Office of the Information and
Privacy Commissioner of Alberta

ANNUAL REPORT
2017-18

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 2018

Office of the Information and
Privacy Commissioner of Alberta

November 2018

The Honourable Robert E. Wanner
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, 2017 to March 31, 2018.

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.*

Yours truly,

Original signed by

Jill Clayton
Information and Privacy Commissioner

Table of Contents

Commissioner's Message

For the last few years, my annual report messages have been focused in large part on access to information issues, as measured by the number of deemed refusal orders issued by my office (when a public body, for example, simply does not provide a response to an applicant's request for access), time extension requests received, and investigations into overall delays.

I am cautiously optimistic that we may have turned a corner on this front in 2017-18. Not that all issues have been resolved – there is still a long way to go. But the number of deemed refusal orders issued by my office has decreased by 56% (25 issued in 2017-18, compared to 57 in 2016-17), and the number of time extension requests has dropped from 253 to 228. Although the total number of requests to my office to review public body responses to access requests has increased, this may be because more files are being processed by public bodies in a timelier way. I hope this is the case, and I also hope to see these trends continue.

Looking back on 2017-18, though, I think it was a watershed year for another reason as well: it seems privacy issues may once again be coming to the fore in Alberta, as these issues also garner more attention around the world.

At the close of 2017-18, the European Union's *General Data Protection Regulation* (GDPR) was just weeks away from coming into force, and it felt as if the world spent much of the entire year gearing up for the new legislation. Although it will be many years before GDPR's full impacts are realized, there can be no doubt that it has upped the threshold for strong, rigorous data protection. It seems clear that GDPR will lead to (or force) changes to privacy laws in many jurisdictions around the world.

The need for privacy law reform is obvious, as was clearly demonstrated in 2017-18 and continuing into 2018-19, by the almost daily revelations about companies such as Facebook and Cambridge Analytica, as well as myriad data breaches reported in all sectors. Despite week after week of front page media coverage of privacy stories it feels as if we have only just started to raise the curtain on many of the underlying issues. As we move increasingly towards global, national and provincial information economies, the vast amount of personal information collected and generated from and about citizens – by businesses, governments and health care entities – coupled with mind-boggling technology, has led to an ever increasing demand for transparency and effective oversight.

There is an appreciation and optimism for the potential of these new technologies themselves, but at what cost? And how do we reap the benefits without exposing ourselves, perhaps irreparably, to potential harms that range from the manipulation and compromise of democratic processes, to data breaches that could affect virtually everyone in the world?

Both the deliberate, malicious use of personal information and the potential for data breaches were front and centre for my office in 2017-18. We saw a 43% increase in the number of breaches reported under Alberta's private sector privacy legislation, many of which involved social engineering and phishing schemes, or hacked ecommerce websites. Across all sectors, we saw over 400 breaches reported. This number is expected to increase dramatically in 2018-19 as Alberta's health sector adjusts to mandatory breach reporting requirements that came into effect August 31, 2018.

The increase in self-reported breaches is just one of the great many challenges my office finds itself responding to. We opened a record 2,467 new cases in 2017-18. Along with self-reported breaches, much of the increase in volume was made up by privacy impact assessments – 771 in 2017-18, an increase of 32% from the previous year.

As an office, we continue to try to streamline our processes, improve efficiency, and resolve matters in a timely way. For example, in fall 2017, we undertook a review of our adjudication processes, and in spring 2018, we took a deep look at the processes at the intersection of Intake and Case Review, Mediation and Investigation, and Compliance and Special Investigations. A number of opportunities were identified and we are prioritizing and putting in place short, medium and long-term plans. In addition, we determined a need to dedicate staff to special projects and investigations, in an effort to report in a timelier way on matters of public interest and broad systemic issues, and to provide proactive guidance to regulated stakeholders and citizens.

Despite these efforts, it is no longer possible to manage the volume of incoming files with my office's current resources, which remain at essentially the same number of FTEs as in 2013-14. As a result, I will be requesting an increase in funding for 2019-20 to address these challenges and ensure Albertans have effective and timely independent oversight of access and privacy matters.

As always, I would like to offer my sincere thanks to my colleagues for their commitment to our legislated mandate, which they fulfill, year after year, with dedication and good humour.

Jill Clayton
Information and Privacy Commissioner

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 1,108 public bodies, including provincial government departments and 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 more than 54,900 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.

The Act 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 Alberta's provincial electronic health record system (i.e. 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.

The Act seeks to balance the right of the individual to have his or her personal information protected with the need of organizations to collect, use or disclose personal information for reasonable purposes. PIPA also gives individuals the right to access their own personal information held by organizations and to request corrections. 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 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
- Educating the public about the Acts, their rights under the Acts and access and privacy issues in general
- Receiving comments from the public concerning the administration of the Acts
- Giving advice and recommendations of general application respecting the rights or obligations of stakeholders under the Acts
- Engaging in or commissioning research into any matter affecting the achievement of the purposes of the Acts
- Commenting on the implications for access to information or for protection of personal privacy of proposed legislative schemes and existing or proposed programs
- Commenting on the access and privacy implications of privacy impact assessments submitted to the Commissioner
- 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

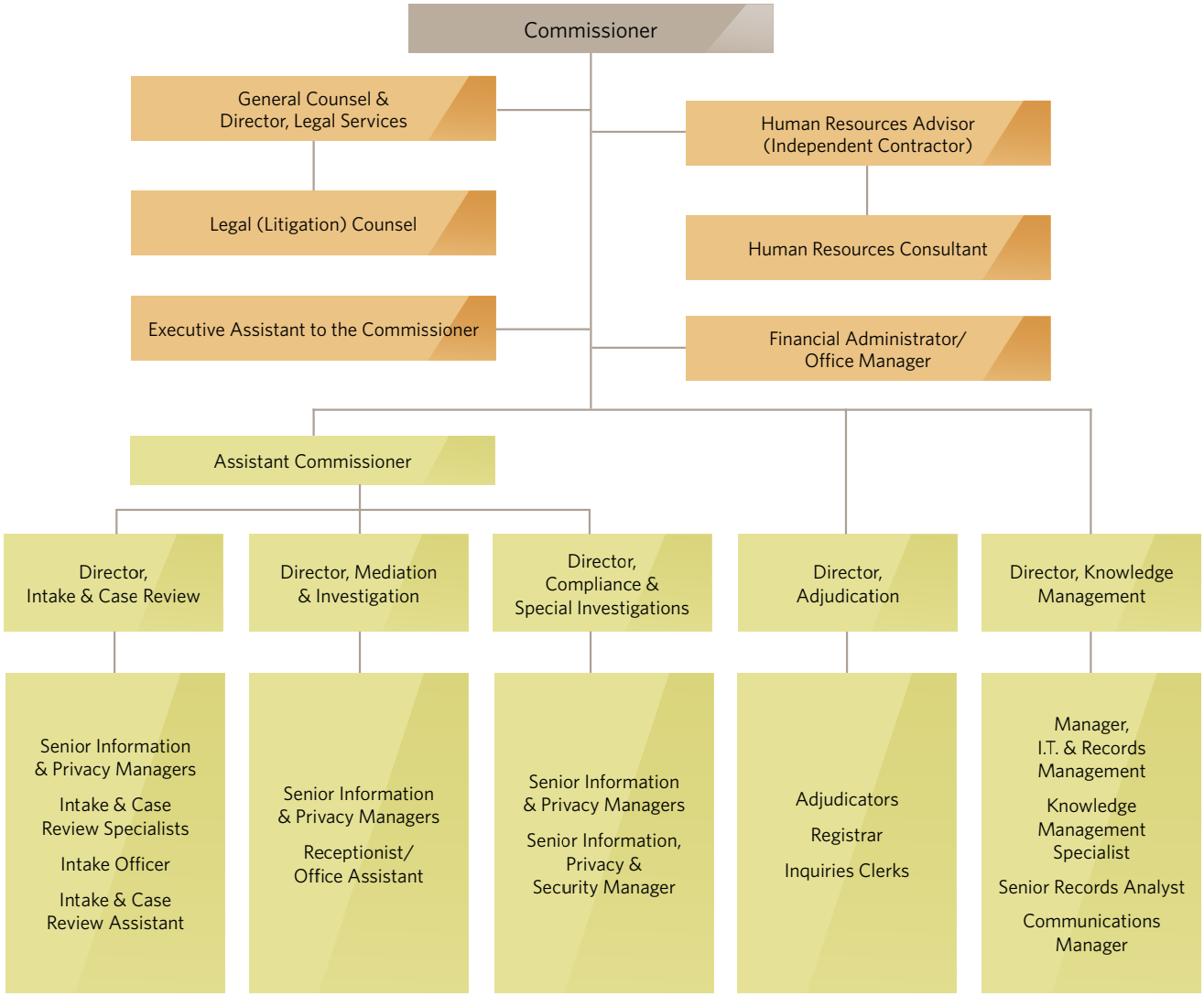
A society that values and respects access to information and personal privacy.

