles.[3]

Dozens of apps were released globally, with different purposes or functionalities.[4]

When comparing different apps, most discussions focused on what types of personal information were collected, whether the apps collected precise location or used Bluetooth "handshakes", whether safeguards were in place to protect against improper access (such as by law enforcement for a different purpose), and whether these apps were effective in their purpose to support public health. There was also plenty of discussion about socioeconomic barriers to accessing apps and technical challenges on certain devices.

The reviews and analyses of these apps – the effectiveness and limitations both technologically and for public health – have been fascinating. There has been a commendable level of cooperation between governments, privacy regulators, healthcare professionals, technology companies, academics and the public in introducing and reviewing these apps.

[1] OIPC, "ABTraceTogether Privacy Impact Assessment Review Report", July 2020.

[2] Joint statement by Canada's federal, provincial and territorial privacy commissioners, "Supporting public health, building public trust: Privacy principles for contact tracing and similar apps", May 7, 2020. The OIPC was reviewing the ABTraceTogether PIA when the federal, provincial and territorial privacy commissioners issued a joint statement. The Commissioner agreed with the principles, but decided to provide recommendations directly to the Government of Alberta due to an active PIA review at the time and did not sign the joint statement.

[3] Office of the Privacy Commissioner of Canada and Information and Privacy Commissioner of Ontario, "Federal and Ontario privacy commissioners support use of COVID Alert application subject to ongoing monitoring of its privacy protections and effectiveness", July 31, 2020.

[4] O'Neill, Patrick Howell, Ryan-Mosley, Tate and Johnson, Bobbie, "A flood of coronavirus apps are tracking us. Now it's time to keep track of them.", MIT Technology Review, May 7, 2020.

CUSTOMER LISTS

As COVID-19 pandemic restrictions loosened, many Alberta businesses began requiring customers' contact information before allowing entry into their premises. Some jurisdictions mandated certain types of businesses to collect patrons' contact information.[5] The purpose was to assist with contact-tracing efforts in case of a known exposure to the virus.

These collection practices raised some concerns, and there were several examples of businesses leaving paper copies of contact information in plain view. The OIPC responded to these concerns by issuing guidance to help ensure organizations comply with PIPA.[6]

The guidance provided an overview of requirements for consent and notice, reasonable purpose for collection, reasonable extent of collection, secondary use restrictions, retention, safeguarding, and customer rights. With respect to reasonable purpose for collection and reasonable extent of collection of personal information, the advisory said:

> PIPA requires that organizations collect personal information only for purposes that are reasonable and only to the extent reasonable for meeting those purposes (section 11).
>
> For example, an organization may decide as a health and safety measure for employees and customers to collect personal information in order to assist contact-tracing efforts during the COVID-19 pandemic. The organization can only collect personal information that would be reasonably required to meet the purpose. For example, it might be reasonable to collect an individual's name, cellphone number or email address, and the date and time the customer attended the store or restaurant. It is unlikely that it would be reasonable to collect other types of personal information that are not required for the purposes of contact tracing.

With respect to having a single sign-in sheet upon entry, the OIPC said:

> Organizations subject to PIPA are required to make reasonable security arrangements to protect personal information against unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction (section 34).
>
> Using a single customer sign-in sheet can disclose personal information about one customer to others.
>
> Organizations should consider how they can collect and retain the customer's personal information in a manner that does not disclose it to others, and ensure that access to this information is strictly controlled by certain employees (e.g. not all employees have access to the information).

The OIPC also reminded organizations of the obligation to have someone who can answer questions about why personal information is being collected and other privacy practices.

The guidance proved timely as it instantly became among the OIPC's most viewed website resources.

[5] Office of the Information and Privacy Commissioner for British Columbia, "Collecting personal information at food and drink establishments, gatherings, and events during COVID-19", July 2020.

[6] OIPC, "Pandemic FAQ: Customer Lists", June 2020.

VIRTUAL HEALTHCARE

In August 2019, the Canadian Medical Association (CMA) issued a discussion paper on virtual care in Canada, with the following opening paragraph:[7]

> While technologies to deliver health care through means other than face-to-face contact, such as tele-medicine/ telehealth, have been around for decades, they have yet to be adopted into routine use by health care systems around the industrialized world.

Fast forward to a May 2020 survey commissioned by CMA, 47% of Canadians said they used some electronic method to receive care during the pandemic.[8] The survey concluded, "Very few (Canadians) see downsides in making this a more common option."[9]

From "yet to be adopted' to nearly half the population – in nine months.

The OIPC witnessed this tremendous acceleration of virtual care. Within a month, custodians submitted 250 privacy impact assessments on virtual care projects to respond to the pandemic.

Some of the proposed projects brought unique considerations under Alberta's HIA, particularly in light of the relationship between private sector virtual care system developers and providers and custodians' HIA accountabilities for protecting Albertans' health information. One notable example was the Babylon by Telus Health app, which the OIPC opened investigations into in April 2020 under HIA and PIPA after compliance concerns were identified during the OIPC's review of PIAs that were submitted on the app.

Privacy and security issues requiring review for the provision of virtual health services can include location tracking, digital verification and authentication, biometrics, system interoperability, complex third-party service provider agreements, and storage of health information outside of Canada. Prior to the pandemic, these topics were mostly limited to multi-stakeholder projects in the health sector, such as large-scale, multi-year provincial information system projects. Due to the pandemic, healthcare professionals instantly started dealing with these complex digital privacy and security issues.

The OIPC balanced the review of virtual care PIAs with the operational challenges faced by healthcare professionals by adapting its practice for receiving PIAs on projects meant to help custodians navigate the pandemic.[10] The OIPC said in March 2020:

> During these unprecedented times, if a health custodian is considering new administrative practices or information systems with implications for individuals' privacy to combat the pandemic, the OIPC is asking that health custodians, at the very least, notify the Commissioner about the new administrative practice or information system. Notification of a new administrative practice or information system can be submitted to the OIPC via email.
>
> When notifying the Commissioner, please describe what the new program is meant to achieve and any safeguards for health information.
>
> Health custodians need to determine what are reasonable safeguards in the circumstances and be prepared to justify their decision. Health custodians should also ensure individuals are aware of any heightened risks to privacy as a result of a new administrative practice or information system being implemented.

[7] Canadian Medical Association, "Virtual Care in Canada: Discussion Paper", August 2019.

[8] Zafar, Amina, "Many Canadians used virtual medical care during COVID-19, poll suggests", CBC, June 8, 2020.

[9] Abacus Data and Canadian Medical Association, "What Canadians Thinks About Virtual Health Care: Nationwide Survey Results", May 2020.

[10] OIPC, "Notice: PIAs During a Public Health Emergency", August 2019.

> The OIPC recognizes the pressures all organizations, especially health custodians, are facing. The OIPC also knows first-hand through breaches reported to the Commissioner that security and privacy risks significantly increase when processes are interrupted, new processes are established or new tools are implemented during an emergency without proper planning or security and privacy controls.
>
> Public health is the number one priority, but ensuring security and privacy risks are considered and mitigated to the greatest extent possible will help reduce other incidents from emerging during these challenging months ahead.

The OIPC worked with the College of Physicians and Surgeons, Alberta Medical Association, among others, to ensure custodians understood what the OIPC expected through this adapted process. The adapted PIA process remained in effect as of March 31, 2021.

ACCESS TO INFORMATION

Early in the pandemic, many governments, including the Government of Alberta, through ministerial order or otherwise, increased time limits for responding to access to information requests. This was in part a response to the uncertainties around accessing records as employees transitioned from the office to working from home.

As public health orders or emergency declarations were lifted, however, time limits went back to normal. Consequently, the OIPC saw a decrease in time extension requests for the first several months of 2020-21, before seeing numbers increase in the second half of the year.

There was also a visible trend through media reports and on social media that people were making access to information requests to government departments and other public bodies about the pandemic response.

Recognizing the COVID-19 pandemic is a pivotal moment in history, international information commissioners came together in April 2020 to issue a statement about access to information in the context of a global pandemic.[11] The statement read in part (see full statement in the Education and Outreach section of this report):

> As a global community, we recognise that resources may be diverted away from usual information rights work. Public organisations will rightly focus their resources on protecting public health, and we recognise our role in taking a pragmatic approach, for example around how quickly public bodies respond to requests.
>
> But the importance of the right to access information remains.
>
> Public bodies must also recognise the value of clear and transparent communication, and of good record-keeping, in what will be a much analysed period of history.

Additionally, the OIPC was finalizing its report on public bodies' use of section 32, the FOIP Act's public interest override. In July 2020, the investigation report was issued with the backdrop of the COVID-19 pandemic response (see Regulation and Enforcement section of this report).

The investigation found that Alberta public bodies understand and take seriously the requirement to disclose "information about a risk of significant harm to the environment or to the health or safety of the public" (section 32(1)(a)), but rarely turn their minds to disclosing information proactively when it is "clearly in the public interest" (section 32(1)(b)).

[11] OIPC, "Access to Information in the Context of a Global Pandemic", April 14, 2020.

In making this finding, the Commissioner made the following comments in the news release:[12]

> The COVID-19 pandemic has raised a myriad of privacy issues, but access to information rights cannot be forgotten during what will be a much analyzed period of history. This report is timely for government institutions at all levels to consider what information must be made public as they respond to public health, economic and social concerns.
>
> Some public bodies may want clarity from my office on what information is 'clearly in the public interest', but ultimately it is public bodies that are in the best position to know what information they hold to make those decisions. I want to remind Alberta public bodies that the 'public interest override' places a duty upon them to disclose information.

Section 32(3) requires a public body releasing information proactively in the public interest to notify the Commissioner about such disclosure. As of March 31, 2021, there were no notifications made to the Commissioner by a public body citing section 32(1)(b) for releasing records about the COVID-19 pandemic response.

The OIPC began to see a number of time extension requests and requests for review in 2020-21 where the records at issue concern public bodies' pandemic response, and related information.

[12] OIPC, "'Public Interest Override' in Alberta's Freedom of Information Law Reviewed in Commissioner's Report", July 29, 2020.

COMMISSIONER WRITES TO MINISTER OF SERVICE ALBERTA

In the 2019-20 Annual Report, the Commissioner committed to writing to the Minister of Service Alberta to ask for updates to the FOIP Act and PIPA. The letter was sent in November 2020 and is available at www.oipc.ab.ca.

The recommendations were selected by the Commissioner with a view to adapting the legislation to reflect accelerated digitization in all sectors in light of the COVID-19 pandemic and enhanced societal expectations relating to access to information and privacy rights.

FOIP Recommendations

With respect to the FOIP Act, the recommended amendments are meant to further digitize the freedom of information system, improve information sharing for effective and efficient service delivery, modernize privacy protections and accountability mechanisms, strengthen oversight, reduce court burdens, improve the time extensions process, and ensure regular legislation reviews.

The FOIP Act recommendations include:

- Adopting the Ontario approach for information sharing. Ontario recently enacted amendments to its *Freedom of Information and Protection of Privacy Act* (Part III.1: Data Integration) which allow for the creation of data integration units within and outside of public bodies. The Ontario approach facilitates data pooling across government, and builds numerous protections including data minimization, de-identification requirements, approval of data standards by the Commissioner, written agreements, PIA requirements, mandatory breach reporting, and regular reviews of policies and processes by the Commissioner.
- Requiring public bodies to complete and submit to the Commissioner PIAs for certain information sharing initiatives (described in the Ontario approach), where the public body is developing an information system or an electronic service delivery project, or where the public body plans to disclose personal information without consent or to disclose personal information outside of province.
- Mandating notification of a privacy breach to an individual and to the Commissioner where there is a real risk of significant harm to the individual as a result of the loss or unauthorized access or disclosure of personal information, with the associated powers for the Commissioner that exist in PIPA.
- Requiring that, upon request, information supplied in response to an access request be released electronically to an applicant using a structured, commonly used technological format.
- Allowing the head of a public body to extend the time for responding to an access request for up to 30 days, or, with the Commissioner's permission, for a longer period in unforeseen emergency or disaster situations.

  In addition, a number of technical amendments to section 14 are recommended in *Making the FOIP Act Clear, User-friendly & Practical,* a submission to the 2013 government review of the FOIP Act.

- Stating explicitly that:
  - The Commissioner has the power to require public bodies to produce to the Commissioner records over which solicitor-client privilege and other similar privileges (for example, litigation privilege or informer privilege) are claimed
  - The Commissioner may require those records when, in the Commissioner's opinion, it is necessary to perform the Commissioner's functions (such as when a public body does not provide enough evidence to satisfy the Commissioner that the records are privileged)
  - Solicitor-client privilege or other legal privilege is not waived when the privileged records are provided to the Commissioner
  - The Commissioner may not disclose to the Minister of Justice and Solicitor General, as evidence of an offence, records to which solicitor-client privilege applies
- Stating in section 92(5) that a prosecution of an offence under the Act be commenced within two years after the day on which evidence of the alleged offence first came to the attention of the Commissioner, but not afterwards.
- Requiring in section 97 that a special committee of the Legislative Assembly must begin a comprehensive review of the FOIP Act and the regulations made under it with certain parameters.

PIPA Recommendations

With respect to PIPA, the recommended amendments are meant to enhance accountability measures for the protection of personal information, better enable the use of de-identified personal information for innovation and research, give consumers more choice by enhancing business competition, strengthen oversight, and build public trust in personal information practices by expanding the scope of the law.

The PIPA recommendations include:

- Requiring organizations to have a privacy management program in place and that organizations provide written information about their privacy management program to the Commissioner and to individuals, upon request. The requirements of a privacy management program should be adaptable and scalable to the size of the organization and to the volume and sensitivity of the personal information that is in its custody or under its control. Other aspects that could make up part of the requirement to establish a privacy management program include mandatory PIAs for projects meeting certain criteria and requiring certain criteria for the use of automated decision-making.
- Exploring data trusts as a potential enabler of responsible innovation.

  At minimum, permitting the use of de-identified personal information without consent for internal research and development purposes; defining "de-identified" to mean removing any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual; and making it an offence for attempting to re-identify individuals using de-identified information
- Making PIPA apply fully to all non-profit organizations and political parties.
- Including the right to data portability. In addition, the government should conduct further consultations on the right to erasure and the right to de-indexing.
- Strengthening oversight and offence and penalty provisions by, for example, granting the Commissioner the power to impose administrative monetary penalties for certain violations and increasing offence fines.

The recommendations to PIPA were provided in light of the significant changes to private sector privacy law since 2016, when the last PIPA review was undertaken, including:

- Quebec introducing Bill 64 in June 2020, which proposes sweeping amendments to both public and private sector laws, and underwent extensive public consultation.
- The federal government introducing Bill C-11 in November 2020, which proposes an overhaul to the *Personal Information Protection and Electronic Documents Act*.
- Ontario launching a public consultation in August 2020 with the aim to introduce its own private sector privacy law.
- British Columbia reviewing PIPA through a special parliamentary committee.

The national discussions and proposed changes federally and provincially notably reflect many principles in the European Union's *General Data Protection Regulation*, which came into force in 2018.

Call for Consultation on Legislation Reform

The Commissioner's November 2020 letter to the Minister of Service Alberta noted that the recommendations provided were not exhaustive, and the Commissioner said both Acts deserve comprehensive reviews by a special committee of the Legislative Assembly.

Over the past several years, public scrutiny of access and privacy laws has increased, and the COVID-19 pandemic intensified the spotlight on access and privacy rights. The Commissioner noted that these realities reinforce the need for a guided public consultation on how to improve the FOIP Act and PIPA, and that public reviews by a special committee of the Legislative Assembly would allow all stakeholders to engage in meaningful and helpful discussions on improving the laws.

BILL 46, HIA AMENDMENTS

Before the Commissioner had the opportunity to send a letter to the Minister of Health outlining recommendations to HIA as noted in the 2019-20 Annual Report, the Minister of Health tabled Bill 46, the Health Statutes Amendment Act (No. 2), in November 2020. Bill 46 proposed amendments to several pieces of legislation, including significant changes to HIA.

The Commissioner expressed disappointment in not being consulted on the amendments prior to Bill 46 being tabled, and committed to making comments on the amendments available publicly while the bill was being debated in the legislature.

Eight days after the bill was tabled in the legislature, the Commissioner described the potential problems posed by certain amendments and outlined amendments supported by the OIPC. A news release and letter are available at www.oipc.ab.ca.

The Commissioner listed the proposed amendments of particular concern in the news release, including:

- Expanding Netcare access to "authorized users" outside Alberta, without compensating controls to address risks to Albertans' privacy. Broadening access to Netcare beyond Alberta's borders may also pose potential jurisdictional challenges to effective oversight and may limit the recourse available to Albertans.
- Expanding the use of health information made available via Netcare. Privacy risks are escalated by proposing to increase the number of users of Netcare and significantly expanding purposes for how health information available via Netcare may be accessed and used. These proposals must include updated and enhanced controls that reasonably mitigate the risks. Transparency is critical in this regard.

- Eliminating the PIA requirement for the collection, use and disclosure of health information shared between Alberta Health, Alberta Health Services and the Health Quality Council of Alberta for certain purposes, unless implementing a new information system or making changes to an existing information system. This amendment will significantly reduce transparency and accountability for certain information sharing initiatives.

Despite the concerns raised, the Commissioner supported some amendments, including a change to the limitation period for offences, removing the "imminence test" for disclosing health information to prevent significant harm, and increasing accountability for researchers to comply with research agreements they have signed with a health custodian. The Commissioner also appended a list of 10 suggested HIA improvements to the letter.

Upon issuing the letter, the Commissioner said, "I am hopeful that the government will either make amendments to the bill or ideally pause deliberations to allow for further consultation on the implications these proposed amendments have for the protection of Albertans' health information."

No amendments were made to the bill prior to passing third reading in December 2020. Many of the amendments require associated updates to regulations before coming into force and the Minister of Health committed to consulting the Commissioner on regulations.

> "While many jurisdictions around the world are introducing new or enhanced privacy laws to build public trust and ensure accountability mechanisms are in place to protect personal or health information, many of the proposed amendments to HIA are heading in the other direction. Alberta has been considered a leader in health information privacy law and we should aspire to remain that way in the years to come."
>
> *- Commissioner Jill Clayton, November 13, 2020*

BY THE NUMBERS

Totals Opened/Closed
(excluding Intake and AMVIR cases)

14% | 18%

INCREASE IN OPENED/CLOSED TOTAL CASES

4,166 total opened files in 2020-21; 3,658 in 2019-20

3,517 total closed files in 2020-21; 2,968 in 2019-20

Totals Opened/Closed under HIA
(excluding Intake cases)

16% | 22%

INCREASE IN OPENED/CLOSED HIA FILES

2,921 opened HIA files in 2020-21; 2,510 in 2019-20

2,264 closed HIA files in 2020-21; 1,851 in 2019-20

Privacy Impact Assessments (PIAs)

31% | 42%

INCREASE IN OPENED/CLOSED PIAs

1,908 opened PIAs in 2020-21; 1,454 in 2019-20

1,522 closed PIAs in 2020-21; 1,071 in 2019-20

Totals Opened/Closed under PIPA
(excluding Intake cases)

16% | 16%

INCREASE IN OPENED/CLOSED PIPA FILES

478 opened PIPA files in 2020-21; 413 in 2019-20

457 closed PIPA files in 2020-21; 394 in 2019-20

Totals Opened/Closed under FOIP
(excluding Intake cases)

4% | 10%

INCREASE IN OPENED/CLOSED FOIP FILES

767 opened FOIP files in 2020-21; 735 in 2019-20

796 closed FOIP files in 2020-21; 723 in 2019-20

Self-Reported Breaches (SRBs)

3% | 8%

INCREASE IN OPENED/CLOSED SRBs

1,388 opened SRBs in 2020-21; 1,344 in 2019-20

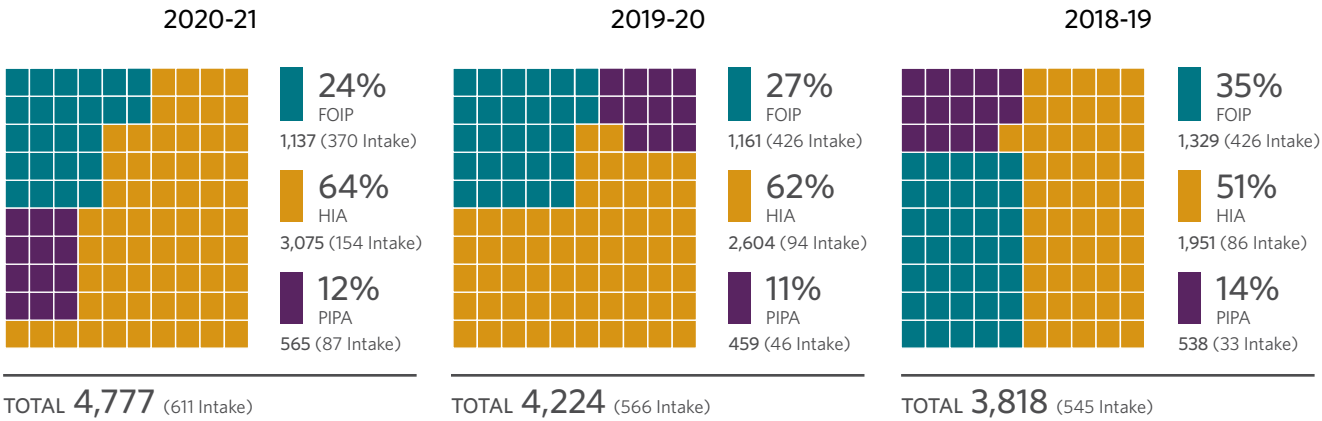
1,115 closed SRBs in 2020-21; 1,030 in 2019-20

294

TIME EXTENSION REQUESTS UNDER FOIP

GRAPH A: TOTAL CASES OPENED

Three Year Comparison



GRAPH B: TOTAL CASES CLOSED

Three Year Comparison

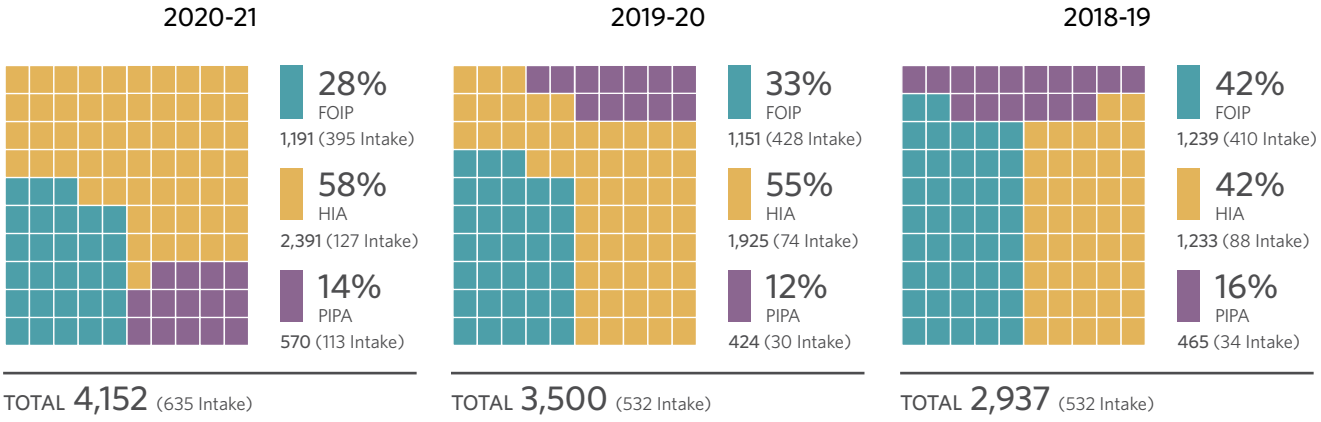


TABLE 1: CASES OPENED BY CASE TYPE

FOIP	2020-2021	2019-2020	2018-2019
Advice and Direction	0	1	1
Authorization to Disregard a Request	4	7	9
Complaint	28	45	91
Disclosure to Commissioner (Whistleblower)	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fee	2	7	16
Investigation Generated by Commissioner	4	9	8
Notification to OIPC	7	29	7
Offence Investigation	1	0	3
Privacy Impact Assessment	14	23	23
Request Authorization to Collect Indirectly	0	0	0
Request for Information	9	14	23
Request for Review	283	251	358
Request for Review 3rd Party	40	23	32
Request Time Extension	294	231	226
Self-reported Breach	81	95	106
Subtotal	**767**	**735**	**903**
Intake cases	370	426	426
Total	**1,137**	**1,161**	**1,329**

HIA	2020-2021	2019-2020	2018-2019
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	0	3
Complaint	33	64	43
Engage in or Commission a Study	0	0	0
Excuse Fee	1	0	1
Investigation Generated by Commissioner	19	7	11
Notification to OIPC	0	0	0
Offence Investigation	11	18	11
Privacy Impact Assessment	1,888	1,428	1,059
Request for Information	19	38	39
Request for Review	19	17	24
Request Time Extension	1	0	0
Self-reported Breach	930	938	674
Subtotal	**2,921**	**2,510**	**1,865**
Intake cases	154	94	86
Total	**3,075**	**2,604**	**1,951**

PIPA	2020-2021	2019-2020	2018-2019
Advice and Direction	0	0	1
Authorization to Disregard a Request	1	1	3
Complaint	46	52	112
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	0
Investigation Generated by Commissioner	7	8	7
Notification to OIPC	0	0	0
Offence Investigation	0	0	0
Privacy Impact Assessment	6	3	8
Request for Advanced Ruling	0	1	1
Request for Information	4	11	31
Request for Review	37	25	51
Request Time Extension	0	1	1
Self-reported Breach	377	311	290
Subtotal	**478**	**413**	**505**
Intake cases	87	46	33
Total	**565**	**459**	**538**

Notes

(1) See Appendix A for a complete listing of cases opened in 2020-21.

(2) Only FOIP allows a third party to request a review of a decision to release third party information to an applicant.

(3) Intake cases include determining whether parties coming to the OIPC are properly exercising the rights set out in FOIP, HIA and PIPA; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints.

(4) There were three *Access to Motor Vehicle Information Regulation* (AMVIR) registrar decision notifications opened in 2020-21. The Commissioner may review a decision of the Registrar of Motor Vehicle Services to grant or deny access to personal driving and motor vehicle information under AMVIR.

TABLE 2: CASES CLOSED BY CASE TYPE

FOIP	2020-2021	2019-2020	2018-2019
Advice and Direction	0	1	0
Authorization to Disregard a Request	1	3	6
Complaint	53	61	82
Disclosure to Commissioner (Whistleblower)	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fee	11	8	14
Investigation Generated by Commissioner	6	2	31
Notification to OIPC	7	29	7
Offence Investigation	3	2	0
Privacy Impact Assessment	27	15	12
Request Authorization to Collect Indirectly	0	0	0
Request for Information	14	10	24
Request for Review	241	239	316
Request for Review 3rd Party	28	47	23
Request Time Extension	303	222	231
Self-reported Breach	102	84	83
Subtotal	**796**	**723**	**829**
Intake cases	395	428	410
Total	**1,191**	**1,151**	**1,239**

HIA	2020-2021	2019-2020	2018-2019
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	1	0
Complaint	42	31	81
Engage in or Commission a Study	0	0	0
Excuse Fee	0	1	0
Investigation Generated by Commissioner	2	5	5
Notification to OIPC	0	0	0
Offence Investigation	12	9	6
Privacy Impact Assessment	1,491	1,050	669
Request for Information	24	44	30
Request for Review	17	15	18
Request Time Extension	1	0	0
Self-reported Breach	675	695	336
Subtotal	**2,264**	**1,851**	**1,145**
Intake cases	127	74	88
Total	**2,391**	**1,925**	**1,233**

PIPA	2020-2021	2019-2020	2018-2019
Advice and Direction	0	1	0
Authorization to Disregard a Request	1	0	5
Complaint	66	83	108
Engage in or Commission a Study	0	0	0
Excuse Fee	0	0	0
Investigation Generated by Commissioner	7	2	2
Notification to OIPC	0	0	0
Offence Investigation	0	0	0
Privacy Impact Assessment	4	6	0
Request for Advanced Ruling	1	1	0
Request for Information	4	14	30
Request for Review	36	35	66
Request Time Extension	0	1	1
Self-reported Breach	338	251	219
Subtotal	**457**	**394**	**431**
Intake cases	113	30	34
Total	**570**	**424**	**465**

Notes

(1) See Appendix B for a complete listing of cases opened in 2020-21.