MISSION

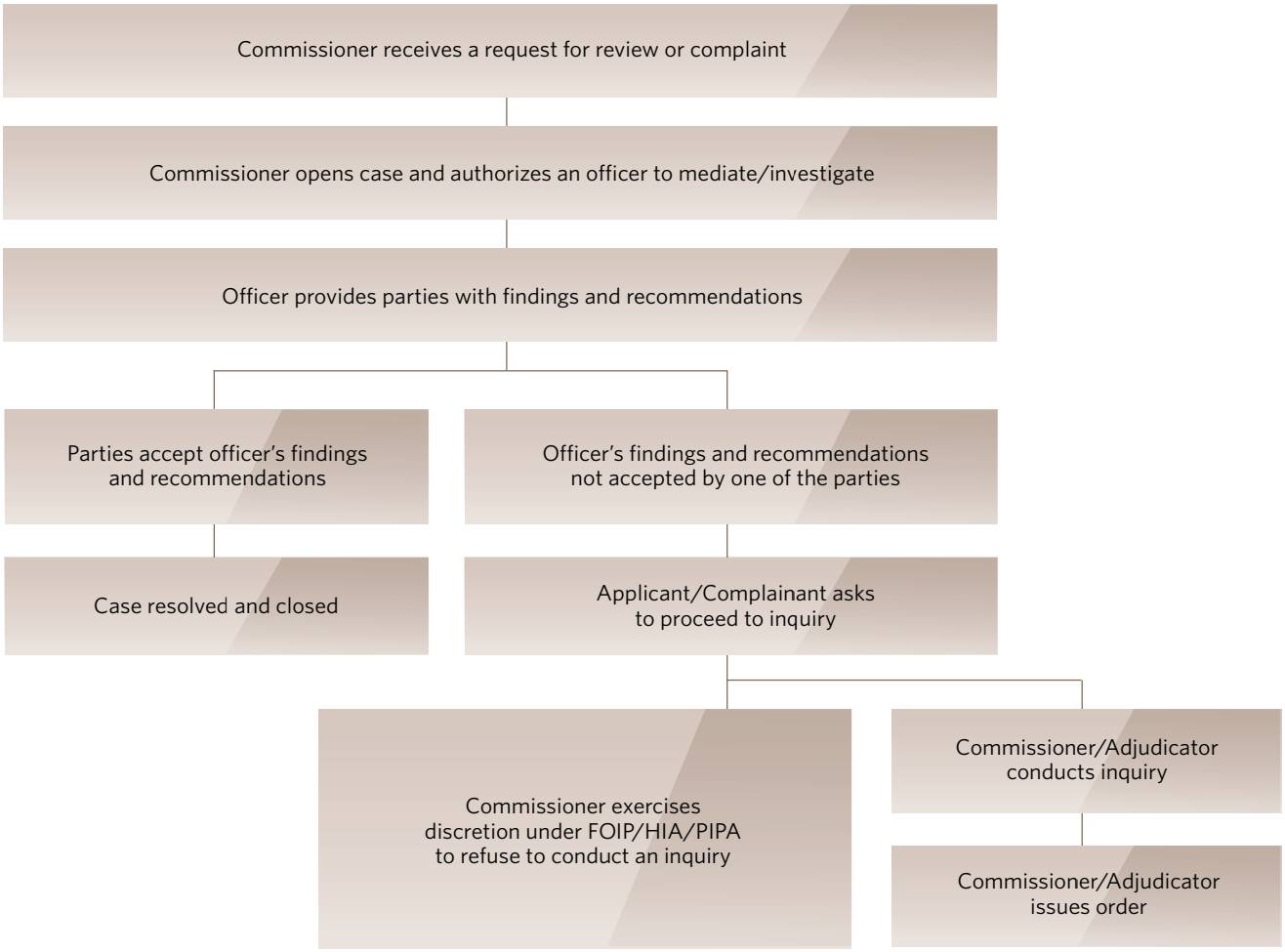
Our work toward supporting our vision includes:

- 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

OIPC Organizational Structure 2017-18



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 2017-18, the OIPC received eight general information requests under the FOIP Act, and seven informal requests for information. The OIPC responded to all of the requests within 30 days.

There are two outstanding requests for review related to access requests made to the OIPC. Both matters are awaiting appointments of an External Adjudicator by Order-in-Council to determine whether the OIPC properly excluded records subject to an access request after the applicants requested reviews of the OIPC's decisions.

One request for review of an OIPC decision was resolved by Adjudication Order No. 11 on April 27, 2017. The External Adjudicator determined that the OIPC had properly excluded records requested by the applicant as the records related to the statutory functions of the Commissioner under the FOIP Act. The Act excludes a record that is created by or for or is in the custody or under the control of an Officer of the Legislature and relates to the exercise of that Officer's functions under an Act of Alberta (section 4(1)(d)). The order is available at www.oipc.ab.ca.

OIPC PRIVACY MATTERS

In 2017-18, the OIPC conducted three investigations into internal incidents involving potential privacy breaches.

Incident 1

The office was advised that it sent correspondence to a law firm that had initially been identified as the registered office for an organization who was a party to a complaint, but was no longer the registered office for the organization.

OIPC policy requires employees to ensure contact information is kept current and accurate. When written authorization is received from an individual or organization to request a change to contact information, paper records and the electronic case management system should be updated, according to policy.

In this incident, the office was advised that the law firm was no longer the registered office for the organization. The OIPC's electronic case management system was not updated and therefore incorrectly continued to have the law firm's address as the registered office for the organization. The address placed on the correspondence was used from the electronic case management system without recognizing that it was outdated.

The OIPC immediately requested that the correspondence be returned when it was discovered that the information was mistakenly sent to the incorrect address. The correspondence was subsequently returned to our office, but not before it had been opened.

The affected individual was notified about this incident. The OIPC also reviewed its "Account and Contact Records

Policy", and took steps to clarify the policy and ensure staff are aware of it in an effort to reasonably prevent a similar incident from occurring.

Incident 2

The office was advised that a privacy complaint letter had been sent to the former owner of an organization, rather than to the current owner for whom it was intended.

When the complaint was made to the OIPC, the organization's name and address were provided on the complaint form. A file was opened under the organization's name based on the information provided.

A CORES (i.e. Corporate Registry System) search was also conducted, and the closest match belonged to a numbered company. The office sent correspondence to the "Registered Office" from CORES, as opposed to the address provided by the complainant.

When the former owner of the organization received the correspondence he personally notified the current owner and delivered the complaint letter to her. The current owner explained that she had purchased the organization from the former owner through a numbered company. The current owner has more than one numbered company and also clarified which company was the correct party to the complaint.

The personal information involved in this incident could not reasonably be used to cause harm. The personal information received by the former owner was provided to the current owner of the organization who was a party to the complaint. No notification was necessary.

Incident 3

The office was notified that a first contact letter intended for a public body was sent to the FOIP Coordinator for another public body. The incident was caused by mistakenly placing the correspondence for the public body into an envelope that had been prepared for another public body.

The public body who received the correspondence in error immediately alerted the OIPC, and at the office's request confirmed that the letter had been shredded.

The correspondence was received by a FOIP Coordinator, and steps were immediately taken to contain the breach by reasonably ensuring that the correspondence was securely destroyed. There is no reason to believe the information was further used or disclosed, and there was no real risk of harm. No notification was necessary.

PROACTIVE TRAVEL AND EXPENSES DISCLOSURE

The OIPC publicly discloses the vehicle, travel and hosting expenses of the Commissioner and the travel and hosting expenses of the Assistant Commissioner and Directors on a bi-monthly basis.

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 2016 calendar year, the threshold was adjusted to $126,375. 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

No disclosures under the *Public Interest Disclosure Act* were received by the OIPC's designated officer in 2017-18.

Financial Overview

For the 2017-18 fiscal year, the total approved budget for the OIPC was $6,873,291. The total cost of operating expenses and capital purchases was $6.7 million. The OIPC returned $184,856 (2.69% of the total approved budget) to the Legislative Assembly.

TOTAL ACTUAL COSTS COMPARED TO BUDGET

	VOTED BUDGET	ACTUAL	DIFFERENCE
Operating Expenses*	$ 6,873,291	$ 6,668,403	$ 204,888
Capital Purchases	-	20,032	-20,032
Total	$ 6,873,291	$ 6,688,435	$ 184,856

*Amortization is not included

Salaries, wages, and employee benefits make up approximately 80% of the OIPC's operating expenses budget. In 2017-18, payroll related costs were $427,469 under budget. Legal fees were under budget $155,714. External adjudication for three inquiries were over budget $137,623 due to additional records provided for review. Other contract services were over budget $240,587. Capital purchases were $20,032 over budget due to purchasing new exchange and active directory hardware.

TOTAL ACTUAL COSTS COMPARED TO PRIOR YEAR

	2017-2018	2016-2017	DIFFERENCE
Operating Expenses	$ 6,668,403	$ 6,644,235	$ 24,165
Capital Purchases	20,032	72,111	-52,079
Total	$ 6,688,435	$ 6,716,346	$ -27,911

Total costs for operating expenses and capital purchases decreased by $27,911 from the prior year. The reduction was primarily due to a decrease in salaries, wages, and employee benefits of $369,412 as well as decreases in legal fees of $35,760 and in capital expenditures of $52,079. These decreases were offset by an increase in materials, supplies and technology services of $71,017, external adjudication of $95,529 as well as an increase of $262,794 for other contract services incurred primarily for internal business process review, records and email management, and administrative assistance, as well as a cloud services privacy impact assessment, general population survey and commissioned research.

TRENDS & ISSUES

Political Parties

In early 2018, how political parties handle the personal information of citizens captured public attention after it came to light that certain political parties had used the services of Cambridge Analytica and AggregateIQ, data analytics firms at the centre of a controversy over the use of personal information obtained from Facebook.

The revelations in March 2018 that Cambridge Analytica had acquired information from 87 million Facebook users allegedly without consent raised awareness about how most political parties in Canada, including in Alberta, are not covered by access and privacy laws.

What followed were a series of investigations by privacy protection authorities in several countries, parliamentary and house legislative committees were formed, Facebook, Cambridge Analytica and AggregateIQ executives were summoned by lawmakers, and myriad questions were asked about whether voters were being manipulated by the alleged illegitimate disclosure of their personal information from private sector companies to political parties for voter research purposes.

In Canada, only political parties in British Columbia are covered by access and privacy laws. B.C.'s *Personal Information Protection Act* applies to political parties.

In Alberta, the OIPC has received several privacy complaints from Albertans about how political parties have handled their personal information. In each of the cases, the OIPC has had to inform individuals that the office does not have jurisdiction to investigate their concerns.

Similarly, federal political parties are not covered by the federal *Privacy Act* or the *Personal Information and Protection of Electronic Documents Act*.

Soon after the news broke about data sharing between Cambridge Analytica and Facebook, the House of Commons' Standing Committee on Access to Information, Privacy and Ethics committed to studying this matter and to make recommendations to government.[1]

[1] Recommendations were submitted to government in June 2018. The report can be found on the website of the Standing Committee on Access to Information, Privacy and Ethics at https://www.ourcommons.ca/Committees/en/ETHI.

GDPR and Private Sector Privacy Laws

As reported last year by the OIPC, the Standing Committee on Alberta's Economic Future completed its review of PIPA by making one recommendation to clarify the definition of a commercial activity.

Meantime, the European Union (EU) and indeed the global business community invested heavily in preparing for the EU's GDPR as it significantly changed the private sector privacy law landscape by placing several new requirements on organizations to bolster privacy, a fundamental human right for European citizens.

GDPR introduced several enhanced provisions around the themes of consent, accountability and breach reporting, and it introduced significant penalties for non-compliance.

The federal government began to respond to GDPR in February 2017. The Standing Committee on Access to Information, Privacy and Ethics (ETHI Committee) undertook a year-long study of the *Personal Information Protection and Electronic Documents Act* that resulted in a 95-page report to the Government of Canada titled *Towards Privacy by Design*.[2]

The ETHI Committee report had 19 recommendations. One of the recommendations was to consider "legislative amendments required to maintain adequacy status". Adequacy status of Canadian private sector privacy law with the EU currently allows for the transfer of European citizens' personal data to Canada. The committee noted that if maintaining adequacy was deemed not be in the Canadian interest then another mechanism to maintain the transfer of personal data between Canada and the EU would need to be considered (i.e. similar to the Privacy Shield pact between the United States and the EU in the absence of private sector privacy laws in the United States).

Relatedly, the Government of Canada determines whether provincial private sector privacy law is "substantially similar" to the federal law to allow for provincial governments to establish their own jurisdiction, such as in Alberta, B.C. and Quebec. As a result, the Government of Alberta will need to remain abreast of determinations on whether the federal law remains adequate with GDPR and by extension Alberta law remains substantially similar to federal law for the continued transfer of European citizens' personal information across Canada.

[2] The Government of Canada responded to the report in June 2018. The government's response to the report can be found on the website of the Standing Committee on Access to Information, Privacy and Ethics at https://www.ourcommons.ca/Committees/en/ETHI.

Artificial Intelligence and Machine Learning

Artificial intelligence and machine learning have permeated nearly every aspect of modern life.

Algorithms are used to determine what ads we are most likely to view online, what news story we are likely to read, what restaurant we want to visit or what movie we will watch. These technologies are also being used for driverless technologies, such as ploughing fields without human assistance and transportation at industrial sites, and are being tested on public roads. There are also the stranger applications, such as shoe recognition to track habits of people more likely to wear one type of shoe compared to another shade or style.

These programs require the collection of data to learn, and often require the collection of personal information, raising inherent privacy risks. Many observers voice concerns about what is being done behind the scenes, potential prejudicial impacts, and predicted job losses in the millions.

With all these considerations, the OIPC dedicated its Data Privacy Day event in January 2017 to learning more about artificial intelligence and machine learning – from theory to practice to assessment.

A stellar lineup of speakers from the University of Alberta, Google Canada and the Information Accountability Foundation, a thinktank dedicated to information management rights, spoke about what these concepts are, how they are being used in practice and what some of the limitations will be.

Additionally, these technologies raise ethical considerations – just because these technologies can be used in ways that were once reserved for science fiction, does it mean that they should be used in such ways? What are the ethical implications beyond privacy rights? How can we properly assess these implications?

Virtually every organization, including government departments, are exploring ways in which the information they gather can be harnessed to improve effectiveness in delivering services. Like every technology, deploying it over time becomes cheaper and new opportunities are discovered. There are countless benefits, plus many privacy risks that must be considered, analyzed and mitigated.

Genetic Testing

Described as "the year consumer DNA testing blew up", 2017 saw the number of DNA or genealogy tests sold more than double over 2016 to more than 12 million.[3] In comparison, only 330,000 tests were sold in 2013. Several factors have led to the increase in sales, including a sharp decrease in how much a test kit costs.

While most testing kits are sold to United States residents, more attention was paid to this trend in consumer behaviour in Canada. The *Genetic Non-Discrimination Act* was passed by the federal government and received royal assent on May 4, 2017. This law prohibits any person from requiring an individual to undergo a genetic test or to disclose the existing results of genetic tests. An individual may voluntarily provide written consent to disclose results to their employer or insurer, however.

This was an important law considering the privacy implications of these tests and potential for discrimination based on results. Access to an individual's test results by employers or insurance companies could conceivably limit their job prospects or insurance coverage.

In response to these developments, the OIPC partnered with the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for British Columbia in updating the "Direct-to-Consumer Genetic Testing and Privacy" policy statement and guidelines in December 2017.

The guidance is intended to help individuals make informed decisions before undertaking genetic or DNA tests.

The guidance addresses:

- Questions you may ask the company
- Personal questions you may ask yourself before signing up for a service
- What is direct-to-consumer genetic testing?
- What the potential privacy risks of direct-to-consumer genetic testing are

The guidance is available from www.oipc.ab.ca.

[3] Regalado, A. February 12, 2018. "2017 was the year consumer DNA testing blew up". MIT Technology Review. Retrieved from https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up/.

Blockchain

Blockchain is another technology that was very much on the radar in 2017-18. It seems every privacy and security conference included a session devoted to the topic, and myriad articles appeared extolling the technology's potential to radically transform multiple businesses and industries, in large part by tackling privacy and security issues associated with more traditional cloud and internet technologies.

Despite its ubiquity in 2017-18, the technology has been implemented to various degrees for about 10 years, and is most commonly associated with cryptocurrencies, in particular bitcoin; however, there are many variations. Typical features of the technology are that it consists of a distributed ledger in which data is stored in "blocks" that are linked to each other through cryptography. No single entity owns or controls the chain; instead, a network of participating computers contributes to and secures the system. Blockchains can be either public or private, and are permanent in that previous transactions cannot be altered, only new transactions can be added.

The various applications of blockchain are starting to become manifest in a number of real-world examples that go beyond cryptocurrencies:

- In September 2017, Reuters reported that "Royal Bank of Canada is experimenting with blockchain to help move payments between its U.S. and Canadian banks."[4]
- Researchers in California are using blockchain technology to allow people to share their medical data while retaining control over it.[5]
- West Virginians living overseas can now use a blockchain-enabled mobile voting app to cast absentee ballots.[6]

In support of such uses, the technology is touted as having the potential to: improve data security as a result of being distributed, decentralized and immutable; increase individual control of personal information by, for example, facilitating patient access to their own health information stored on a blockchain; and even potentially enhance compliance with GDPR.[7]

Nonetheless, there are challenges. Among them, the technology is not immune to hackers[8], details of transactions can usually be seen by anyone (although solutions to this problem are being worked on), and there are issues of scalability, in that the technology requires massive investments of infrastructure and resources.

Despite all of the above, it is clear that it will be important to watch this technology over the next few years.

[4] Scuffman, M. September 27, 2017. "Exclusive: Royal Bank of Canada using blockchain for U.S./Canada payments – executive". *Reuters.* Retrieved from https://www.reuters.com/article/us-rbc-blockchain/exclusive-royal-bank-of-canada-using-blockchain-for-u-s-canada-payments-executive-idUSKCN1C237N.

[5] Maxmen, A. March 9, 2018. "AI researchers embrace Bitcoin technology to share medical data". Nature. Retrieved from https://www.nature.com/articles/d41586-018-02641-7.

[6] Mak, A. September 25, 2018. "West Virginia Introduces Blockchain Voting App for Midterm Election". SLATE. Retrieved from https://slate.com/technology/2018/09/west-virginia-blockchain-voting-app-midterm-elections.html.

[7] Hussain, R. June 18, 2018. "Can Blockchain Really Address Data Privacy Concerns?" EContent. Retrieved from http://www.econtentmag.com/Articles/News/News-Feature/Can-Blockchain-Really-Address-Data-Privacy-Concerns-125624.htm.

[8] Khan, S. January 24, 2018. "Hacking and theft: the dark side of Blockchain". Pitmans Law. Retrieved from https://www.pitmans.com/insights/news/hacking-and-theft-the-dark-side-of-blockchain/.

BY THE NUMBERS

Totals Opened/Closed

72%

INCREASE OF OPENED FILES OVER FIVE YEARS

2,467 opened files in 2017-18
1,436 in 2013-14

98%

INCREASE OF CLOSED FILES OVER FIVE YEARS

2,293 closed files in 2017-18
1,159 in 2013-14

Privacy Impact Assessments under HIA

771

PRIVACY IMPACT ASSESSMENTS OPENED

32% increase over 2016-17 (583)

672

PRIVACY IMPACT ASSESSMENTS ACCEPTED

23% increase over 2016-17 (548)

Requests for Review under FOIP, HIA and PIPA

572

REQUESTS FOR REVIEW OPENED

6% increase over 2016-17 (538)

474

REQUESTS FOR REVIEW CLOSED

7% increase over 2016-17 (442)

Requests for Time Extensions under FOIP

228

10% decrease from 2016-17 (253)

Breach Reports Opened under PIPA

231

43% increase over 2016-17 (162)

Complaints under FOIP, HIA and PIPA

271

COMPLAINTS OPENED

16% decrease from 2016-17 (321)

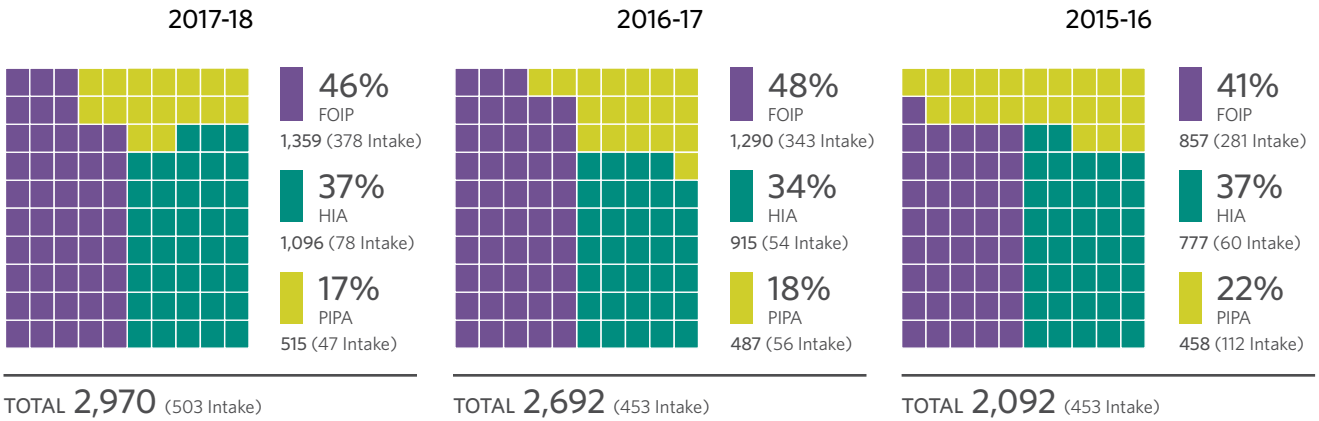
267

COMPLAINTS CLOSED

12% increase from 2016-17 (238)