(2) A listing of all privacy impact assessments accepted in 2020-21 is available at www.oipc.ab.ca.

(3) Only FOIP allows a third party to request a review of a decision to release third party information to an applicant.

(4) Intake cases include determining whether parties coming to the OIPC are properly exercising the rights set out in FOIP, HIA and PIPA; whether the matters or issues identified by the parties are within the Commissioner's legislative jurisdiction; and investigating and trying to resolve certain requests or complaints.

(5) There were three *Access to Motor Vehicle Information Regulation* (AMVIR) registrar decision notifications closed in 2020-21. The Commissioner may review a decision of the Registrar of Motor Vehicle Services to grant or deny access to personal driving and motor vehicle information under AMVIR.

TABLE 3: CASES CLOSED BY RESOLUTION METHOD

Under FOIP, HIA and PIPA, only certain case types can proceed to Inquiry if the matters are not resolved at Mediation/Investigation. The statistics below are for those case types that can proceed to Inquiry (Request for Review, Request for Review 3rd Party, Request to Excuse Fees and Complaint files).

RESOLUTION METHOD	NUMBER OF CASES (FOIP)	NUMBER OF CASES (HIA)	NUMBER OF CASES (PIPA)	TOTAL	%
Mediation/Investigation	262	52	83	397	80%
Order or Decision	44	4	10	58	12%
Commissioner's decision to refuse to conduct an Inquiry	7	0	3	10	2%
Withdrawn during Inquiry process	3	3	0	6	1%
Discontinued during Inquiry process	17	0	6	23	5%
Total	**333**	**59**	**102**	**494**	**100%**

FOIP Orders: 41 (41 cases); FOIP Decision: 1 (1 case); HIA Orders: 3 (4 cases); PIPA Orders: 9 (10 cases)

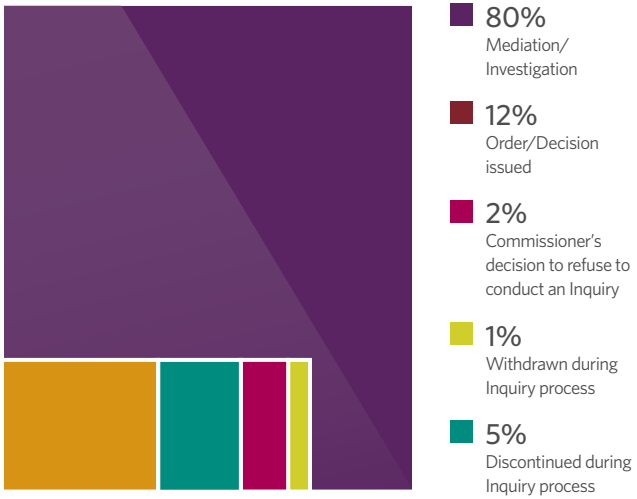
Notes

(1) This table includes only the Orders and Decisions issued that concluded/closed the file. See Appendix C for a list of all Orders, Decisions and public Investigation Reports issued in 2020-21. Copies of Orders, Decisions and Public Investigation Reports are available at www.oipc.ab.ca.

(2) Orders and Decisions are recorded by the date the Order or Decision was signed, rather than the date the Order or Decision was publicly released.

(3) An inquiry can be discontinued due to a lack of contact with or participation of the applicant or complainant or the issues have become moot.

GRAPH C:
PERCENTAGE OF CASES CLOSED BY RESOLUTION METHOD



Of the **494** cases that could proceed to Inquiry:
1% were resolved within 90 days
4% were resolved within 180 days
95% were resolved in more than 180 days

TABLE 4: GENERAL ENQUIRIES

TELEPHONE CALLS		
FOIP	Number	Percentage
Public Bodies	31	11%
Individuals	250	89%
Total	**281**	**100%**

HIA	Number	Percentage
Custodians	445	55%
Individuals	360	45%
Total	**805**	**100%**

PIPA	Number	Percentage
Organizations	56	8%
Individuals	652	92%
Total	**708**	**100%**

NON-JURISDICTIONAL	151
EMAILS FOIP/HIA/PIPA	420
Total	**2,365**

REGULATION & ENFORCEMENT

Investigation Reports

CLEARVIEW AI

A joint investigation by the OIPC, Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec and the Office of the Information and Privacy Commissioner for British Columbia concluded that Clearview AI violated federal and provincial privacy laws.

The investigation found that Clearview had collected highly sensitive biometric information without the knowledge or consent of individuals. Furthermore, Clearview collected, used and disclosed Canadians' personal information for inappropriate purposes, which could not be rendered appropriate via consent.

> "As the use of facial recognition technology expands, significant issues around accuracy, automated decision making, proportionality and ethics persist. The Clearview investigation shows that across Canada we need to be discussing acceptable uses and regulation of facial recognition. Regulation would not only assist in upholding privacy rights, it would provide much needed certainty to all organizations thinking about using or developing the technology."
>
> *- Commissioner Jill Clayton, February 3, 2021*

Clearview AI's technology allowed law enforcement and commercial organizations to match photographs of unknown people against the company's databank of more than three billion images for investigation purposes. Commissioners found that this creates a risk of significant harm to individuals, the vast majority of whom have never been and will never be implicated in a crime.

The privacy authorities recommended that Clearview stop offering its facial recognition services to Canadian clients, stop collecting images of individuals in Canada, and delete all previously collected images and biometric facial arrays of individuals in Canada.

Shortly after the investigation began, Clearview agreed to stop providing its services in the Canadian market. It stopped offering trial accounts to Canadian organizations and discontinued the RCMP's subscriber service in July 2020.

Clearview AI, however, disagreed with the findings of the investigation and did not commit to all recommendations. The refusal to commit to recommendations highlighted Canadian Privacy Commissioners' repeated calls for strengthened oversight and enforcement mechanisms.

Investigation Report P2021-IR-01: 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

USE OF SECTION 32 BY ALBERTA PUBLIC BODIES

The OIPC released an investigation report on July 29, 2020 that looked into the use of the "public interest override" provision (section 32) by public bodies under the FOIP Act. Section 32 requires a public body to disclose information if it is in the public interest.

The investigation found that Alberta public bodies take seriously and understand using section 32 as the authority to disclose "information about a risk of significant harm to the environment or to the health or safety of the public, of the affected group of people, of the person or of the applicant" (section 32(1)(a) of the FOIP Act). The report, in particular, highlighted the work of Portage College and Alberta police services in developing public interest disclosure policies and procedures.

In terms of section 32(1)(b), however, the investigation found that Alberta's public bodies rarely turn their minds to disclosing information proactively when it is "clearly in the public interest". Public bodies cited several reasons for this, namely that it is difficult to discern between what information is "of interest to the public" and what information is "clearly in the public interest".

The investigation recommended that public bodies more often consider section 32(1)(b) as the authority to proactively disclose information, and to document decisions where section 32(1)(b) has been considered whether or not a disclosure is made.

The report analyzed decisions related to the public interest override in Alberta, survey results of Alberta public bodies regarding section 32, and reviewed public interest disclosures in Canadian jurisdictions.

Investigation Report F2020-IR-01: Investigation into Public Bodies' Compliance with Section 32, the Public Interest Override Provision

> "The COVID-19 pandemic has raised a myriad of privacy issues, but access to information rights cannot be forgotten during what will be a much analyzed period of history. This report is timely for government institutions at all levels to consider what information must be made public as they respond to public health, economic and social concerns."
>
> *- Commissioner Jill Clayton, July 29, 2020*

CADILLAC FAIRVIEW COLLECTED IMAGES WITHOUT CONSENT

The OIPC joined the Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner for British Columbia in investigating Cadillac Fairview's use of facial recognition technology at certain malls it operates across Canada.

The investigation found that Cadillac Fairview embedded cameras inside its digital information kiosks at 12 shopping malls and used facial recognition technology without its customers' knowledge or consent. Cadillac Fairview said decals it had placed on shopping mall entry doors that referred to their privacy policy made customers aware of the activity, which the investigation determined to be insufficient.

The investigation also found:

- Cadillac Fairview did collect personal information, and contravened privacy laws by failing to obtain meaningful consent as they collected the 5 million images with small, inconspicuous cameras. Cadillac Fairview also used video analytics to collect and analyze sensitive biometric information of customers. Cadillac Fairview had argued that it did not collect personal information, since the images taken by the camera were briefly analyzed then deleted.
- Facial recognition software was used to generate additional personal information about individual shoppers, including estimated age and gender.
- While the images were deleted, investigators found that the sensitive biometric information generated from the images was stored in a centralized database by a third party. Cadillac Fairview stated that it was unaware that the database of biometric information existed, which compounded the risk of potential use by unauthorized parties or, in the case of a data breach, by malicious actors.

In response to the investigation, Cadillac Fairview removed the cameras from its digital directory kiosks. It also deleted all information associated with the video analytics technology that is 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, which the investigation found it had retained for no discernable reason.

The investigation 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.

Investigation Report P2020-IR-01: Joint investigation of the Cadillac Fairview Corporation Ltd. by the Information and Privacy Commissioner of Alberta, the Privacy Commissioner of Canada, and the Information and Privacy Commissioner for British Columbia

> "This investigation exposes how opaque certain personal information business practices have become. Not only must organizations be clear and up front when customers' personal information is being collected, they must also have proper controls in place to know what their service providers are doing behind the scenes with that information."
>
> *- Commissioner Jill Clayton, October 29, 2020*

Mediation and Investigation

The mediation and investigation (MI) team, consisting of a director and six Senior Information and Privacy Managers (SIPMs), reviews access request responses (requests for review) and responds to privacy complaints from Albertans under all three laws.

In 2020-21, 80% of files that could proceed to Inquiry were resolved at mediation and investigation. In total, 397 files were resolved by mediation and investigation.

MEDIATION AND INVESTIGATION PROCESS AND TIMELINES

When a request for review or complaint is received, the Commissioner can authorize an individual to investigate and try to settle the issue under the Acts.

In order to try to resolve a matter under the laws, the MI process involves gathering information from the parties and providing findings about how the law applies to their situation. The MI team also educates parties about the laws and OIPC's processes, and by managing expectations about possible outcomes.

For requests to review responses to access to information requests (or FOIP requests), the assigned SIPM gathers the records and submissions from the public body, custodian or organization and reviews whether information was properly severed or withheld under the laws, and to ensure other legal processes were properly followed. For privacy complaints, the assigned SIPM gathers submissions from the public body, custodian or organization and compares the submissions against the situation described by the complainant. At the conclusion, the SIPM issues findings and recommendations. If the parties agree with the findings and recommendations, the case is closed. If one of the parties disagrees with the findings and recommendations, it may proceed to inquiry (a formal decision making process).

Parties involved in the MI process are sometimes frustrated by the time it takes to try to settle a matter. The frustration is understandable. It is taking approximately 18 months – sometimes more, sometimes less – to resolve a file after it is opened. If a matter proceeds to inquiry, it takes at least 18 months more to settle the matter.

Many factors contribute to delays. When a privacy complaint is submitted, the public body, custodian or private sector organization is often unaware that an individual has concerns until they are contacted about the complaint. This means the OIPC starts at square one in ensuring there is a mutual understanding of the situation between the parties. Additionally, the employees tasked with responding to access requests within legislated timelines are also typically responsible for managing responses for a request for review. Similar realities exist for privacy officers in larger organizations, custodians operating their own practices, and small business owners who take on many responsibilities. As a result, applicants and complainants must endure long wait times to get information or answers to their questions or concerns about records or privacy practices.

Also contributing to delays is caseload realities. The OIPC has a caseload cap for SIPMs in order to effectively balance workload and devote the attention necessary to settle each file. This means that files are inactive until which time that space opens within caseload caps.

CASE TRENDS

Pandemic-Related Issues

The OIPC began to see complaints and reviews related to how public bodies, custodians and organizations responded to the pandemic. For example, complaints were submitted about the use of personal information for contact tracing, contrary to the reason for which the information was collected. There were also requests to review responses from government departments about personal protective equipment procurement and school re-entry plans, among other topics.

Increase in HIA Complaints Linked to Mandatory Breach Reporting

On August 31, 2018, it became mandatory under HIA for custodians to notify individuals if there was a risk of harm because of a privacy breach. Under section 8.2(4)(i) of the *Health Information Regulation*, when a custodian sends a notice to an individual that there has been a loss or unauthorized access to or disclosure of health information, the notice must include a statement that an individual may ask the Commissioner to investigate the incident.

The OIPC has noticed an increase in complaints resulting from privacy breach notices sent to individuals. These investigations focus on a custodian's duty to protect health information under section 60 of HIA. An important role the MI process plays in reviewing these complaints is educational. Individuals often seek compensation or employment sanctions, which are remedies that do not exist under HIA. Nevertheless, the investigations are valuable for assessing the safeguards and providing an opportunity to discuss, if applicable, improvements to safeguarding health information, especially for smaller health custodians operating their own practices.

Surveillance

Requests for surveillance records and concerns about privacy in relation to the use of surveillance or CCTV is a continuing trend. The OIPC once again saw requests for surveillance in correctional facilities. The OIPC also saw an uptick in reviews involving public bodies or organizations that have security surveillance and where applicants are trying to access footage for private litigation purposes, such as insurance or personal injury claims.