GRAPH A: TOTAL CASES OPENED

Three Year Comparison



GRAPH B: TOTAL CASES CLOSED

Three Year Comparison

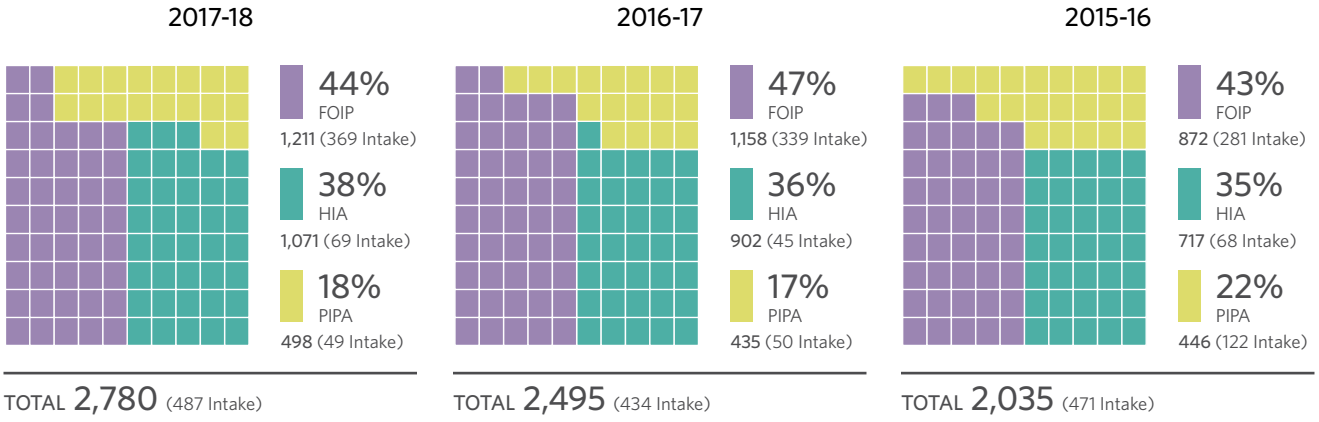


TABLE 1: CASES OPENED BY CASE TYPE

FOIP	2017-2018	2016-2017	2015-2016
Advice and Direction	1	2	0
Authorization to Disregard a Request	21	10	3
Complaint	96	92	78
Disclosure to Commissioner (Whistleblower)	0	0	0
Engage in or Commission a Study	1	0	0
Excuse Fees	9	10	10
Investigation Generated by Commissioner	10	27	13
Notification to OIPC	3	3	7
Offence Investigation	3	1	0
Privacy Impact Assessment	18	23	22
Request Authorization to Indirectly Collect	0	1	0
Request for Information	22	23	14
Request for Review	454	430	255
Request for Review 3rd Party	65	22	35
Request Time Extension	228	253	101
Self-reported Breach	50	50	38
Subtotal	**981**	**947**	**576**
Intake cases	378	343	281
Total	**1,359**	**1,290**	**857**

HIA	2017-2018	2016-2017	2015-2016
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	0	1
Complaint	56	70	72
Engage in or Commission a Study	0	0	0
Excuse Fees	0	1	0
Investigation Generated by Commissioner	1	2	28
Notification to OIPC	0	0	0
Offence Investigation	3	7	1
Privacy Impact Assessment	771	583	427
Request for Information	23	37	33
Request for Review	31	30	26
Request Time Extension	0	1	0
Self-reported Breach	133	130	129
Subtotal	**1,018**	**861**	**717**
Intake cases	78	54	60
Total	**1,096**	**915**	**777**

PIPA	2017-2018	2016-2017	2015-2016
Advice and Direction	0	0	0
Authorization to Disregard a Request	5	2	2
Complaint	119	159	129
Engage in or Commission a Study	0	0	0
Excuse Fees	0	0	0
Investigation Generated by Commissioner	6	6	5
Notification to OIPC	0	0	0
Offence Investigation	0	2	1
Privacy Impact Assessment	3	5	3
Request for Advance Ruling	1	0	0
Request for Information	16	17	8
Request for Review	87	78	54
Request Time Extension	0	0	0
Self-reported Breach	231	162	144
Subtotal	**468**	**431**	**346**
Intake cases	47	56	112
Total	**515**	**487**	**458**

Notes

(1) See Appendix A for a complete listing of cases opened in 2017-18.

(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.

TABLE 2: CASES CLOSED BY CASE TYPE

FOIP	2017-2018	2016-2017	2015-2016
Advice and Direction	1	2	0
Authorization to Disregard a Request	7	4	4
Complaint	83	69	76
Disclosure to Commissioner (Whistleblower)	1	0	0
Engage in or Commission a Study	1	0	0
Excuse Fees	8	8	6
Investigation Generated by Commissioner	19	15	4
Notification to OIPC	3	3	7
Offence Investigation	0	0	0
Privacy Impact Assessment	17	24	18
Request Authorization to Indirectly Collect	0	1	0
Request for Information	18	21	12
Request for Review	372	352	292
Request for Review 3rd Party	37	23	31
Request Time Extension	225	251	93
Self-reported Breach	50	46	48
Subtotal	**842**	**819**	**591**
Intake cases	369	339	281
Total	**1,211**	**1,158**	**872**

HIA	2017-2018	2016-2017	2015-2016
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	0	1
Complaint	58	48	39
Engage in or Commission a Study	0	0	0
Excuse Fees	1	0	1
Investigation Generated by Commissioner	16	25	16
Notification to OIPC	0	0	0
Offence Investigation	4	1	1
Privacy Impact Assessment	707	576	415
Request for Information	26	37	33
Request for Review	48	23	31
Request Time Extension	0	1	0
Self-reported Breach	142	146	112
Subtotal	**1,002**	**857**	**649**
Intake cases	69	45	68
Total	**1,071**	**902**	**717**

PIPA	2017-2018	2016-2017	2015-2016
Advice and Direction	0	0	0
Authorization to Disregard a Request	2	3	0
Complaint	126	121	111
Engage in or Commission a Study	0	0	0
Excuse Fees	0	0	0
Investigation Generated by Commissioner	3	9	6
Notification to OIPC	0	0	0
Offence Investigation	2	1	0
Privacy Impact Assessment	4	4	4
Request for Advance Ruling	1	0	0
Request for Information	15	16	8
Request for Review	54	67	70
Request Time Extension	0	0	0
Self-reported Breach	242	164	125
Subtotal	**449**	**385**	**324**
Intake cases	49	50	122
Total	**498**	**435**	**446**

Notes

(1) See Appendix B for a listing of cases closed in 2017-18.

(2) A listing of all privacy impact assessments accepted in 2016-17 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.

TABLE 3: PERCENTAGE OF CASES CLOSED BY RESOLUTION METHOD

Under the Acts only certain case types can proceed to Inquiry if the matters are not resolved at Mediation/Investigation. The statistics below are 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	%
Resolved by Mediation/Investigation	391	78	153	622	79%
Resolved by Order or Decision	70	25	8	103	13%
Resolved by Commissioner's Decision to Refuse to Conduct an Inquiry	15	4	9	28	4%
Withdrawn during Inquiry Process	14	0	8	22	3%
Discontinued during Inquiry Process	10	0	2	12	1%
Total	500	107	180	787	100%

FOIP Orders: 62 (68 cases); **FOIP Decisions:** 2 (2 cases); **HIA Orders:** 1 (25 cases); **PIPA Orders:** 8 (8 cases)

NOTES:

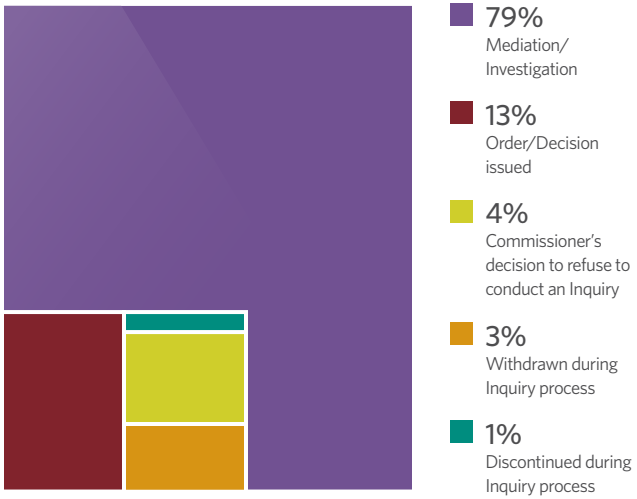
(1) This table includes only the Orders and Decisions issued that concluded/closed the case file. See Appendix C for a list of all Orders, Decisions and public Investigation Reports issued in 2017-18. Copies of Orders, Decisions and public Investigation Reports are available at www.oipc.ab.ca.

(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. Investigation Reports are recorded by the date the Investigation Report was publicly issued.

(3) Nine FOIP case files were closed by three Orders.

(4) 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 **787** cases that could proceed to Inquiry:
12% were resolved within 90 days
27% were resolved within 91-180 days
61% were resolved in more than 180 days

TABLE 4: GENERAL ENQUIRIES

TELEPHONE CALLS		
FOIP	Number	Percentage
Public Bodies	116	19%
Individuals	481	81%
Total	597	100%

HIA	Number	Percentage
Custodians	307	37%
Individuals	517	63%
Total	824	100%

PIPA	Number	Percentage
Organizations	242	25%
Individuals	724	75%
Total	966	100%

EMAILS FOIP/HIA/PIPA	232
NON-JURISDICTIONAL	158
Overall Total	2,777

REGULATION & ENFORCEMENT

Producing Records to the Commissioner: Special Report to the Legislative Assembly

Two developments compromising the ability of the Commissioner to perform functions under the *Freedom of Information and Protection of Privacy Act* (FOIP Act) led to a special report that was submitted to the Legislative Assembly in April 2017.[9]

First, the Supreme Court of Canada in *Alberta (Information and Privacy Commissioner) v. University of Calgary*[10] (U of C case) said that the legislature did not use the right words in the FOIP Act[11] to allow the Commissioner to require public bodies to provide records to the Commissioner over which public bodies are claiming solicitor-client privilege.

Second, public bodies have not been giving the Commissioner records when the records are needed as evidence for decisions the Commissioner is required to make under the FOIP Act. During the time that the U of C case was making its way through the court system, many public bodies, especially government, refused to provide the Commissioner with records over which solicitor-client privilege and other similar privileges were being claimed.

After the Supreme Court of Canada issued its decision in November 2016, the Commissioner issued a public statement indicating that a letter would be written to government with options for proceeding on this matter. However, the Commissioner is an independent Officer of the Legislature who reports to the Legislative Assembly and not to government.

As the Commissioner's ability to perform core functions as an Officer of the Legislature had been compromised, the Commissioner decided instead to submit the special report to the Legislative Assembly.

In the report, the Commissioner requested that the FOIP Act be amended to explicitly state that the Commissioner has the power to require public bodies to produce records over which solicitor-client privilege and other similar privileges are claimed, when in the Commissioner's opinion it is necessary to review those records, such as when a public body does not provide enough evidence to satisfy the Commissioner that the records are privileged.

The Commissioner maintained that the legislature established the position of Information and Privacy Commissioner to provide for an accessible, affordable and timely process for reviewing access to information decisions made by public bodies. The alternative, the report said, is to transfer the power of the Commissioner to the courts and have the courts decide whether a public body properly applied solicitor-client privilege to records when responding to an access request. For a number of reasons, the Commissioner stated that this would not be feasible, including increasing the cost for the courts, public bodies, the OIPC and citizens, and having multiple decision makers in a single case, as well as multiple appeal routes, unduly complicating the process.

The Commissioner has not yet received a response from the Legislative Assembly to the report.

[9] A copy of the special report is available at https://www.oipc.ab.ca/media/804484/Report_Producing_Records_to_the_Commissioner_Apr2017.pdf.

[10] *Alberta (Information and Privacy Commissioner) v. University of Calgary,* [2016] 2 SCR 555, 2016 SCC 53 (CanLII), http://canlii.ca/t/gvskr.

[11] Related to "Powers of Commissioner in conducting investigations or inquiries", section 56(3) of the FOIP Act reads that the Commissioner may require any record "despite any other enactment or any privilege of the law of evidence".

Investigation Reports

Allegations of Delays and Possible Interference by the Government of Alberta in Responding to Access Requests

This investigation was initiated in the spring of 2014 after a number of media articles reported on the concerns of opposition parties and interest groups who alleged political interference in the processing of access requests they had made to Government of Alberta (GoA) departments.

When the investigation was opened, one of the goals for the Commissioner was to either quell concerns and reassure Albertans that there was no evidence of political interference in GoA responses to access requests or shine a light on government decisions and actions that were contrary to the aims of the FOIP Act. For a variety of reasons, this goal was not achieved.

The report identified a number of factors that contribute to delays, including a significant increase in the number of access requests, the complexity of requests and applicant expectations. Some of the findings were expected and similar to those outlined in two separate investigation reports on delays in responding to access requests at Alberta Justice and Solicitor General, Executive Council and Public Affairs Bureau released in February 2017.[12] However, the investigation faced a number of challenges that made it impossible to make meaningful and reliable findings with respect to other potential issues in the access request response process.

Among these challenges, nearly 800 pages of records provided by the GoA for review in the investigation were either fully or partially redacted, including 466 pages of records that were entirely blacked out. In addition, all witnesses for the investigation were represented by a lawyer from Alberta Justice and Solicitor General, who also represented the respondent ministries.

This type of representation whereby one lawyer represented both witnesses and the ministries was unprecedented in the history of the office's investigations. In addition to significantly delaying the investigation, the lawyer may have prevented witnesses from candidly sharing their experiences and assessments.

At the time, this was one of approximately 80-90 cases in the office affected by the Supreme Court of Canada's decision in *Alberta (Information and Privacy Commissioner) v. University of Calgary,* which said that the legislature did not use the right words in the FOIP Act[13] to allow the Commissioner to require public bodies to provide records to the Commissioner over which public bodies are claiming solicitor-client privilege.

> "All in all, I am deeply disappointed in how this matter has unfolded. What should have been a relatively straightforward investigation has concluded under a shadow that brings the very notion of independent oversight of the executive branch of government into question and has the potential to erode public confidence in an open and accountable government."
>
> *- Commissioner Jill Clayton, April 11, 2017*

[12] The OIPC's Investigation Reports F2017-IR-01 and F2017-IR-02 look at delays in the context of specific departments. The investigations provide findings and recommendations, some of which may be applicable to all GoA departments. Investigation Report F2017-IR-01 is available at www.oipc.ab.ca/media/788396/f2017-ir-01.pdf. Investigation Report F0217-IR-02 is available at www.oipc.ab.ca/media/788394/f2017-ir-02.pdf.

[13] See page 32.

In the interests of avoiding further delays in concluding this investigation, the Commissioner instructed the investigator to complete the report. Further, given that the original ministers involved no longer held positions, the qualified nature of the investigation's findings, the fact that the investigation made no recommendations and the series of challenges, the Commissioner chose to present the report directly to the Legislative Assembly, in conjunction with the special report to the Legislative Assembly on producing records to the Commissioner.

Multiple Alleged Unauthorized Accesses of Health Information at South Health Campus

On September 8, 2015, a patient was admitted to the South Health Campus emergency department in Calgary. The South Health Campus is a hospital operated by Alberta Health Services (AHS). The patient was flagged as a "confidential patient". Many staff members were aware of media reports concerning the patient and her daughter. The patient remained in the emergency department until September 11, 2015.

On September 10, 2015, the AHS Information and Privacy Office (AHS Privacy Office) was notified by a South Health Campus emergency department manager of a possible contravention of HIA involving a disclosure of the patient's health information. Due to the circumstances of the patient's admission to the emergency department, the AHS Privacy Office decided to complete a proactive audit of all accesses to the health information of the patient, and the patient's daughter, within the Sunrise Clinical Manager electronic medical records system (SCM EMR), and the provincial electronic health record (Netcare).

The audit identified 160 employees of the South Health Campus emergency department who accessed the health information of the patient, or both the patient and her daughter (the health information). The audit reports were distributed to emergency department managers for review to determine if these accesses were authorized. The review confirmed that the majority of the accesses were necessary to provide health services and were authorized; however, accesses made by 75 employees required further investigation.

An AHS investigation team was mobilized, including staff from the AHS Privacy Office, human resources and management. The team interviewed the 75 employees and determined that 49 of them accessed health information "outside their role" of providing a health service.

AHS disciplined the 49 employees who were found to have accessed the health information without authority; however, a majority of the employees filed grievances pursuant to their respective collective bargaining agreements. Following grievance resolution meetings with the employees and their union representatives, AHS rescinded discipline for 38 of the employees and reduced discipline for the remaining 11.

The alleged unauthorized accesses were reported to the OIPC on September 18, 2015. On October 15, 2015, the Commissioner opened this investigation.

The objectives of this investigation were to determine whether health information was accessed and used in accordance with HIA, to review safeguards and training, and determine whether sanctions for contravening safeguards were in place.

The investigation found that AHS contravened HIA when its affiliates accessed and used health information for purposes that were not authorized under the Act. AHS affiliates also contravened HIA when they accessed and used health information for purposes that were not in accordance with their duties to AHS.

The investigation determined that AHS has clear policies and training in place; however, policies were not properly implemented. While affiliates were required to read and observe the policies, AHS did not take reasonable steps to ensure the policies were known, understood, applied and monitored.

AHS also contravened the *Health Information Regulation* by failing to ensure that its affiliates were aware of and adhering to all of the custodian's administrative, technical and physical safeguards in respect of health information.

Finally, AHS properly established sanctions that may be imposed if an affiliate breaches or attempts to breach safeguards, as required by the *Health Information Regulation*.

There were six recommendations made to AHS. During the OIPC's investigation, AHS began a review of relevant policies and practices within the South Health Campus emergency department. Several activities were implemented or were in the process of being implemented in response to the incident that led to this investigation.

The investigation noted that this case highlighted a significant breach of privacy where the focus of the investigation shifted from the affiliates to the custodian. While the affiliates improperly accessed health information, the custodian had not met its duties to implement safeguards and ensure affiliates were aware of them. In addition, the custodian had not conducted periodic monitoring to ensure compliance.

> "This incident highlights the significant gap that existed between the requirements of the law and AHS policies, and the actual practices implemented in the South Health Campus emergency department. The HIA requires custodians to have safeguards, training and policies in place to protect patient privacy, but even the best efforts can be completely undermined without a commitment to implementation and monitoring, and communication to staff."
>
> *- Commissioner Jill Clayton, November 29, 2017* [15]

Alberta Gaming and Liquor Commission's Collection of Personal Information for Casino Advisor Background Checks

On August 10, 2015, the OIPC received a complaint from an individual about the extent of personal information required by the Alberta Gaming and Liquor Commission (AGLC) for that individual to continue acting as a Casino Advisor.

The matter was not resolved at mediation and the individual requested an inquiry; however, the individual had not provided AGLC with the requested personal information. Therefore, no personal information was at issue. Upon review of the matter, rather than focus on the particular circumstances of the individual's complaint, the Commissioner initiated an investigation to more broadly review AGLC's authority under Part 2 of the FOIP Act regarding its personal information practices for applications and renewals of Casino Advisor positions.

The Casino Advisor Application Forms under review in this investigation were similar to, but updated from, those at issue in Investigation Report F2002-IR-008.[14] AGLC explained there had been changes to the forms in question since the first time they were reviewed by the OIPC, and it provided details regarding the changes that had been made.

The application forms are lengthy and require a great deal of extremely detailed and sensitive personal information about an applicant as well as individuals closely associated

[14] Investigation Report F2002-IR-008 is available at www.oipc.ab.ca/media/127659/F2002-008IR.pdf.

[15] OIPC news release, "AHS Responsible for Unauthorized Accesses by 49 Employees", is available at https://www.oipc.ab.ca/news-and-events/news-releases/2017/ahs-responsible-for-unauthorized-accesses-by-49-employees.aspx.

with the applicant. An applicant must provide, among other things, a complete disclosure of their financial situation, employment history, family relationships, and criminal, litigation or disciplinary history. Depending on AGLC's initial review of the application forms, it may require some applicants to provide additional detailed personal information.

The investigation concluded that the legislature entrusted AGLC with governing the gaming industry in Alberta, which included determining which individuals may be registered as Casino Advisors. Sections 9 and 9.1 of the *Gaming and Liquor Regulation* gives AGLC broad authority to conduct background checks, which necessitates the collection of personal information from Casino Advisor applicants and individuals associated with them. As such, the investigation was satisfied that AGLC is collecting personal information in its Casino Advisor Application Forms in accordance with sections 33(a) and (c) of the FOIP Act, which address the purpose of collecting personal information.

Based on the considerable latitude with which public bodies are able to decide what personal information is necessary for them to collect, and in consideration of AGLC's submissions as well as the OIPC's previous investigation of substantially the same matter, the investigation found that AGLC was compliant with Part 2 of the FOIP Act regarding the personal information collected for Casino Advisor positions in its Casino Advisor Application Forms.

Investigation Concerning Health Custodians and Information Managers

On August 17, 2015, a physician reported to the OIPC that a consultation letter he prepared concerning one of his patients was inadvertently made accessible over the internet as a result of actions taken by an outside company he hired to provide transcription services (service provider).

The service provider had previously reported the same incident to the OIPC on July 28, 2015.

On October 27, 2015, the patient affected by this incident complained to the OIPC about the lack of information provided to her by the service provider regarding the cause of the incident, and the length of time her health information was exposed on the internet.

This investigation highlighted three important issues with respect to the roles and responsibilities of custodians and information managers under HIA.

First, when custodians do not sign agreements with their information managers, they may find themselves unable to exercise control over health information they are responsible for. Custodians remain accountable for health information they collect and use, and for the actions of any information manager to whom they may subsequently disclose health information. In this instance, a properly executed information manager agreement would have allowed the physician to specify whether the information manager, upon receiving the health information for the purpose of performing a service to the physician, was allowed to further disclose the health information.

Second, since there was no information manager agreement in place, the physician was unable to properly consider all applicable legal requirements. In a situation where health information is stored or used outside Alberta, the *Health Information Regulation* requires that custodians consider additional safeguards to ensure the confidentiality of health information.