Access Requests for Information of Deceased Persons

Family members of deceased individuals often request information wanting to know the circumstances surrounding their loved one's death. These files present a challenge as often the deceased persons are adults and the information concerning the death is sensitive.

While the laws allow others to "step into the shoes" of deceased persons to exercise any right or power conferred on an individual under the laws, the ability to do so is limited. For example, under section 84(1)(a) of the FOIP Act, if the individual is deceased, the rights and powers under the Act can only be exercised by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate.

It is difficult to explain to family members who want access to a deceased person's records, but do not function as their personal representatives or want the records for estate administration purposes, that they do not meet the legal criteria for a right of access to the records. This is an example of the human side of access to information.

Credit Checks in the Private Sector

The OIPC received a number of complaints against organizations regarding the collection, use and disclosure of personal information in performing credit checks. In many cases, the individuals have consented to the collection and use of their personal information in the application of credit. Many sectors are represented in these complaints, including jewellery retail and credit application services. The intersection of PIPA and the *Consumer Protection Act* is considered in such cases.

Jurisdictional Questions for Non-Profit Organizations

PIPA applies to certain non-profits in limited circumstances in Alberta, most notably when the personal information at issue is connected to a commercial activity. Of particular relevance are complaints against sports associations and organizations offering (free) mediation services, such as the Better Business Bureau. Other complaints that raise interesting jurisdictional questions are requests for employment records when the non-profit organization is not engaged in a commercial activity.

Unlike British Columbia where its PIPA includes all non-profits, the requirement to determine if the personal information is connected to a "commercial activity" in order to fall under Alberta's PIPA is often challenging and difficult to distinguish. The OIPC continues to recommend that PIPA apply to all non-profit organizations.

High Volume Applicants

There continue to be individuals who submit multiple requests for review or complaints in short periods. For example, an individual submitted approximately 80 requests for review or complaints in one year. There are other examples where five or more requests for reviews are submitted at the same time, often to or about the same public body, custodian or organization.

These situations balance the right to request a review and fairness in resource allocation. When several individuals submit multiple reviews or complaints, it strains the OIPC's resources and the ability to try to settle matters in a timely manner, and in effect limits the rights of other individuals in having their matters reviewed in a timely manner.

The Commissioner is able manage the OIPC's processes and put strategies in place to address fair distribution of resources. For example, individuals are limited in how many of their files the OIPC will actively work on at one time. This helps to ensure that other applicants and complainants have a fair opportunity to have their matter reviewed by the OIPC, while not limiting any individual's right to request a review.

Requests for Time Extensions by Public Bodies

A public body must make every reasonable effort to respond to an access request under the FOIP Act within 30 calendar days (section 11). A public body may extend the time limit for responding by up to 30 days on its own authority in certain circumstances (section 14(1)).

An extension period longer than an additional 30 days requires the Commissioner's approval (section 14(2)). A failure by a public body to respond to a request within the 30-day time limit, or a time limit extended under section 14, is treated as a decision to refuse access (section 11(2)).

In 2020-21, there were 294 requests for time extensions submitted by public bodies to the OIPC, representing a 27% increase from 2019-20 (231). Of the 294 time-extension requests received:

- 75% were made by provincial government departments
- 7% were made by boards and commissions
- 6% were made by municipalities
- 4% were made by post-secondary institutions
- 4% were made by the regional health authority (Alberta Health Services)
- 2% were made by law enforcement
- 2% were made by other public bodies

The following decisions were made on time extension requests:

- 74% were granted
- 12% were partially granted (i.e. extension period permitted was less than what the public body requested)
- 5% were denied
- 5% were not within the Commissioner's jurisdiction to decide
- 4% were withdrawn by the public body

Deemed Refusals on the Decline

In 2015-16, the OIPC began streamlining requests for review to the inquiry process when an applicant has not received a response to an access request that they have submitted to a public body, health custodian or organization within the time limits set out in the FOIP Act, HIA and PIPA, respectively. The Commissioner established this process after seeing an increase in requests for review where the only issue was that an applicant had not received a response to their access request within the time limits set out in the Acts.

The OIPC did not issue any deemed refusal orders in 2020-21 where the only issue was that the public body, custodian or organization was ordered to respond to the access request. This is welcome news. In 2016-17, for example, 48 deemed refusal orders were issued.

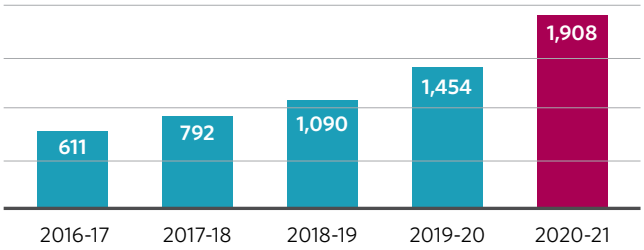
However, notably, section 11 was raised as an issue at mediation and investigation 35 times in 2020-21, an increase of 105% from 2019-20 (17). The issue of delays in responding to access to information requests continues to be observed.

Privacy Impact Assessment Reviews

There were 1,363 privacy impact assessments (PIA) accepted by the OIPC in 2020-21, representing a 32% increase from 2019-20 (1,031). Nearly all accepted PIAs, 98% or 1,341, were submitted by health custodians under HIA.

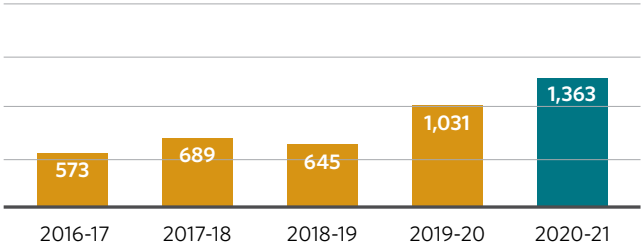
Only health custodians are required to submit PIAs to the OIPC in certain circumstances. Similar PIA requirements do not exist for public bodies and private sector organizations under the FOIP Act and PIPA.

PIAs OPENED ANNUALLY OVER FIVE YEARS*



*Not all opened files are accepted

PIAs ACCEPTED ANNUALLY OVER FIVE YEARS*



*Not all opened files are accepted

ALBERTA'S CONTACT-TRACING APP

With the global attention on contact-tracing apps during the COVID-19 pandemic, the OIPC prioritized review of Alberta Health's ABTraceTogether app and took the additional step of publishing a report on the PIA review.

The report highlighted ABTraceTogether's clear purpose to supplement already established contract-tracing processes, Alberta Health's consent-based approach, limited collection of health or personal information when registering to use the app, and Alberta Health's efforts to mitigate the risk of secondary use of information collected by the app.

However, there were ongoing concerns related to the functionality of the app on Apple devices at the time the report was released. The app needed to run in the foreground on Apple devices leading to an unmitigated security risk. For example, running the app on Apple devices required the device to remain unlocked, which significantly increased privacy risks in case of theft or loss.

The OIPC noted that the risk on Apple devices increases for employers in the public, health and private sectors that have obligations to reasonably safeguard health or personal information under Alberta's privacy laws.

For employers that provide employees with devices or allow employees to use their own devices for work purposes, and those devices store or otherwise make accessible health or personal information (for example, email or cloud service portals), the risk for running the app on Apple devices represented a potential contravention for failure to safeguard under Alberta's privacy laws.

The OIPC accepted the ABTraceTogether PIA with recommendations. Some recommendations related to clarifying inconsistencies found between documentation provided during the PIA review and what is made available publicly. The OIPC also recommended Alberta Health to continue to report publicly on the use and effectiveness of ABTraceTogether, and on its plans to dismantle the app when the time comes.

> "[Alberta Health] has done an excellent job being mindful of privacy and security in the deployment of ABTraceTogether. The app's clear purpose, guided by principles of consent and individual control, is commendable. I want to thank the team at [Alberta Health] responsible for the PIA for their cooperation during this review. Their consultative approach, responsiveness, and transparency throughout the process has been greatly appreciated, and we look forward to hearing how ABTraceTogether progresses as we all work together to address the COVID-19 pandemic."
>
> *- Commissioner Jill Clayton, July 2020*

Privacy Breaches

The OIPC received 1,388 reports of privacy breaches in 2020-21 under all three laws, representing a 3% increase from 2019-20 (1,344).

There are obligations under HIA and PIPA for health custodians and private sector organizations to report certain privacy breaches to the OIPC. Public bodies may report breaches voluntarily.

The OIPC also closed 1,115 self-reported breach files in 2020-21 under all three laws, representing an 8% increase from 2019-20 (1,030).

Certain breaches are prioritized for review, including files where affected individuals have not yet been notified or when a potential offence is suspected.

PIPA

There were 377 breaches reported in 2020-21, a 21% increase from 2019-20 (311).

The Commissioner issued 338 breach decisions in 2020-21, representing a 35% increase from 2019-20 (251). The following determinations were made in 2019-20:

- 255 were found to have a real risk of significant harm
- 50 were found to have no real risk of significant harm
- 33 where PIPA did not apply (that is, the Commissioner did not have jurisdiction to make a decision)

Of the 255 breaches where the Commissioner determined a real risk of significant harm to an individual, there were:

- Nearly 150 incidents caused by electronic systemic compromises, often through a combination of factors, such as hacking, phishing, malware or system vulnerabilities.
- Approximately 50 incidents involved human error, such as transmission errors by email, mail or fax, or during IT system upgrades or settings changes.
- Nearly 35 incidents of theft.
- More than 10 incidents caused by rogue employees.

Other causes of breaches include social engineering or loss (for example, couriered packages go missing).

It is mandatory for an organization with personal information under its control, to notify the Commissioner, without unreasonable delay, of a privacy breach where "a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure" (section 34.1). Section 37.1 of PIPA provides authority for the Commissioner to require an organization to notify individuals of a loss or unauthorized access or disclosure of personal information.

HIA

There were 930 breaches reported by custodians to the OIPC in 2020-21, representing a slight decrease from 2019-20 (938).

It is mandatory for a custodian having individually identifying health information in its custody or control to notify the Commissioner of a privacy breach if the custodian determines "there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure" (section 60.1(2)). In addition to notifying the Commissioner of the privacy breach, the custodian is also required by section 60.1(2) of HIA to notify the Minister of Health and the individuals affected by the privacy breach.

FOIP

There were 81 breaches reported voluntarily by public bodies in 2020-21, representing a 15% decrease from 2019-20 (95).

The FOIP Act is Alberta's only privacy law that does not require regulated entities to report privacy breaches to the Commissioner and notify affected individuals.

Offence Investigations under HIA

There were four convictions for unauthorized access to health information in 2020-21, including:

- An Edmonton-based pharmacist who received a $5,000 fine, plus a $1,000 victim fine surcharge, for using the health information of an individual with whom he was in a vehicle accident in an attempt to persuade the individual from submitting an insurance claim for the vehicle accident.
- Two Alberta Health Services employees in northern Alberta who were convicted in related snooping incidents. The proceedings were subject to a publication ban to protect victim identity.
- A former medical clinic employee who pleaded guilty to breaching the health information of several individuals. The former medical clinic employee was fined $6,000, given three years probation including not being able to access health information, and was ordered to complete 180 hours of community service.

The four convictions in 2020-21 brought the total number of convictions under HIA to 18.

As of March 31, 2021, two cases were before the courts.

Summary of Significant Decisions

Accuracy of Personal Information in Police Street Check Record

On May 27, 2013, while he was depositing money at the bank from the sale of a motor vehicle, an individual was arrested by a member of the Edmonton Police Service (EPS) who applied force in making the arrest. Prior to the arrest, a citizen had contacted 911 to report that he was observing the individual and two of his acquaintances attempting to steal a car. The citizen referred to the people he was observing as being Black. He added that he did not think that the people he was observing were the kind of people he expected to drive the car legally.

The police officer who arrested the applicant consulted EPROS (Edmonton Police Reporting and Occurrence System) prior to making the arrest and determined from the information he reviewed (and recorded in the arrest report) that the individual had a "violent history including weapons offences and drugs". After the police officer arrested the individual, the police officer learned that the individual and his acquaintances were legally authorized to occupy and drive the vehicle that was the subject of the 911 call. The money the police officer observed the individual deposit in the bank was the proceeds of the lawful sale of the vehicle, rather than drugs.

Litigation followed this incident. In the course of this process, the individual was given access to the police officer's report of the arrest and to street checks and other information about the individual located in EPROS that the officer reviewed prior to making the arrest.

One of the street checks that the individual obtained states:

> 12Jul07 conducting walkthrough of Boneyard Ale House at 9212 34 Ave near closing time. Observed known gang member [redacted in original] at the front entrance. I had dealt with him before at Rumours and he was hostile. Less trouble on this date and seemed mellow, said he was working occasionally for his cousin who owns [a construction company] but would not say how his [cousin] was. Watched as he left with [the Applicant] who is also a known trafficker and wanna be bad dude. [Street check report submitted for association].

The individual made the following correction request under the FOIP Act to EPS regarding this street check:

> It has come to [the individual's] attention that on July 7, 2012, [a Constable] authored a Street Check Report in which he asserted that [the individual] is "a known trafficker and wanna be bad dude". This information is inaccurate, inflammatory and highly prejudicial.
>
> Pursuant to s.36 of the *Freedom of Information and Protection of Privacy Act*, I am hereby requesting on [the individual's] behalf that this record be corrected to remove the allegation that [the individual] is a "known trafficker" and a "wanna be bad dude".

EPS refused to correct the information on the basis that it was opinion. It appended the information to the individual's request pursuant to section 36(3) of the FOIP Act, which requires a public body to annotate or link a correction request to personal information, rather than correct it, when the personal information that is the subject of the request is opinion.

The Adjudicator determined that EPS had complied with its duty under section 36 of the FOIP Act.