Third, when custodians notify individuals whose health information was accessed, used or disclosed in contravention of HIA, it is important they communicate with those patients openly, accurately and completely. In this case, the physician decided to voluntarily notify the complainant both in writing and by calling her. He provided her with information about the cause of the incident, the extent of the health information at issue and the actions he took to address the issue. The steps taken by the physician reflect the recommendations found in OIPC publications with regard to responding to and reporting

privacy breaches. However, the complainant took issue with the lack of information received from the service provider. It would have been helpful to all parties involved if the physician and the service provider had coordinated their efforts in notifying the complainant and addressing her subsequent questions.

The investigation recommended that the physician sign an agreement with the service provider, as well as with any other person or body providing services to him that is an information manager as defined under HIA. The physician accepted this recommendation and established an information manager agreement with the service provider.

Police Street Checks Public Consultation

In the fall of 2017, Alberta Justice and Solicitor General undertook a public consultation on the practice of police street checks in response to concerns raised by community groups and members of the public that street checks disproportionately affect certain minority populations. Media coverage of the practice also focused on its impacts on privacy rights.

In response to the public consultation, the Commissioner wrote a letter outlining the relevant access and privacy questions that should be answered to bring transparency to the practice of police street checks and to ensure that police services are complying with the FOIP Act.

It was the OIPC's understanding that the feedback received during the public consultation would provide the information needed to help develop provincial guidelines for the practice of police street checks. The Commissioner raised 12 questions on access and privacy issues that the guidelines should address.

As of March 31, 2018, provincial guidelines on the practice of police street checks had not been developed by Alberta Justice and Solicitor General.

The letter the Commissioner submitted for the public consultation is available at www.oipc.ab.ca.

Deemed Refusals to Respond to Access Requests

The OIPC streamlines 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 or PIPA, respectively. These types of requests for review are described as "deemed refusals".

Typically, the only issue at inquiry is that the public body, health custodian or organization has not responded within the time limit under the Acts, and the Adjudicator orders the public body, health custodian or organization to respond to the applicant and meet its remaining duties under the Acts in responding to the applicant.

Of the 25 deemed refusal orders in 2017-18, 22 were issued to government public bodies. Two deemed refusal orders were issued to municipal police services under the FOIP Act and one to an organization under PIPA. In the order related to an organization, an applicant had not received responses to three access requests. All three access requests were addressed in one order.

In six deemed refusal orders in 2017-18, the Adjudicator acknowledged that the public body or organization responded during the inquiry process. As such, no order to respond to the applicant was made.

The 25 deemed refusal orders in 2017-18 was a 56% reduction compared to 2016-17, during which 57 deemed refusal orders were issued.

The streamlined deemed refusals process was in effect for its first full fiscal year in 2016-17. The process was established in 2015-16 after an influx of requests for review in which the only issue was that the applicant had not received a response to an access request.

LIST OF DEEMED REFUSAL ORDERS IN 2017-18

Alberta Justice and Solicitor General

1. ..... F2017-78
2. ..... F2017-59
3. ..... F2017-56
4. ..... F2017-50
5. ..... F2017-46
6. ..... F2017-42

Executive Council

7. ..... F2017-76
8. ..... F2017-75
9. ..... F2017-74
10. ..... F2017-72
11. ..... F2017-71

Alberta Treasury Board and Finance

12. ..... F2018-04
13. ..... F2018-03
14. ..... F2017-70
15. ..... F2017-69
16. ..... F2017-68
17. ..... F2017-41

Alberta Labour

18. ..... F2017-66
19. ..... F2017-52

Alberta Community and Social Services

20. ..... F2018-11

Alberta Health

21. ..... F2018-10

Alberta Environment and Parks

22. ..... F2017-64

Calgary Police Service

23. ..... F2018-02

Edmonton Police Service

24. ..... F2017-80

CO-OP Taxi

25. ..... P2017-09

Requests for Time Extensions by Public Bodies

There were 228 requests for time extensions under the FOIP Act received in 2017-18, representing a 10% decrease from 2016-17 (253).

Of the 228 time extension requests received in 2017-18:

- 64%, or 147, were made by provincial government departments
- 11%, or 24, were made by a regional health authority
- 7%, or 17, were made by post-secondary institutions
- 7%, or 16, were made by municipalities
- 4%, or nine, were made by law enforcement
- 4%, or nine, were made by boards and commissions
- 2%, or five, were made by other public bodies
- One was made by a school district

In addition, the following decisions were made on the time extension requests:

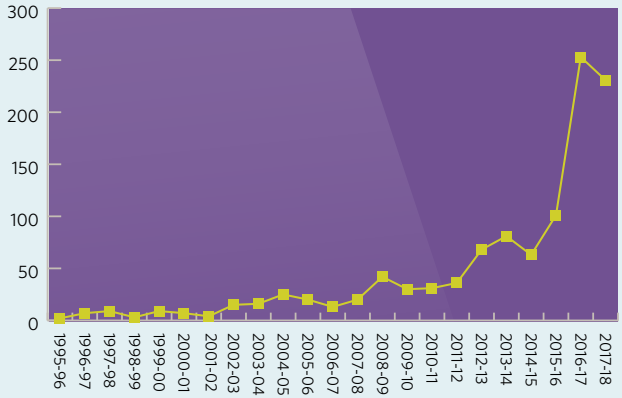
- 58% were granted
- 19% were partially granted (extension period permitted was less than what was requested by the public body)
- 16% were denied
- 7% were withdrawn by the public body

A public body must make every reasonable effort to respond to a request for access 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. 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 to be treated as a decision to refuse access under the FOIP Act (section 11(2)).

HISTORY OF TIME EXTENSION REQUESTS

The ability for public bodies to extend the time for responding to access requests has existed since the FOIP Act was enacted. However, only in the past few years have public bodies used these provisions with increasing regularity, and requested the Commissioner to extend the time limit for responding.



Mediation and Investigation

Hundreds of files were opened for mediation and investigation in 2017-18. These files include requests to review responses to access requests, and privacy complaints related to the alleged improper collection, use, disclosure or safeguarding of personal or health information, under all three Acts.

In total, 79%, or 622, of closed files that could proceed to adjudication were resolved by mediation and investigation.

There are certain common issues in the public, health and private sectors that result in similar requests for review or privacy complaints being submitted to the OIPC in any given year.

EMPLOYEE REQUESTS FOR PERSONAL INFORMATION

Over the past few years, terminated employees or employees with grievances often requested review of responses they received to access requests for personal information in their employee files. There have also been several requests for review concerning workplace investigations. These issues arise under both the FOIP Act and PIPA.

However, under PIPA specifically, there are some common challenges when organizations respond to these types of personal information requests.

Organizations are not always familiar with what is "personal information" under PIPA and often do not provide all of the applicant's personal information when responding to a request. Alternatively, organizations will provide records which are generally not considered personal information under PIPA, such as work product.

Another common issue is organizations failing to cite the relevant provision of PIPA on which they are relying to withhold certain information when responding to an access request. Organizations must provide this rationale, which can be as simple as noting the section number that supports the severing of information on the record so the applicant can see why the organization redacted that part of the record.

When receiving a request that may be overly broad or it is not clear what the employee is requesting, it is often to the organization's benefit to clarify the expectations of the requestor.

Before responding to access requests, organizations are encouraged to review OIPC orders to assist in determining what is and what is not personal information under PIPA, to properly cite sections for withholding information, and to decide how and when to clarify expectations of applicants.

MOBILE DEVICES AND EMPLOYEE SURVEILLANCE CONCERNS

The OIPC has been receiving more privacy complaints related to employer-provided mobile devices used for personal purposes and surveillance technologies used for purposes contrary to the organization's purpose for collection.

Clear policies for mobile devices supplied by employers are required to understand what is and what is not acceptable use for personal purposes. Employees are often provided devices for employment purposes. Personal information unrelated to the employment context is then put on the devices or in accounts to which the employer has access. These matters

cause confusion about who has custody or control of the personal information. If an employee chooses to put personal information on the employer's device, is the employer required to give it back in response to an access request? The answer is not clear in the absence of policies that are made known to the employee before or during access to a mobile device.

As surveillance technologies continue to permeate workplaces, often for the purpose of theft prevention or security, there has been an increase of workplace privacy complaints. These complaints typically centre on the purpose for the collection of recorded images not being consistent with the use of the personal information. For example, employees complain that surveillance cameras are being used to monitor work or attendance, despite the cameras being installed to prevent theft or maintain security.

PERSONAL INFORMATION PRACTICES IN DISABILITY CLAIMS

There has been a significant increase in complaints by employees about the amount and nature of information that is gathered for short- or long-term disability claims, workers' compensation claims, or return to work arrangements. The complexity and specificity of issues in these types of complaints has also increased.

Typically, complainants will first request and gain access to their personal information. Upon receipt of the information, the complainants will, for example, question why medical information was disclosed to certain third parties with respect to their disability claims or the parameters of their return to work arrangement. Similar complaints arise for the collection and use of personal information from or by third parties with respect to disability claims or return to work arrangements.

These complaints are understandably complex. The issues often require examination of other pieces of legislation, such as the *Workers' Compensation Act*, and how they interact with access and privacy laws. It also requires examining whether personal information can be collected, used or disclosed without the consent of the complainant. Human rights legislation may also interact with these claims in terms of the amount and nature of an individual's personal medical information shared between insurance providers and employers.

PERSONAL INFORMATION REQUESTS IN VIDEO RECORDINGS

Increasingly, there are access requests for personal information in all recorded formats, including video recordings.

The requests for video surveillance recordings range from condominium complexes or retail business security footage under PIPA to penitentiary footage of individuals who are incarcerated or traffic surveillance cameras in municipalities under the FOIP Act.

Severing other individuals' personal information from videos, which often capture public spaces, can be challenging. Often, the capability to sever images or protect the personal information of third parties captured on recordings can be expensive or the entity does not have those skills internally. Also, when responding to requests for a specified time period, the challenge to respond is exacerbated since entities must also abide by policies on retention and destruction.

With the increasing use of technology that captures and stores personal information in various mediums, this trend for requesting access will continue.

Privacy Breaches

PIPA

There was a sharp 43% increase in breaches reported under PIPA in 2017-18. Organizations reported 231 breaches compared to 162 in 2016-17. It was the fifth consecutive year of increases, and 2017-18 set the mark for the most breaches reported since mandatory breach reporting and notification requirements for the private sector came into force on May 1, 2010.

Self-Reported Breaches Opened Per Year under PIPA

Mandatory Breach Reporting and Notification Provisions Were Enacted January 1, 2010

2010-11: **49**
2011-12: **92**
2012-13: **84**
2013-14: **96**
2014-15: **138**
2015-16: **144**
2016-17: **162**
2017-18: **231**

The greatest number of breach notification decisions were also issued in 2017-18. There were 242 breach decisions, representing a 48% increase over 2016-17 (164). Of the 242 breach decisions rendered, the Commissioner made the following determinations:

- 165 were found to have a real risk of significant harm
- 66 were found to have no real risk of significant harm
- 11 where PIPA did not apply

It is mandatory for an organization with personal information under its control, to notify the Commissioner, 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" of personal information (section 34.1). Organizations are required to notify the Commissioner of reportable breaches without unreasonable delay (section 34.1).