The Adjudicator found that the correction request was more properly characterized as a privacy complaint, rather than a correction request, in that EPS had not met its duty to the applicant to ensure the accuracy and completeness of personal information that it would use to make decisions affecting the individual's rights.

The Adjudicator found that EPS had not demonstrated that it had made all reasonable efforts to ensure that the personal information at issue was accurate and complete for the purposes of making decisions when it was entered into EPROS and maintained in that database.

EPS was directed to comply with its duty under section 35 with regard to the statement that the applicant is a "known trafficker and wanna be bad dude", by ensuring that it would not be used to make decisions affecting the applicant's rights in the future.

Edmonton Police Service, Order F2021-03

Ensuring Accuracy of Statements in Health Records

An individual was treated at a hospital in his community and then the University of Alberta Hospital emergency department for an open tibia or fibula fracture. At his community hospital, a physician wrote the following statement on the applicant's chart: "supposedly was hit by a vehicle (whilst pointing a gun @ them)". A physician at the University of Alberta hospital also made a chart note regarding the individual pointing a gun.

The individual made a request under HIA to Alberta Health Services (AHS) that it delete both statements. He also complained that AHS had not collected the information that was the source of the statement directly, as required by HIA, and that it had not used his health information in accordance with that Act.

The Adjudicator found that AHS' collection and use of the individual's information was in compliance with HIA, given the emergency department setting in which the information was collected and used. However, with respect to potential future use or disclosure, the Adjudicator made the following order to AHS at para. 75:

> I order AHS to determine whether there is any likelihood that the statements at issue could be accessed and then used or disclosed in the future. If it determines that there is any possibility that the information could be used again, then AHS should take steps to ensure that the information is not accessible, or to amend it to warn future users that the information may not be sufficiently reliable for use or disclosure unless reasonable steps are first taken to ensure its accuracy.

In making this order, the Adjudicator set out the following three questions at para. 50 for evaluating a request for correction or amendment:

1. Is the information likely to be used in the future? For example, is the information located in a paper record to which no one has access, or is the information part of an electronic health record accessible by many health service providers?
2. If it is likely that the information will be used or disclosed in the future, for what purpose is the information likely to be used or disclosed? For example, could the information be used to provide medical treatment in the future?
3. Is the information sufficiently accurate and complete to be reasonably used for those purposes? For example, could the information in question as it is written have a negative effect on treatment in the future or result in unfairness?

AHS applied for judicial review on this order. AHS challenged the Adjudicator's finding that the information at issue was not a professional opinion or observation under section 13(6) of HIA, and the reasonableness of the direction given to AHS to resolve the issue.

Alberta Health Services, Order H2020-05

Request for Staff Directory from Alberta Energy Regulator

An applicant requested under the FOIP Act an electronic copy of the complete staff directory for the Alberta Energy Regulator (AER), including job titles, phone numbers, email addresses and organization structure. AER located 61 pages of responsive records, but withheld all information citing disclosure harmful to personal privacy (section 17(1)) and information that is or will be available to the public (section 29). During the inquiry, AER also cited disclosure harmful to individual or public safety (section 18) as a reason for withholding all of the responsive records.

In Order F2019-09, the Adjudicator found that the information at issue is business contact information and not personal

information to which section 17(1) can apply. With respect to records withheld under section 29, AER said it only applied to certain staff members. The Adjudicator found that section 29 applied to limited information about certain staff members, but did not apply to the direct phone lines for those staff members or the organizational charts in the records at issue, as it was not publicly available. The Adjudicator also found that section 18(1)(a) did not apply to all of the information in the records at issue.

With respect to section 18, however, AER argued that because certain employees had been exempted from disclosure under the *Public Sector Compensation Transparency Act* "it could reasonably be expected that disclosure of any of their personal information into the public domain could jeopardize their safety." The Adjudicator responded, "Stating that another decision maker has found a similar test was met in a different context under a different statute is not sufficient." AER also said it would be improper for it to ask its own employees about highly sensitive personal information regarding potential harms to their safety or mental or physical health, specifically spousal abuse.

The Adjudicator ordered AER to disclose the information in the records at issues relating to employees who did not object to the disclosure on the grounds that disclosure could reasonably be expected to threaten their (or another's) safety or mental or physical health. The Adjudicator retained jurisdiction to decide the application of section 18(1) to the information relating to individuals who have objected to the disclosure of their names, job titles and business contact information in the records at issue. In order to retain jurisdiction, the Adjudicator said:

> This will require [AER] to provide notice to its employees.
>
> [AER] has indicated that information regarding spousal abuse is too sensitive for [AER] to ask its staff about. However, [AER] needn't inquire about that specific topic. There may be other reasons for the application of section 18(1) to an individual's name, title and contact information. In this case, I will direct [AER] to inform its staff that it has been ordered to disclose their names, job titles, contact information and the organizational structures in the records at issue to an applicant, subject to individual objections on the grounds that disclosure could reasonably be expected to threaten their (or another's) safety or mental or physical health under section 18(1).
>
> I require [AER] to inform the individual employees of the standard [AER] will have to meet for section 18(1) to apply to their information. [AER] can then inform me of the names of employees objecting to the disclosure of their names, job titles, and business contact information. [AER] will be required to inform the Applicant only of the number of individuals who have objected on the grounds of section 18(1). I will then determine how best to obtain submissions from these individuals in order to determine if section 18(1) applies in each case.

Sixteen AER employees provided submissions for the Adjudicator's review. In Order F2020-08, the Adjudicator found that several employees met the test for the application of section 18(1)(a), but most did not. The Adjudicator provided a list to AER of employees whose information must be disclosed to the applicant.

Alberta Energy Regulator, Order F2020-08

Privilege Properly Claimed on Edmonton Downtown Arena Deal Records

An applicant made a request to the City of Edmonton for records relating to the downtown arena development in Edmonton.

The City of Edmonton located responsive records but withheld them in their entirety, citing disclosure harmful to business interests of a third party (section 16(1)) and privileged information (section 27(1)(a)). The applicant requested a review of the records withheld and the time taken by the City of Edmonton to respond to his request (section 11).

While the City of Edmonton applied section 16(1) to some information in the records, no records were provided to the Adjudicator for the inquiry as all were withheld citing privilege. As a result, the Adjudicator addressed the City of Edmonton's claim of privilege under section 27(1) and the applicant's

concerns regarding the time taken to respond. The Adjudicator said section 16(1) would be addressed in a second part of the inquiry, if necessary.

The Adjudicator determined that the City of Edmonton's claim of privilege met the standard for claiming privilege as set out in *Canadian Natural Resources Limited v. ShawCor Ltd.,* 2014 ABCA 289 (CanLII), and was consistent with case law regarding solicitor-client privilege.

Following the Court's direction in *Edmonton Police Service v. Alberta (Information and Privacy Commissioner),* 2020 ABQB 10, the Adjudicator found that the City of Edmonton established its claim of privilege on a balance of probabilities.

Given that the Adjudicator found the City of Edmonton properly claimed privilege, there was no need to conduct a second part of the inquiry to decide on the City of Edmonton's application of section 16(1) to some of the information in the records.

The Adjudicator also found that the City of Edmonton did not respond the applicant within the time limit set out in section 11.

City of Edmonton, Order F2020-14

Distinguishing Between Personal and Representative Capacities

An individual, who appears as an agent in traffic court, complained that Alberta Justice and Solicitor General (JSG) had used his personal information in contravention of the FOIP Act.

The complainant said JSG diverted his request for disclosure in a traffic court matter on behalf of clients to its corporate security branch. The complainant alleged JSG then disclosed his personal information in contravention of the FOIP Act when the corporate security branch referred to the complainant as a "complex client" in a disclosure package he had requested on behalf of clients.

The Adjudicator found that JSG had not collected or used the complainant's personal information when it diverted his request for disclosure to the corporate security branch, as the complainant was acting in a representative, not personal, capacity when he made the request for disclosure.

The Adjudicator found, however, that the reference to the complainant as a "complex client" contravened the FOIP Act, because it was about the complainant in a personal, not a representative, capacity.

The Adjudicator ordered JSG to ensure that it did not include emails of this kind from the corporate security branch in Crown disclosure packages in the future, absent authority under section 40 of the FOIP Act to do so.

Alberta Justice and Solicitor General, Order F2020-30

Law Firm Improperly Collects Credit Report

An individual complained that Gowling WLG (Canada) LLP (Gowling WLG) violated PIPA when, during the course of ongoing litigation, it obtained his credit report and filed the credit report in Court as evidence in support of an application for security for future costs.

The Adjudicator considered the scope of PIPA with regard to section 4(3)(k) (the exclusion for court records). The Adjudicator held that Gowling WLG's use and disclosure of the information that occurred once it was filed in court were beyond the scope of PIPA; however, collection, use and disclosure that occurred prior to that were still subject to review.

The primary issue before the Adjudicator was whether the collection, use, and disclosure of the credit report in the absence of the complainant's consent was permitted by sections 14(d), 17(d) and 20(m) of PIPA (collection, use and disclosure that is reasonable for the purposes of an investigation or legal proceeding).

Underlying the issues of whether Gowling WLG complied with PIPA was the interaction between PIPA and the *Consumer Protection Act* (CPA). While PIPA prescribes when personal information may be collected without consent, CPA prescribes circumstances under which an organization may obtain a credit report from a reporting agency, and makes it an offence to collect the report in circumstances other than those prescribed. The question arose whether Gowling WLG had complied with the terms of CPA in obtaining the information, and if it had not,

whether this meant that its dealings with the information were "reasonable" as required by sections 14(d), 17(d), and 20(m) of PIPA.

The Adjudicator found that the terms of terms of PIPA and CPA are not inconsistent and therefore operate alongside each other. PIPA permits only reasonable collection. To determine reasonable collection, whether the information was collected under circumstances that are permitted by CPA must be considered.

The Adjudicator concluded that he did not have jurisdiction to determine whether CPA was contravened. However, the Adjudicator decided that under the Commissioner's powers to determine all questions of fact and law in section 50(1) of PIPA, the Adjudicator was able to take the terms of CPA into account in the inquiry. The terms of CPA were relevant to determining whether Gowling WLG's dealings with the complainant's personal information had been reasonable.

The Adjudicator found that Gowling WLG collected the personal information in the credit report outside of the circumstances permitted under section 44 of CPA.

Since collecting information outside of the circumstances under section 44 of the CPA is an offence under section 161(c) of CPA, collecting it in such circumstances was not reasonable for the purposes of a legal proceeding. Accordingly, Gowling WLG did not have authority to collect, use, and disclose personal information under sections 14(d), 17(d), and 20(m), and had not complied with section 7(1) of PIPA.

The Adjudicator applied similar reasoning to conclude that Gowling WLG's collection, use, and disclosure of the credit report had been beyond a reasonable extent under sections 11(2), 16(2) and 19(2) of PIPA.

The Adjudicator ordered Gowling WLG to cease collecting, using and disclosing personal information in contravention of PIPA, and to destroy the complainant's personal information, with the exception of the copy of the credit report contained in the court file and any copy made from such a copy.

Gowling WLG (Canada) LLP, Order P2020-03

Paternity Test and Genetic Information Improperly Disclosed

In the course of divorce proceedings, an individual underwent paternity testing to determine if he was the father of his daughter. Divergent Health Care Limited (Divergent Health) performed the test. The individual's (now) former wife was his daughter's legal guardian at the time of the test. Since his daughter was a minor, his former wife provided consent for his daughter to participate in the test. The lawyer representing the individual's former wife arranged the test with Divergent Health. Per its standard practice, Divergent Health released the results of the test to the individual and his former wife. Divergent Health also disclosed the results directly to the lawyer.

The individual complained that Divergent Health disclosed his personal information, without consent, in contravention of PIPA.

The Adjudicator found that information confirming the complainant's relation to his daughter was jointly the complainant's and his daughter's personal information. The Adjudicator found that while the complainant's former wife had authority to consent to disclosure of his daughter's personal information under section 61(1)(c) of PIPA as her guardian, that authority did not extend to consent to disclosure of the complainant's personal information, even for personal information that was jointly the complainant's and his daughter's.

The Adjudicator found that Divergent Health collected the complainant's personal information for the particular purpose of conducting its business of paternity testing, as usual. Disclosure to the lawyer, or to anyone for the purposes of a legal proceeding, was not included in that particular purpose. Therefore, per section 8(4), section 8(2) could not be construed to allow it. The same reasoning applied regarding Divergent Health's authority to disclose personal information under section 8(3) of PIPA.

The Adjudicator found that the complainant is deemed to have consented to disclosure of some of his personal information to his former wife, under section 8(2), for the purpose for which his personal information was collected. The Adjudicator found that the complainant was not deemed to consent to disclosure

of genetic information about his alleles. Given that disclosing it was not necessary to determine paternity, the complainant did not voluntarily provide his genetic information for the purposes of disclosure as required by section 8(2)(a).

The Adjudicator found that Divergent Health did not give proper notice under section 8(3) that it would disclose the complainant's genetic information. Even if it had, given the sensitivity of that information, disclosure was not reasonable under section 8(3)(c).

The Adjudicator found that Divergent Health did not in fact disclose the complainant's personal information to either his former wife or her lawyer for the purposes of a legal proceeding within the terms of section 20(m). Even had that been the case, the Adjudicator found that it would not have been reasonable for Divergent Health to disclose the complainant's personal information under section 20(m) for the purposes of legal proceedings between the complainant and his former wife. There was no nexus between Divergent Health and the legal proceedings. Disclosing information for the purposes of a legal proceeding was therefore unreasonable.

The Adjudicator found that, with the exception of the complainant's genetic information, disclosure of his personal information to his former wife as part of providing paternity testing services was for a reasonable purpose under section 19(1), and to a reasonable extent under section 19(2). Since disclosing the complainant's genetic information was not necessary to inform the complainant's former wife about the results of the paternity test, disclosure of it was not for a reasonable purpose under section 19(1) and went beyond a reasonable extent under section 19(2).

Since there was no reasonable purpose for it to disclose information to the lawyer, the Adjudicator found that disclosure to the lawyer was unreasonable under section 19(1), and beyond a reasonable extent under section 19(2).

The Adjudicator ordered Divergent Health to cease disclosing information in contravention of PIPA.

Divergent Health Care Limited, P2020-05

Using Health Information to Defend the Provision of Health Services

An individual made a complaint under HIA that his electronic health record may have been accessed by Alberta Health Services (AHS) without authority.

Many of the accesses were found to be authorized under various section 27 provisions. However, AHS and the complainant indicated that a number of the disputed accesses related to a civil action initiated by the complainant against named AHS doctors and AHS itself.

For the accesses related to civil action, the Adjudicator applied the principles set out by the Alberta Court of Appeal in *JK v. Gowrishankar* to use of health information for providing health services in HIA (section 27(1)(a)). The Adjudicator determined that using health information to provide a health service includes using that information to defend the provision of the health service in a subsequent proceeding (see paras. 16-53 for the rationale, application and limits of this interpretation).

Overall, the Adjudicator determined that each affiliate of AHS had authority to access the complainant's health information in the electronic health record.

Alberta Health Services, H2020-04

Judicial Reviews and Other Court Decisions

JUDICIAL REVIEWS

Alberta Health Services v Farkas

2020 ABQB 281 - Judicial Review of Orders F2019-19 and H2019-01

An individual (applicant) was the executor of his mother's estate and made an access request to Alberta Health Services (AHS) for records relating to the care of his mother. AHS provided a response under the FOIP Act, withholding some information under section 17(1) (disclosure harmful to personal privacy), 24(1)(b) (advice to officials) and 27(1)(a) (privileged information). At inquiry, the Adjudicator determined that as the information was about the applicant's mother's health and the care provided to her, the majority of AHS' severing decisions fell within HIA, rather than the FOIP Act. Accordingly, the FOIP Act did not apply and the information severed under sections 24(1)(b) and 27(1)(a) of the FOIP Act could not be withheld from the applicant.

On judicial review, the Court held that as the redactions under section 27(1)(a) of the FOIP Act raised issues of solicitor-client privilege, they were questions of central importance to the legal system as a whole and were subject to review on the correctness standard. The redactions under section 24(1)(b) of the FOIP Act were reviewable on a reasonableness standard.

The Court held that some of the withheld information was health information, but as other withheld information contained solicitor-client privileged information, it was not health information, and the FOIP Act applied. The Court held that solicitor-client privilege is entitled to near absolute protection under the law and quashed Orders F2019-19 and H2019-01. In concluding, the Court held that the privileged records should not be disclosed to the applicant, some of the records containing health information should be disclosed to the applicant, and the remainder of the matter, concerning redactions under section 24(1)(b) of FOIP, was remitted back to the Commissioner.

Cyrynowski v Edmonton Public School District No 7

2020 ABQB 544 – Judicial Review of Order F2019-25

An individual (applicant) requested access to records between staff of the Edmonton Public School District No 7 (EPSD) relating to himself. EPSD provided some responsive information, but withheld some as non-responsive and withheld other information under sections 17 (disclosure harmful to personal privacy), 20 (disclosure harmful to law enforcement), 24(1)(b) (advice from officials) and 27 (privileged information). The applicant requested a review of EPSD's severing decisions with regard to section 24(1)(b) only. In Order F2019-25, the Adjudicator confirmed EPSD's decision to sever the information to which it had applied section 24(1)(b) only.

The applicant requested a judicial review. The Court noted that the underlying policy rationale for the "consultations and deliberations" exception is the encouragement of the free seeking and giving of advice and suggestions among public decision makers, with a view to ensuring informed, responsive, thorough and timely decisions. The Court upheld the Adjudicator's decision upholding EPSD's redactions under section 24(1)(b) of FOIP, and dismissed the judicial review.

OTHER COURT DECISIONS

Alberta Health Services v Alberta (Information and Privacy Commissioner)

2020 ABQB 263

This matter involved the interpretation of the provisions of Restricted Court Access Order that had previously been granted in the judicial review of Order H2014-02 *(Alberta Health Services v Information and Privacy Commissioner of Alberta,* 2018 ABQB 467). The Restricted Court Access Order allowed the Court to seal the contents of the Certified Record of Proceedings so that the personal information, including the medical information of an individual, was not publicly available, and required destruction of that information by some parties.

Following the conclusion of the judicial review, both the individual and Alberta Health Services (AHS) applied to the Court for direction on the interpretation of the order. The Court held the OIPC and its legal counsel had complied with the order. The Court dismissed the individual's application and granted the variation sought by AHS, holding that the order applied to the information that was created or shared within the context of the judicial review proceedings, but not to all of the individual's personal, medical or health information.

Makis v Alberta Health Services

2020 ABCA 168

In 2018, an individual was declared a vexatious litigant, and as part of that decision, the Court stayed all actions ongoing before any non-judicial body, which included matters before the OIPC (2018 ABQB 976). The Court of Appeal granted the Commissioner leave to intervene in the appeal (2019 ABCA 288).

The Court of Appeal heard this matter as part of a trilogy of vexatious litigant cases in which the Court confirmed that the legal test set out in the *Judicature Act* is to be applied by Courts when reviewing vexatious litigant applications. On the issue of courts restraining access to administrative tribunals, the Court of Appeal held that such orders should *prima facie* be made only with notice to an affected tribunal and on the request or concurrence of an affected tribunal. The matter was remitted to the case management judge.

EDUCATION & OUTREACH

25 Years of the FOIP Act

The OIPC was planning to host an event to celebrate 25 years of the FOIP Act on October 1, 2020. When those plans came to a halt, the plan shifted.

To recognize 25 years of public sector access and privacy law in Alberta, the OIPC developed a logo that staff used in email signature lines. The logo was also on the OIPC's website.

On October 1, 2020, the OIPC issued a chronology (tweet thread) about the FOIP Act's beginnings:

- Today marks 25 years of Alberta's *Freedom of Information and Protection of Privacy Act.* To recognize the day, let us look back on how it came to be.
- The first iteration of an access to information law in Alberta was introduced on June 5, 1989 as Bill 203, Freedom of Information and Protection of Personal Privacy Act. It was a private member's bill sponsored by Opposition Leader Laurence Decore.
- Mr. Decore reintroduced the Freedom of Information and Protection of Personal Privacy Act as Bill 205 in March 1990, Bill 204 in March 1991, Bill 202 in March 1993 and Bill 201 in September 1993. None made it past first reading.
- NDP Leader Ray Martin also introduced Bill 201, Freedom of Information and Personal Privacy Act, in March 1993. In total, opposition members submitted six private member's bills for a freedom of information law.
- On April 26, 1993, Premier Ralph Klein introduced Bill 61, Access to Information and Protection of Privacy Act, in the legislature stating that it is "a major step" towards ensuring access to government information and protection of privacy.
- On August 31, 1993, Premier Klein reintroduced the Access to Information and Protection of Privacy Act, 1993 as Bill 1. He also introduced to the legislature the all-party committee that would lead a public consultation on the bill.
- The committee that facilitated the public review of Bill 1 was chaired by Government MLA Ty Lund. The committee's final report and recommendations were issued in December 1993.
- The committee made several recommendations, such as giving the Commissioner the power to make binding rulings and adding public interest provisions. The panel also recommended changing the name to "freedom of information" rather than "access to information".
- "Consultations with Albertans have allowed us to prepare a Bill that reflects the needs, desires, and goals of the people of this province," said Premier Klein on March 31, 1994 when introducing Bill 18, Freedom of Information and Protection of Privacy Act.
- When Bill 18 passed third reading on May 31, 1994, Opposition MLA Gary Dickson – who would later serve as the Information and Privacy Commissioner of Saskatchewan – recognized the government's efforts to improve the bill.
- Mr. Lund returned the comments in kind and recognized the work of the committee and the public's thoughtful feedback in making recommendations to improve the law.

- When the FOIP Act came into force on October 1, 1995, the Calgary Herald ran two articles – one that described some of the early issues facing government and another that introduced the public to the process for submitting requests.
- In particular, the Herald spoke to three people for whom "the new law marks the completion of a real labor of love" – Mr. Dickson, Sue Kessler, Public Works' director of info. management and privacy, and John Ennis, one of the OIPC's first staff members.
- At first, FOIP only applied to the provincial government. It was extended to school boards and health care bodies in 1998, and post-secondary institutions and local government bodies, such as municipalities and police services, in 1999.
- In closing, we must also recognize the tremendous contributions of Robert C. Clark, Alberta's first Information and Privacy Commissioner, who passed away [in 2020]. He left an indelible imprint on the access and privacy world in Alberta.

Speaking Engagements

The Commissioner and staff made 14 presentations in 2020-21, a significant reduction due to the COVID-19 pandemic. The OIPC has also declined more speaking engagement requests over the past three years in order to focus on increasing caseloads.

UNESCO'S AI4IA

For the 2020 International Day for Universal Access to Information, also known as Right to Know Day, the Commissioner was invited by UNESCO's Information For All Programme Working Group on Information Accessibility to present on the theme of Artificial Intelligence for Information Accessibility (AI4IA). UNESCO's global theme for Right to Know Day was, "Saving Lives, Building Trust, Bringing Hope".

The Commissioner's presentation focused on ethical tech development in the context of information accessibility. In particular, the presentation discussed ethical assessments of AI, algorithmic transparency when decisions are being made about or for individuals, and the promise of synthetic data and other AI-driven privacy protective technologies to uphold privacy while dealing with sensitive humanitarian development projects.

Right to Know Day occurs every September 28 to highlight the importance of access to information in supporting effective and accountable government institutions.

Collaboration with Other Jurisdictions

The OIPC works with Information and Privacy Commissioners across Canada, as well as international counterparts, on a variety of initiatives.

ACCESS TO INFORMATION IN THE CONTEXT OF A GLOBAL PANDEMIC

The Commissioner, who also serves as a governance working group member of the International Conference of Information Commissioners (ICIC), supported the following statement issued in April 2020 by the ICIC:

> The impact of coronavirus (COVID-19) brings unprecedented challenges for our society, both nationally and globally.
>
> Public authorities must make significant decisions that affect public health, civil liberties and people's prosperity.
>
> The public's right to access information about such decisions is vital.
>
> As a global community, we recognise that resources may be diverted away from usual information rights work. Public organisations will rightly focus their resources on protecting public health, and we recognise our role in taking a pragmatic approach, for example around how quickly public bodies respond to requests.
>
> But the importance of the right to access information remains.
>
> Public bodies must also recognise the value of clear and transparent communication, and of good record-keeping, in what will be a much analysed period of history.
>
> As an international network, the ICIC supports a flexible approach that takes into account the compelling public interest in the current health emergency, while safeguarding the values of the right to access information. We ask governments to support this vision.
>
> We add our support and gratitude to those who are dedicated to tackling the current pandemic.
>
> *- Members of the ICIC Governance Working Group*

SECURING PERSONAL INFORMATION SELF-ASSESSMENT TOOL

In recognition of Cybersecurity Month, the OIPC, Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner for British Columbia updated their guidance on securing personal information with a self-assessment tool for public bodies and organizations.

Public bodies and organizations are required under law to take reasonable steps to safeguard the personal information in their custody or control from such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction. The self-assessment tool is designed to help public bodies and organizations determine how well they are protecting personal information.

Media Awareness

TRADITIONAL MEDIA

The OIPC had 86 media requests in 2020-21, a decrease of 9% from 2019-20 (95).

The following topics generated the most media requests:

- Contact tracing, generally, and specifically questions about the ABTraceTogether contact-tracing app
- The release of the Clearview AI investigation report
- The release of the Cadillac Fairview investigation report
- Bill 46, which made amendments to HIA, and the OIPC's concerns with those amendments
- The announcement of the Babylon by Telus Health investigation

SOCIAL MEDIA

Twitter is used by the OIPC to share orders, investigation reports, publications and news releases, and promote events or raise awareness about access and privacy laws.

The following topics received among the most views or engagements on Twitter:

- The Commissioner's comments on proposed amendments to HIA within Bill 46
- The Commissioner's statement that there was no consultation on Bill 46
- The announcement of the Babylon by Telus Health investigation
- The Commissioner's statement in response to the announcement of the ABTraceTogether contact-tracing app
- The release of the section 32 investigation report, which looked into the use of the FOIP Act's "public interest override" provision by Alberta public bodies

The OIPC's Twitter account is available at www.twitter.com/ABoipc.

Publications

The OIPC issued the following resources in 2020-21:

- Managing Records When Transitioning from Work to Home (April 2020)
- Pandemic FAQ: Customer Lists (June 2020)
- Forms for Inquiry Procedures (September 2020)
- Securing Personal Information: A Self-Assessment Tool for Public Bodies and Organizations (October 2020)
- Advisory for Web Buckets (October 2020)
- Access to Information Laws in Alberta Brochure (March 2021)
- Privacy Laws in Alberta Brochure (March 2021)
- Guidelines for Usage-Based Insurance (March 2021)

FINANCIAL STATEMENTS

Auditor General
OF ALBERTA

Independent Auditor's Report

To the Members of the Legislative Assembly

Report on the Financial Statements

Opinion

I have audited the financial statements of the Office of the Information and Privacy Commissioner (the OIPC), which comprise the statement of financial position as at March 31, 2021, and the statements of operations, change in net debt, and cash flows for the year then ended, and notes to the financial statements, including a summary of significant accounting policies.

In my opinion, the accompanying financial statements present fairly, in all material respects, the financial position of the OIPC as at March 31, 2021, and the results of its operations, its changes in net debt, and its cash flows for the year then ended in accordance with Canadian public sector accounting standards.

Basis for opinion

I conducted my audit in accordance with Canadian generally accepted auditing standards. My responsibilities under those standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Statements* section of my report. I am independent of the OIPC in accordance with the ethical requirements that are relevant to my audit of the financial statements in Canada, and I have fulfilled my other ethical responsibilities in accordance with these requirements. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my opinion.