Central Reservation System

A service provider for hotel and resort accommodations had its central reservation system accessed by an unauthorized party, permitting the intruder to gain access to personal information.

Each incident involved name and payment card information, and may have involved email address, contact information and other information associated with a hotel reservation.

More than 30,000 Alberta residents were affected in total.

Preferred Hotels & Resorts, P2018-ND-043
Four Seasons Hotels Limited, P2018-ND-028
Rosewood Hotel Group, P2018-ND-015
New World Management Limited, P2017-ND-158
Six Continents Hotels, Inc., P2017-ND-157
Owner's Association of Rivertide Suites, P2017-ND-155
Aimbridge Hospitality Holdings, P2017-ND-142
Hyatt Hotels Corporation, P2017-ND-141
Hartz Hotel Services, Inc., P2017-ND-123
Magellan Vacations, P2017-ND-108
Activision Blizzard, Inc., P2017-ND-107
Loews Hotels & Co., P2017-ND-105
Noble House Hotels and Resorts, P2017-ND-94

Phishing

Several organizations were subject to phishing scams.

In one case, an employee with the organization received an email that was purportedly a request for tax forms from the organization's president and CEO. Believing the email was legitimate, the employee replied to the message but it was sent to the unauthorized individual posing as the organization's president and CEO.

In a similar case, an email appearing to be from an executive with the organization was sent to an executive assistant requesting payment of a fraudulent invoice. The executive's email account was compromised in order to perpetrate the scam, potentially exposing personal information.

A third incident involved an unauthorized individual acting as an organization's executive. The employee who received the email, which appeared to be from the organization's CEO, forwarded information about employees in Excel format, as was requested by the attacker.

In another case, an employee opened a phishing email which led to malware being installed on the organization's system exposing clients' credit card information. Credit card brands notified the organization that fraudulent activity was detected.

Four employee email accounts were compromised by a phishing email from which a link was clicked. The compromised accounts automatically distributed additional phishing emails. From those additional phishing emails, another employee clicked on the link which led to four additional employee accounts being compromised.

A phishing email went undetected by an employee in another case and the employee's credentials were provided to the unauthorized individual. The attacker then accessed the individual's email account and placed an automatic email forwarding rule to the attacker's own mailbox leading to inadvertent disclosure of personal information.

In total, these incidents affected more than 1,100 Albertans.

Geokinetics Inc., P2017-ND-133
Best Western Plus Wine Country Hotel & Suites in West Kelowna, operated by 626498 Alberta Ltd., P2017-ND-130
Brion Energy Corporation, P2017-ND-110
The Empire Life Insurance Company, P2017-ND-100
Aecon Group Inc., P2017-ND-61
ISN Software Canada Ltd., P2017-ND-51

Rogue Employees' Disclosures to Unions

In one incident, an employee responsible for recruitment with authorized access to the organization's scheduling software database accessed and ran a number of human resource reports containing personal employee information without a legitimate business purpose.

Shortly thereafter, the organization received complaints from approximately five to 10 employees who claimed that individuals identifying themselves as union representatives had arrived at their homes and knew details of the information contained in the reports. Some of the complainants said they had received multiple telephone calls from union representatives. At the time, the workplace was not yet unionized.

The organization concluded that the employee disclosed the information to the union. The information in the reports had not been recovered. This incident affected 530 individuals.

In the second incident, an employee mistakenly saved an electronic spreadsheet to an internal server accessible to all employees of the organization. The spreadsheet contained name, social insurance number and salary information for the past five years.

The organization reported that at least two employees accessed the spreadsheet while it was available and shared it with other employees, including local union representatives. The organization later discovered that some employees printed or saved the spreadsheet and shared it with their union association.

CBI Home Health (AB) Limited Partnership, P2017-ND-97
FPInnovations, P2017-ND-79

User Credentials Acquired Illicitly

Customer loyalty programs were compromised in two incidents. In both cases, the organizations did not find that their systems had been compromised, but rather that user credentials had been acquired through illicit means online and used on the loyalty program websites the affected organizations operate.

The organizations believed that an unauthorized third party acquired usernames and passwords from the "dark web", which may have been linked to privacy breaches on other organizations' websites.

These incidents serve as a reminder to individuals to use different usernames and/or passwords on each website for which they have an account.

These two incidents affected nearly 20,000 Albertans.

Imperial Oil Limited, P2018-ND-019
Canadian Tire Corporation Limited, P2017-ND-165

Theft

Theft was the second most common cause of breaches involving a real risk of significant harm behind only external system compromises (e.g. malwear). Approximately 25 incidents resulted from stolen mobile devices or paper records from vehicles, couriers, or during break and enters. These breaches affected more than 4,000 Albertans.

These incidents serve as a reminder to employees that work devices or paper records be safely secured when out of the office, in particular the numerous incidents when information was stolen from vehicles.

HIA

There were 133 breaches reported voluntarily by health custodians to the OIPC in 2017-18.

While a significant portion of breaches reported by law under PIPA were from external system compromises, only five, or 4%, of breaches voluntarily reported by health custodians to the OIPC were external system compromises.

Rogue employees or snooping cases accounted for nine of the 133 self-reported breaches, or 7%.

Meanwhile, 34 breaches were caused by human error, as reported by health custodians.

In May 2014, amendments to the *Health Information Act* were passed under the *Statutes Amendments Act, 2014.* The amendments include requiring that health custodians:

- Notify an individual affected by a privacy breach when the custodian determines there is a risk of harm to the individual.
- Notify the Information and Privacy Commissioner of a privacy breach when there is a risk of harm to an individual.
- Notify the Minister of Health of a privacy breach when there is a risk of harm to an individual.

These amendments were not in force as of March 31, 2018.[16]

FOIP

A vast majority of the 50 privacy breaches voluntarily reported by public bodies to the OIPC were considered human error. There were 36 breaches reported as human error incidents by public bodies, or 72%.

Despite recommendations from the Commissioner, a public body is not required by law to notify the OIPC of a privacy breach; however, public bodies are encouraged to voluntarily report privacy breaches to the Commissioner as part of the public body's breach response process.

When the OIPC receives breach reports from public bodies, the OIPC:

- Analyzes the circumstances of the situation as reported by the public body.
- Makes recommendations to respond to the breach and prevent similar incidents.
- Encourages the public body to notify affected individuals based on risk assessment.

[16] Order-in-Council 120/2018, approved on May 8, 2018, set August 31, 2018 as the date for the mandatory breach reporting requirements to come into force. Order-in-Council 121/2018, approved on the same day, made changes to the *Health Information Regulation.*

Offence Investigations

HIA

In October 2017, a pharmacist pleaded guilty to knowingly accessing health information in contravention of HIA.

The investigation found that 104 individuals were affected by the unauthorized accesses. Health information, including demographic information, diagnostic images and laboratory results, was accessed despite no formal patient-pharmacist relationship with the affected individuals.

At sentencing, Justice Belzil of the Court of Queen's Bench of Alberta stated, "The Court in these types of offences is concerned with sending a message to not only (the pharmacist), but any others that patient information is very important and privacy rights are extremely important in a modern society."

There have been eight convictions under HIA since it was enacted in 2001. As of March 31, 2018, there is one other matter before the courts where an individual has been charged for allegedly accessing health information in contravention of HIA.

Convictions for Unauthorized Access of Health Information

- April 2007
- December 2011
- April 2014
- February 2016
- September 2016
- March 2017 (2)
- October 2017

Privacy Impact Assessment Reviews

PIA STATS

There were 689 privacy impact assessments (PIAs) accepted by the OIPC in 2017-18. Of the 689 accepted PIAs, 672, or 98%, were from custodians under HIA.

Custodians under HIA "must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy" of individuals and submit the PIAs to the OIPC for review and comment prior to implementation of the new practice or system (section 64).

Under the FOIP Act and PIPA, submitting PIAs to the OIPC is voluntary. The OIPC accepted 15 PIAs from public bodies under the FOIP Act, and accepted two PIAs from organizations under PIPA.

When PIAs are submitted to the OIPC, the office reviews the assessment and, once satisfied that a public body, custodian or organization has addressed the relevant privacy considerations, will "accept" the PIA which acknowledges that reasonable efforts to protect privacy have been made. A PIA cannot be used to obtain a waiver of or relaxation from legislated requirements for the collection, use and disclosure of personal or health information in a new or redesigned project or legislative scheme.

A listing of all PIAs accepted by the OIPC in 2017-18 is available at www.oipc.ab.ca.

HIA

In anticipation of gaining authorized access to Netcare by Alberta Health, dentists in the province[17] increased their submission of PIAs for Netcare access. There were 126 PIAs received from dentists in 2017-18, compared to only seven PIAs from dentists for Netcare access in 2016-17.

In November 2017, the OIPC accepted Alberta Health Services' Netcare Shared Health Information Communications Hub PIA. The program is meant to centralize the various processes required to exchange information between different systems for the delivery of:

- Patient health records to the appropriate Netcare clinical repositories from contributing custodians.
- Patient health records flagged by the subscription service to a private clinic or a physician's own electronic medical records (EMR) systems.
- Patient health records from AHS health information repositories to a private clinic or a physician's own EMR systems.
- Patient health records to multiple health information repositories from an originating health information repository.

PIAs Opened Annually Over 10 Years*

2008-09: **405**	2012-13: **420**	2016-17: **611**
2009-10: **714**	2013-14: **384**	2017-18: **792**
2010-11: **530**	2014-15: **356**	
2011-12: **457**	2015-16: **452**	

**Not all opened files are accepted.*

[17] Dentists became authorized custodians for the purpose of Alberta Netcare, the province's electronic medical records, in June 2018. Alberta Health is responsible for authorizing custodians with access to Netcare.

Summary of Significant Decisions

Guardian's Access to Personal Information of Deceased Individual

An applicant submitted three separate access requests to three different public bodies under the FOIP Act. The requests related to the death of her sister, who received supports from a not-for-profit organization and died while on a day trip. The applicant was the legal guardian and trustee for her sister.

In her request to Alberta Health Services (AHS), the applicant requested a copy of the 911 call that was made by a support worker during the trip. AHS provided a copy of the requested 911 call, but severed the cell phone number of a person who had called 911 under the section pertaining to disclosure harmful to personal privacy (section 17(1)). The Adjudicator found there was insufficient evidence to determine that the cell phone number was personal information. The Adjudicator ordered AHS to reconsider its decision to withhold the cell phone number by taking into account evidence that would enable it to determine whether the cell phone number was likely to be personal information.