Other information

Management is responsible for the other information. The other information comprises the information included in the *Annual Report*, but does not include the financial statements and my auditor's report thereon. The *Annual Report* is expected to be made available to me after the date of this auditor's report.

My opinion on the financial statements does not cover the other information and I do not express any form of assurance conclusion thereon.

In connection with my audit of the financial statements, my responsibility is to read the other information identified above and, in doing so, consider whether the other information is materially inconsistent with the financial statements or my knowledge obtained in the audit, or otherwise appears to be materially misstated.

If, based on the work I will perform on this other information, I conclude that there is a material misstatement of this other information, I am required to communicate the matter to those charged with governance.

Responsibilities of management and those charged with governance for the financial statements

Management is responsible for the preparation and fair presentation of the financial statements in accordance with Canadian public sector accounting standards, and for such internal control as management determines is necessary to enable the preparation of the financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, management is responsible for assessing the OIPC's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless an intention exists to liquidate or to cease operations, or there is no realistic alternative but to do so.

Those charged with governance are responsible for overseeing the OIPC's financial reporting process.

Auditor's responsibilities for the audit of the financial statements

My objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with Canadian generally accepted auditing standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

As part of an audit in accordance with Canadian generally accepted auditing standards, I exercise professional judgment and maintain professional skepticism throughout the audit. I also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for my opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the OIPC's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.
- Conclude on the appropriateness of management's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the OIPC's ability to continue as a going concern. If I conclude that a material uncertainty exists, I am required to draw attention in my auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify my opinion. My conclusions are based on the audit evidence obtained up to the date of my auditor's report. However, future events or conditions may cause the OIPC to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

I communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that I identify during my audit.

Original signed by
W. Doug Wylie FCPA, FCMA, ICD.D

Auditor General
July 6, 2021
Edmonton, Alberta

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
STATEMENT OF OPERATIONS

Year ended March 31, 2021

	2021		2020
	Budget	Actual	Actual
Revenues			
Prior Year Expenditure Refund	$ -	$ 1,117	$ 33
Other Revenue	-	1,131	1,075
	-	2,248	1,108
Expenses – Directly Incurred (Note 3b)			
Salaries, Wages, and Employee Benefits	$ 6,172,300	$ 5,805,608	$ 5,469,871
Supplies and Services	1,083,700	1,253,519	1,309,299
Amortization of Tangible Capital Assets (Note 5)	-	29,435	22,369
Total Program-Operations	7,256,000	7,088,562	6,801,539
Net Cost of Operations	$ (7,256,000)	$ (7,086,314)	$ (6,800,431)

The accompanying notes and schedules are part of these financial statements.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

STATEMENT OF FINANCIAL POSITION

As at March 31, 2021

	2021	2020
Financial Assets		
Cash	$ 200	$ 200
Accounts Receivable	57,884	112
	58,084	312
Liabilities		
Accounts Payable and Other Accrued Liabilities	454,277	313,897
Accrued Vacation Pay	536,172	493,589
	990,449	807,486
Net Debt	(932,365)	(807,174)
Non-Financial Assets		
Tangible Capital Assets (Note 5)	223,577	97,255
Prepaid Expenses	53,738	9,509
	277,315	106,764
Net Liabilities	$ (655,050)	$ (700,410)
Net Liabilities at Beginning of Year	$ (700,410)	$ (557,980)
Net Cost of Operations	(7,086,314)	(6,800,431)
Net Financing Provided from General Revenues	7,131,674	6,658,001
Net Liabilities at End of Year	$ (655,050)	$ (700,410)

Contractual obligations (Note 7)

The accompanying notes and schedules are part of these financial statements.

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

STATEMENT OF CHANGE IN NET DEBT

Year ended March 31, 2021

	2021		2020
	Budget	Actual	Actual
Net Cost of Operations	$ (7,256,000)	$ (7,086,314)	$ (6,800,431)
Acquisition of Tangible Capital Assets (Note 5)		(155,757)	(56,009)
Amortization of Tangible Capital Assets (Note 5)	-	29,435	22,369
(Increase)/Decrease in Prepaid Expenses		(44,229)	21,029
Net Financing Provided from General Revenues		7,131,674	6,658,001
Increase in Net Debt		(125,191)	(155,041)
Net Debt, Beginning of Year		(807,174)	(652,133)
Net Debt, End of Year		$ (932,365)	$ (807,174)

The accompanying notes and schedules are part of these financial statements.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
STATEMENT OF CASH FLOWS

Year ended March 31, 2021

	2021	2020
Operating Transactions		
Net Cost of Operations	$ (7,086,314)	$ (6,800,431)
Non-cash Items Included in Net Cost of Operations		
Amortization of Tangible Capital Assets (Note 5)	29,435	22,369
	(7,056,879)	(6,778,062)
Increase in Accounts Receivable	(57,772)	(102)
(Increase)/Decrease in Prepaid Expenses	(44,229)	21,029
Increase in Accounts Payable and Other Accrued Liabilities	182,963	155,143
Cash Applied to Operating Transactions	(6,975,917)	(6,601,992)
Capital Transactions		
Acquisition of Tangible Capital Assets (Note 5)	(155,757)	(56,009)
Financing Transactions		
Net Financing Provided from General Revenues	7,131,674	6,658,001
Cash, Increase	-	-
Cash, at Beginning of Year	200	200
Cash, at End of Year	$ 200	$ 200

The accompanying notes and schedules are part of these financial statements.

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NOTES TO THE FINANCIAL STATEMENTS

March 31, 2021

Note 1 Authority

The Office of the Information and Privacy Commissioner (the Office) operates under the authority of the *Freedom of Information and Protection of Privacy Act*. General Revenues of the Province of Alberta fund both the cost of operations of the Office and the purchase of tangible capital assets. The all-party Standing Committee on Legislative Offices reviews and approves the Office's annual operating and capital budgets.

Note 2 Purpose

The Office provides oversight on the following legislation governing access to information and protection of privacy:

Freedom of Information and Protection of Privacy Act
Health Information Act
Personal Information Protection Act

The major operational purposes of the Office are:

- To provide independent reviews of decisions made by public bodies, custodians and organizations under the Acts and the resolution of complaints under the Acts;
- To advocate protection of privacy for Albertans; and
- To promote openness and accountability for public bodies.

Note 3 Summary of Significant Accounting Policies and Reporting Practices

Reporting Entity

These financial statements are prepared in accordance with Canadian public sector accounting standards, which use accrual accounting. The Office has adopted PS 3450 Financial Instruments. The adoption of this standard has no material impact on the financial statements of the Office, which is why there is no statement of remeasurement gains and losses.

Other pronouncements issued by the Public Sector Accounting Board that are not yet effective are not expected to have a material impact on future financial statements of the Office.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2021

Note 3 Summary of Significant Accounting Policies and Reporting Practices (continued)

Basis of Financial Reporting

(a) Revenue

All revenues are reported on the accrual basis of accounting.

(b) Expenses

Expenses are reported on an accrual basis. The Office's expenses are either directly incurred or incurred by others:

Directly incurred

Directly incurred expenses are those costs incurred under the authority of the Office's budget as disclosed in the Office's budget documents.

Pension costs included in directly incurred expenses comprise employer contributions to multi-employer plans. The contributions are based on actuarially determined amounts that are expected to provide the plans' future benefits.

Incurred by others

Services contributed by other entities in support of the Office's operations are not recognized and are disclosed in Schedule 2.

(c) Financial assets

Financial assets are assets that could be used to discharge existing liabilities or finance future operations and are not for consumption in the normal course of operations.

Accounts Receivable

Accounts receivable are recognized at the lower of cost or net recoverable value. A valuation allowance is recognized when recovery is uncertain.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2021

Note 3 Summary of Significant Accounting Policies and Reporting Practices (continued)

(d) Liabilities

Liabilities are present obligations of the Office to external organizations and individuals arising from past transactions or events, the settlement of which is expected to result in the future sacrifice of economic benefits.

They are recognized when there is an appropriate basis of measurement and management can reasonably estimate the amounts.

(e) Non-financial assets

Non-financial assets are acquired, constructed, or developed assets that do not normally provide resources to discharge existing liabilities, but instead:

- are normally employed to deliver the Office's services;
- may be consumed in the normal course of operations; and
- are not for sale in the normal course of operations.

Non-financial assets of the Office includes tangible capital assets and prepaid expenses.

Tangible capital assets

Tangible capital assets are recorded at historical cost less accumulated amortization. Amortization begins when the assets are put into service and is recorded on a straight-line basis over the estimated useful lives of the assets. The threshold for tangible capital assets is $5,000 except new systems development is $250,000 and major enhancements to existing systems is $100,000.

Prepaid expenses

Prepaid expenses is recognized at cost and amortized based on the terms of the agreement.

(f) Net debt

Net debt indicates additional cash required from General Revenues to finance the Office's cost of operations to March 31, 2021.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2021

Note 4 Future Changes in Accounting Standards

The Public Sector Accounting Board has approved the following accounting standards:

- PS 3280 Asset Retirement Obligations (effective April 1, 2022)
  This standard provides guidance on how to account for and report liabilities for retirement of tangible capital assets.
- PS 3400 Revenue (effective April 1, 2023)
  This standard provides guidance on how to account for and report on revenue, and specifically, it differentiates between revenue arising from exchange transactions and non-exchange transactions.

The Office has not yet adopted these standards. Management is currently assessing the impact of these standards on the financial statements.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2021

Note 5 Tangible Capital Assets

	Leasehold Improvements	Office Furniture and Equipment	Computer Hardware and Software	2021 Total	2020 Total
Estimated Useful Life	5 years	5 years	5 years		
Historical Cost					
Beginning of Year	$ -	$86,445	$492,672	$579,117	$535,661
Additions	43,142	18,772	93,843	155,757	56,009
Disposals	-	-	-	-	(12,553)
	$43,412	$105,217	$586,515	$734,874	$579,117
Accumulated Amortization					
Beginning of Year	$ -	$71,026	$410,836	$481,862	$472,046
Amortization Expense	3,011	3,136	23,288	29,435	22,369
Disposals	-	-	-	-	(12,553)
	$3,011	$74,162	$434,124	$511,297	$481,862
Net Book Value at March 31, 2021	$40,131	$31,055	$152,391	$223,577	
Net Book Value at March 31, 2020	-	$15,419	$81,836		$97,255

Included in the additions is $87,830 (2020 - $40,328) of capital work in progress.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2021

Note 6 Defined Benefit Plans

The Office participates in the multi-employer pension plans: Management Employees Pension Plan, Public Service Pension Plan and Supplementary Retirement Plan for Public Service Managers. The expense for these pension plans is equivalent to the annual contributions of $598,030 for the year ended March 31, 2021 (2020 – $660,040).

At December 31, 2020, the Management Employees Pension Plan reported a surplus of $809,850,000 (2019 - surplus $1,008,135,000) and the Public Service Pension Plan reported a surplus of $2,223,582,000 (2019 – surplus $2,759,320,000). At December 31, 2020 the Supplementary Retirement Plan for Public Service Managers had a deficit of $59,972,000 (2019 - deficit $44,698,000).

The Office also participates in a multi-employer Long Term Disability Income Continuance Plan. At March 31, 2021, the Management, Opted Out and Excluded Plan reported an actuarial surplus of $7,858,000 (2020 – surplus $11,635,000). The expense for this plan is limited to employer's annual contributions for the year.

Note 7 Contractual Obligations

Contractual Obligations are obligations of the Office to others that will become liabilities in the future when the terms of those contracts or agreements are met.

	2021	2020
Obligations under operating leases and contracts	$ 12,600	$ 11,681

Estimated payment requirements for each of the next two years are as follows:

	Total
2021-22	$ 10,743
2022-23	1,857
	$ 12,600

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2021

Note 8 Budget

The budget shown on the statement of operations is based on the budgeted expenses that the all-party Standing Committee on Legislative Offices approved on November 22, 2019. The following table compares the office's actual expenditures, excluding non-voted amounts such as amortization, to the approved budgets:

	Voted Budget	Actual	Unexpended (Over-expended)
Operating expenditures	$ 7,256,000	$ 7,059,127	$ 196,873
Capital investment	-	155,757	(155,757)
	$ 7,256,000	$ 7,214,884	$ 41,116

Note 9 Comparative Figures

Certain 2020 figures have been reclassified to conform to the 2021 presentation.

Note 10 Approval of Financial Statements

These financial statements were approved by the Information and Privacy Commissioner.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 1 - SALARY AND BENEFITS DISCLOSURE

Year ended March 31, 2021

	2021			2020
	Base Salary [a]	Other Non-cash Benefits [b][c]	Total	Total
Senior Official				
Information and Privacy Commissioner	$ 255,424	$ 57,089	$ 312,513	$ 305,446

[a] Base salary is comprised of pensionable base pay.

[b] Other non-cash benefits include the Office's share of all employee benefits and contributions or payments made on behalf of employee, including pension, supplementary retirement plan, health care, dental coverage, group life insurance, short and long term disability plans, health spending account, conference fees, professional memberships, and tuition fees.

[c] Other non-cash benefits for the Information and Privacy Commissioner paid by the Office includes $7,056 (2020: $6,891) being the lease, fuel, insurance and maintenance expenses for an automobile provided by the Office.

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 2 - RELATED PARTY TRANSACTIONS

Year ended March 31, 2021

Related parties are those entities consolidated or accounted for on the modified equity basis in the Government of Alberta's Consolidated financial statements. Related parties also include key management personnel and close family members of those individuals in the Office. The Office and its employees paid or collected certain taxes and fees set by regulations for premiums, licenses and other charges. These amounts were incurred in the normal course of business, reflect charges applicable to all users, and have been excluded from this schedule.

The Office of the Information and Privacy Commissioner had the following transactions with related parties recorded on the Statement of Operations and the Statement of Financial Position at the amount of consideration agreed upon between the related parties:

	Other Entities	
	2021	2020
Expenses - Directly Incurred		
Alberta Risk Management Fund	$ 3,830	$ 3,709
Postage	10,314	11,395
Information Services	-	62
Technology Services	13,900	28,400
Consumption	6,441	3,149
Fleet vehicle	5,412	5,412
	$ 39,897	$ 52,127
Receivable from	$ 57,287	$ -
Payable to	$ 15,532	$ -

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 2 - RELATED PARTY TRANSACTIONS *(continued)*

Year ended March 31, 2021

The Office of the Information and Privacy Commissioner also had the following transactions with related parties for which no consideration was exchanged. The amounts for these related party transactions are estimated based on the costs incurred by the service provider to provide the service. These amounts are not recorded in the financial statements but are disclosed in Schedule 3.

	Other Entities	
	2021	2020
Expenses - Incurred by Others		
Accommodation Costs	$ 460,620	$ 447,481
Telephone Costs	-	16,680
Business Services	164,000	51,000
	$ 624,620	$ 515,161

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 3 - ALLOCATED COSTS

Year ended March 31, 2021

	2021				2020
	Expenses - Incurred by Others				
Program	Expenses [a]	Accommodation Costs [b]	Business Services [c]	Total Expenses	Total Expenses
Operations	$ 7,088,562	$ 460,620	$ 164,000	$ 7,713,182	$ 7,316,700

[a] Expenses - Directly Incurred as per Statement of Operations which include related party transactions as disclosed in Schedule 2.
[b] Costs shown for Accommodation (includes grants in lieu of taxes), allocated by square meters.
[c] Business services includes charges for shared services, finance services, technology services, IMAGIS/1GX, and Corporate Overhead.

APPENDICES

APPENDIX A: CASES OPENED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2020 to March 31, 2021

FOIP Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Disclosure to Commissioner (Whistleblower)	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request Authorization to Collect Indirectly	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies																	**0**
Boards			4				1					9		10	1		**25**
Colleges									1						15		**16**
Commissions									4		2	1	1	8	1		**17**
Committees											1						**1**
Foundations																	**0**
Government Ministries/Departments		1	8				1		2		4	99	21	213	10		**359**
Health Quality Council of Alberta																	**0**
Hospital Board (Covenant Health)												1					**1**
Law Enforcement Agencies			3			1	1	7	1			57		6	3		**79**
Legislative Assembly Office																	**0**
Local Government Bodies												3			6		**9**
Long Term Care Centres												1					**1**
Municipalities			8						3		1	68	11	17	20		**128**
Nursing Homes																	**0**
Office of the Premier/Alberta Executive Council												2		8			**10**
Officers of the Legislature																	**0**
Panels																	**0**
Regional Health Authorities (Alberta Health Services)									2			13	5	12			**32**
School Districts		2	3			1						6		1	18		**31**
Universities		1	2									16	1	13	3		**36**
Other							1		1		1	7	1	6	4		**22**
Total	**0**	**4**	**28**	**0**	**0**	**2**	**4**	**7**	**14**	**0**	**9**	**283**	**40**	**294**	**81**		**767**

Note: The statistics do not include Intake cases.

APPENDIX A: CASES OPENED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2020 to March 31, 2021

HIA

Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Affiliates and Information Managers (Electronic Medical Record Vendors, Consultants)						1			1	1				**3**
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians														**0**
Chiropractors									156		1		5	**162**
Dental Hygienists									22					**22**
Dentists			1						170				4	**175**
Denturists														**0**
Government Ministries/Departments										1		1		**2**
Health Professional Colleges and Associations										2			1	**3**
Health Quality Council of Alberta														**0**
Hospital Board (Covenant Health)									8				18	**26**
Long Term Care Centres									2	1	2		3	**8**
Midwives									7					**7**
Minister of Health (Alberta Health)									15	4	1		45	**65**
Nursing Homes									3				4	**7**
Opticians														**0**
Optometrists									59				1	**60**
Pharmacies/Pharmacists			1						274				274	**549**
Physicians			12			16			1,032	3	5		137	**1,205**
Podiatrists									2					**2**
Primary Care Networks									33				14	**47**
Regional Health Authorities (Alberta Health Services)			17			2			40		7		405	**471**
Registered Nurses									52				2	**54**
Research Ethics Boards														**0**
Researchers														**0**
Subsidiary Health Corporations			1							1	1		6	**9**
Universities/Faculties of Medicine									2	1				**3**
Other			1		1			11	10	5	2		11	**41**
Total	**0**	**0**	**33**	**0**	**1**	**19**	**0**	**11**	**1,888**	**19**	**19**	**1**	**930**	**2,921**

Note: The statistics do not include Intake cases.

APPENDIX A: CASES OPENED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2020 to March 31, 2021

PIPA / Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Advanced Ruling	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Accommodation & Food Services			1			2					1		9		**13**
Admin & Support Services											2		4		**6**
Agriculture, Forestry, Fishing & Hunting													2		**2**
Arts, Entertainment & Recreation										1	1		8		**10**
Child Daycare Services													1		**1**
Construction											1		5		**6**
Credit Bureaus													1		**1**
Credit Unions										1			11		**12**
Dealers in Automobiles			3										2		**5**
Educational Services			1			1					1		14		**17**
Finance			1										45		**46**
Health Care & Social Assistance			1			2			3		1		24		**31**
Information & Cultural Industries						1			1				18		**20**
Insurance Industry			2								2		22		**26**
Investigative & Security Services			1								1		1		**3**
Legal Services			2								2		6		**10**
Manufacturing													25		**25**
Medical & Diagnostic Laboratories															**0**
Mining, Oil & Gas		1									1		9		**11**
Nursing Homes/Home Health Care													3		**3**
Private Health Care & Social Assistance			3								1		7		**11**
Professional, Scientific & Technical			2			1			1				24		**28**
Public Administration			1							1					**2**
Real Estate, Rental, Leasing			11								10		15		**36**
Retail			5										38		**43**
Transportation											3		8		**11**
Utilities			1								1		4		**6**
Wholesale Trade			2								1		13		**16**
Other			9						1	1	8		58		**77**
Total	**0**	**1**	**46**	**0**	**0**	**7**	**0**	**0**	**6**	**0**	**4**	**37**	**0**	**377**	**478**

Note: The statistics do not include Intake cases.

APPENDIX B: CASES CLOSED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2020 to March 31, 2021

FOIP Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Disclosure to Commissioner (Whistleblower)	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request Authorization to Collect Indirectly	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies																	**0**
Boards			8				1		3			14	1	10	4		**41**
Colleges									1			1			18		**20**
Commissions			2						3		3	3	3	9	1		**24**
Committees											1						**1**
Foundations																	**0**
Government Ministries/Departments			13			8	1		10		5	68	15	220	23		**364**
Health Quality Council of Alberta																	**0**
Hospital Board (Covenant Health)																	**0**
Law Enforcement Agencies			8				1	7	1		1	48		6	2		**74**
Legislative Assembly Offices																	**0**
Local Government Bodies			3												10		**13**
Long Term Care Centres															1		**1**
Municipalities			13			2			7		3	64	3	17	18		**127**
Nursing Homes																	**0**
Office of the Premier/Alberta Executive Council												2		8			**10**
Officers of the Legislature							1										**1**
Panels																	**0**
Regional Health Authorities (Alberta Health Services)			1						2		1	8	4	12			**28**
School Districts		1	4			1	1					17	1	1	18		**44**
Universities			1				1					11	1	14	2		**30**
Other									2			5		6	5		**18**
Total	**0**	**1**	**53**	**0**	**0**	**11**	**6**	**7**	**3**	**27**	**0**	**14**	**241**	**28**	**303**	**102**	**796**

Note: The statistics do not include Intake cases.

APPENDIX B: CASES CLOSED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2020 to March 31, 2021

HIA

Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Affiliates and Information Managers (Electronic Medical Record Vendors, Consultants)									3					**3**
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians														**0**
Chiropractors								132				4		**136**
Dental Hygienists								16				1		**17**
Dentists			2					278		1		1		**282**
Denturists														**0**
Government Ministries/Departments									2		1			**3**
Health Professional Colleges and Associations								2	2					**4**
Health Quality Council of Alberta								2						**2**
Hospital Board (Covenant Health)			2					4				15		**21**
Long Term Care Centres								2				3		**5**
Midwives								9						**9**
Minister of Health (Alberta Health)								15	3			36		**54**
Nursing Homes								2	1	1		1		**5**
Opticians														**0**
Optometrists								39		1		2		**42**
Pharmacies/Pharmacists			10				1	198	2	1		160		**372**
Physicians			10					636	4	4		87		**741**
Podiatrists								2						**2**
Primary Care Networks			1					14	1			5		**21**
Regional Health Authorities (Alberta Health Services)			16			1	1	87	2	9		325		**441**
Registered Nurses								43						**43**
Research Ethics Boards														**0**
Researchers														**0**
Subsidiary Health Corporations								1				25		**26**
Universities/Faculties of Medicine								2	1			1		**4**
Other			1			1	10	7	3			9		**31**
Total	**0**	**0**	**42**	**0**	**0**	**2**	**0**	**12**	**1,491**	**24**	**17**	**1**	**675**	**2,264**

Note: The statistics do not include Intake cases.

APPENDIX B: CASES CLOSED UNDER FOIP, HIA, PIPA BY ENTITY TYPE

Statistics are from April 1, 2020 to March 31, 2021

PIPA / Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fee	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Advanced Ruling	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Accommodation & Food Services			4								1		8		**13**
Admin & Support Services			1								1		9		**11**
Agriculture, Forestry, Fishing & Hunting											1				**1**
Arts, Entertainment & Recreation			4					1	1	1			9		**16**
Child Daycare Services			1			1							2		**4**
Construction											3		8		**11**
Credit Bureaus															**0**
Credit Unions											1		10		**11**
Dealers in Automobiles			3										2		**5**
Educational Services													14		**14**
Finance			3			1					1		36		**41**
Health Care & Social Assistance			3			3		1			1		14		**22**
Information & Cultural Industries			4										19		**23**
Insurance Industry			3					1		1			33		**38**
Investigative & Security Services															**0**
Legal Services			6								3		9		**18**
Management of Companies & Enterprises			1			1									**2**
Manufacturing			1										14		**15**
Medical & Diagnostic Laboratories			2												**2**
Mining, Oil & Gas		1									5		12		**18**
Management of Companies & Enterprises			1												**1**
Nursing Homes/Home Health Care			1										1		**2**
Private Health Care & Social Assistance			2					1			5		7		**15**
Professional, Scientific & Technical			1								1		20		**22**
Public Administration			1							1					**2**
Real Estate, Rental, Leasing			11			1					6		8		**26**
Retail			1								2		31		**34**
Transportation			2								1		12		**15**
Utilities			2								1		6		**9**
Wholesale Trade			1										7		**8**
Other			7							1	3		47		**58**
Total	**0**	**1**	**66**	**0**	**0**	**7**	**0**	**0**	**4**	**1**	**4**	**36**	**0**	**338**	**457**

Note: The statistics do not include Intake cases.

APPENDIX C: ORDERS, DECISIONS AND PUBLIC INVESTIGATION REPORTS ISSUED

Statistics are from April 1, 2020 to March 31, 2021

FOIP Respondent	Orders	Decisions	Public Investigation Reports	Total
Alberta Energy Regulator	1			1
Alberta Health Services	3			3
Alberta Labour Relations Board		1		1
Alberta Public Bodies*			1	1
Board of Trustees of Edmonton School Division	1			1
Calgary Board of Education	2			2
Calgary Police Service	4			4
Capital Region Housing Corporation	1			1
Children's Services	1			1
City of Calgary	3			3
City of Edmonton	4			4
Edmonton Police Service	6			6
Energy	2			2
Environment and Parks	2			2
Indigenous Relations	1			1
Justice and Solicitor General	3			3
Regional Munipality of Wood Buffalo	1			1
Service Alberta	1			1
Thorhild County	1			1
Town of Athabasca	1			1
University of Calgary	2			2
Workers' Compensation Board	1			1
Subtotal	41	1	1	43

*Refers to Investigation Report F2020-IR-01 involving 87 public bodies.

HIA Respondent	Orders	Decisions	Public Investigation Reports	Total
Alberta Health Services	3			3
Subtotal	3	0	0	3

PIPA Respondent	Orders	Decisions	Public Investigation Reports	Total
Alberta Blue Cross	1			1
Cadillac Fairview Corporation Ltd.			1	1
Clearview AI, Inc.			1	1
Davidson & Williams LLP	1			1
Divergent Health Care Limited	1			1
General Teamsters Local Union No. 362	1			1
Gowling WLC (Canada) LLP	1			1
Hi Line Farm Equipment Ltd.	1			1
PriceWaterhouseCoopers LLP	1			1
The Anglican Diocese of Calgary	1			1
TWR C Motors GP Inc.	1			1
Weinrich Contracting Ltd.		1		1
Subtotal	9	1	2	12
Total	53	2	3	58

Total number of Orders, Decisions and public Investigation Reports issued:
FOIP Orders: 41 (43 cases)
FOIP Decisions: 1 (1 case)
HIA Orders: 3 (4 cases)
HIA Decisions: 0
PIPA Orders: 9 (10 cases)
PIPA Decisions: 1 (1 case)
FOIP Investigation Reports: 1 (1 case)
PIPA Investigation Reports: 2 (2 case)

Notes:

(1) This table contains all Orders and Decisions released by the OIPC whether the issuance of the Order or Decision concluded the matter or not.

(2) The number of Orders, Decisions and Investigation Reports are counted by the number of Order, Decision or Investigation Report numbers assigned. A single Order, Decision or Investigation Report can relate to more than one entity and more than one file.

(3) Orders and Decisions are recorded by the date the Order or Decision was signed, rather than the date the Order or Decision was publicly released.

(4) Only Investigation Reports that are publicly released are reported.

(5) Copies of all Orders, Decisions and public Investigation Reports are available at www.oipc.ab.ca.

www.oipc.ab.ca