A similar request was made to the City of Edmonton. The applicant requested a copy of a fire captain's report. The city provided a copy of the requested report, but severed the cell phone number of a person who had called 911 citing the section pertaining to disclosure harmful to personal privacy (section 17(1)). The Adjudicator found there was insufficient evidence to determine that the cell phone number was personal information. The Adjudicator ordered the City of Edmonton to reconsider its decision to withhold the cell phone number by taking into account evidence that would enable it to determine whether the cell phone number was personal information.

The applicant also made a request to Alberta Justice and Solicitor General (JSG) related to her sister, including a guardian complaint, a trustee complaint, details of her sister's death completed by the Office of the Public Guardian (OPG) and details of her sister's death completed by the not-for-profit organization submitted to the OPG. The requests spanned records during a specified timeframe, from April 2013 to March 2015.

In its response, JSG provided some of the records but severed the name of its employees, the name of an apartment building and the personal information of the applicant's sister from the records. JSG subsequently reconsidered its decision and provided some of the names of its employees and some information about the applicant's sister, but continued to sever the name of the sister from the records.

JSG asserted that disclosure of some of the personal information at issue would be an unreasonable invasion of personal privacy and that personal information of a deceased person is protected for 25 years following death (sections 17(1) and 17(2)(i)).

The Adjudicator noted that the section pertaining to disclosure harmful to personal privacy does not say that a public body is never allowed to disclose third party personal information. It is only when the disclosure of personal information would be an unreasonable invasion of a third party's personal privacy that a public body must refuse to disclose the information to an applicant.

In this case, the Adjudicator concluded that the name of the applicant's sister was personal information and subject to a presumption that it would be an unreasonable invasion of personal privacy if the name were disclosed. The Adjudicator found this presumption was rebutted on the basis that

disclosure would serve the compassionate purpose of enabling the applicant to understand the circumstances of her sister's death. In addition, given that the applicant's sister's name was inferable from the records JSG's, severing would be inconsistent with the purpose of the FOIP Act and disclosure of the name would not be an unreasonable invasion of personal privacy. The Adjudicator ordered the disclosure of the records.

Alberta Health Services, Order F2018-09
Alberta Justice and Solicitor General, Order F2018-08
City of Edmonton, Order F2018-07

Informer Privilege

An applicant made an access request under the FOIP Act to the Edmonton Police Service (EPS) for a copy of a disciplinary decision involving a named constable.

Prior to the inquiry, EPS claimed informer privilege (section 27) over the information to which it had applied sections related to disclosure harmful to individual or public safety and disclosure harmful to law enforcement (sections 18 and 20).

EPS refused to provide that information to the Adjudicator for the inquiry. The inquiry proceeded in two parts. The first part of the inquiry resulted in Order F2015-30, which addressed EPS' application of the section pertaining to disclosure harmful to personal privacy and three names in the disciplinary decision; those names were withheld under that provision only (section 17).

This order concluded the final part of the inquiry, which addressed EPS' application of informer privilege to the name of a detective appearing in the records at issue.

The Adjudicator found that informer privilege applied to the name of the detective sought by the applicant. The law on informer privilege is clear that it must be applied broadly, to include information that could implicitly reveal the identity of the informer. Evidence provided by EPS *in camera* satisfied the Adjudicator that disclosing the name of the detective could lead to identifying a confidential informant.

Edmonton Police Service, Order F2017-79

Access to Remand Centre's Closed Circuit Television Recordings

The applicant made an access request to Alberta Justice and Solicitor General (JSG) for video surveillance of an incident that occurred on his unit at the Calgary Remand Centre. The applicant stated that he was assaulted by another inmate at the Calgary Remand Centre and sought video surveillance relating to the assault so he may seek legal advice to determine whether he had any recourse regarding the assault.

JSG located 10 closed circuit televised (CCTV) videos, but withheld them in their entirety by applying exceptions pertaining to disclosure harmful to personal privacy and public safety (sections 17 and 20). The Adjudicator found that some of the videos were not responsive to the access request. In other videos that showed the alleged assaulter chasing the applicant, the Adjudicator determined the presumption against disclosure applied to the third party's personal information. The Adjudicator then decided whether JSG made the correct determination of all relevant circumstances to rebut the presumption against disclosure. The applicant argued that disclosure was relevant to a fair determination of his rights (section 17(5)(c)).

The Adjudicator found JSG had legitimate concerns regarding the harm that could be occasioned to third parties and to public safety if the applicant were to be given complete access to the information at issue. The Adjudicator also found that access to the information is of significant importance to the applicant for the limited purpose of seeking advice and instructing counsel and outweighs other factors against disclosure.

The submissions of JSG in determining factors weighing against disclosure appear to be relevant if the video recordings become widely available. In Order F2015-02 issued by the OIPC the Adjudicator found there are various means by which to provide access to information. The Adjudicator in this order followed that example by ordering JSG to permit the applicant and his counsel access to five CCTV recordings by examining the recordings at its premises, as opposed to providing unrestricted access to the recordings. The Adjudicator confirmed the refusal to provide access to the other five video recordings.

Alberta Justice and Solicitor General, Order F2017-55

RCMP as a Service Provider to a Municipality

An individual made a privacy complaint about a vulnerable sector check conducted by the Red Deer RCMP detachment.

The Commissioner decided that this matter should proceed directly to inquiry to determine the preliminary issue as to whether the Commissioner has jurisdiction to review the use and/or disclosure of the complainant's personal information by the Red Deer RCMP detachment.

The Adjudicator found that the RCMP detachment is not subject to the FOIP Act even when providing policing services to the City of Red Deer. As such, the OIPC does not have jurisdiction to consider a complaint regarding the collection, use or disclosure of personal information by the RCMP detachment. The complainant was directed to make her complaint to the Office of the Privacy Commissioner of Canada as the appropriate privacy regulator of the RCMP.

Royal Canadian Mounted Police, Order F2017-81

Non-Profit Organization Operating a Commercial Activity

A former employee of Jester's Gaming Lounge, operated by the Castledowns Bingo Association (the organization), made a privacy complaint, alleging that the organization disclosed her personal information without authority under PIPA. The complainant also alleged that the organization failed to secure her personal information.

The Adjudicator determined that the organization is a non-profit organization as defined in PIPA, but that operating the lounge is a commercial activity.

The Adjudicator also determined that employees hired to perform functions necessary to carry out the commercial activity are hired "in connection with" that commercial activity. In this case, the complainant was hired as a bartender in the lounge, and her personal employee information was collected, used and disclosed in connection with a commercial activity.

However, the Adjudicator found insufficient evidence to conclude that the organization disclosed the complainant's personal information or personal employee information as alleged by the complainant. The Adjudicator also found that the organization made reasonable security arrangements to protect her personal information.

Castledowns Bingo Association, Order P2017-07

Tobacco Inquiries

The applicants made separate access requests under the FOIP Act to Alberta Justice and Solicitor General (JSG) for all records containing information relating to the requests for proposals and agreements with respect to awarding a contract for external legal services related to the recovery of health care costs associated with tobacco under the Crown's *Right of Recovery Act.*

Part of this inquiry has been dealt with in Decision F2014-D-03/Order F2014-50. JSG filed a judicial review of that decision/order.

On June 10, 2016, unexpectedly, counsel for JSG provided 35 pages of documents to the External Adjudicator (some of which were a small sample of the records at issue). The provision of the documents complied in part with the decision/order under judicial review. The documents were provided as a result of counsel receiving new instructions from JSG following the same documents being provided to the Ethics Commissioner following the release of the "Report on the Independent Review Conducted by the Honourable Frank Iacobucci, C.C., Q.C.".

The correspondence from JSG disclosed several factors it had considered in defining the scope of the records at issue, which appeared to be considerations not known to the applicants. An exchange of submissions took place with respect to the new information disclosed by JSG, which resulted in the issue of the scope of the records being referred to another forum and being removed as an issue in this phase of the inquiry.

The External Adjudicator provided instructions to the parties on November 16, 2016 with respect to the adjudication of the June 10, 2016 package of documents. This phase of the inquiry was restricted to the 35 pages of documents provided by JSG on June 10, 2016, and were reviewed based on the sections of the FOIP Act that JSG relied on to withhold the records at issue, namely, harm to business interests (section 16), advice from officials (section 24) and privileged information (section 27).

The External Adjudicator found that sections 16 and 27 did not apply. She also found that, although section 24 applied, JSG did not properly exercise its discretion in withholding those records.

The External Adjudicator ordered JSG to reconsider its decision under section 24, make a new decision and provide reasons as to how it applied its discretion. In addition, if JSG's reconsideration resulted in a decision to release some or all of the records for those pages where there was information that fell under the terms of the harm to business interests mandatory exception, the External Adjudicator ordered JSG to give notice to third party(ies) to enable them to provide their consent to the release of the records or to request a review.

Finally, with respect to the applicants' submissions that the public interest override (section 32) ought to apply, the External Adjudicator held that the issue be postponed for consideration until the main inquiry when the remaining 2,570 records at issue would be reviewed.

JSG applied for a judicial review of this order. As of March 31, 2018, the judicial review had not been heard.

Alberta Justice and Solicitor General, Order F2017-61

Landlord and Tenant

An individual submitted a privacy complaint under PIPA claiming that her personal information was disclosed to other tenants, social services, the Canada Revenue Agency and Alberta Health Services by employees of her landlord, Ascot Garden. The information alleged to have been disclosed was information about the complainant's mental health, medications and living situation.

The Adjudicator found that the organization's employees were acting in their employment capacity when they disclosed the complainant's personal information to other tenants and the police. The Adjudicator found that the organization provided no justification for doing so. As a result, the Adjudicator could find no authority under PIPA for the disclosure of the complainant's personal information. There was no evidence, however, that the landlord disclosed the complainant's personal information to social services, the Canada Revenue Agency or Alberta Health Services.

The Adjudicator ordered the organization to cease disclosing the complainant's personal information and to provide training to its employees regarding the disclosure of personal information in the workplace.

Ascot Investments Inc. O/A Ascot Garden, Order P2017-06

Judicial Reviews and Other Court Decisions

Park Place Seniors Living Inc. v. Alberta Health Services

2017 ABQB 575 – Judicial Review of Order F2014-35

In Order F2014-35, a union made a request to a public body, Alberta Health Services (AHS), for access to the audited financial returns of nursing home operators.

AHS decided to sever some information under section 16 of the FOIP Act (disclosure harmful to business interests of a third party), but to disclose some third party information. AHS provided notice of its decision to the nursing homes under section 30 of the FOIP Act, and some of the nursing homes objected to AHS' decision to disclose and requested a review by the Commissioner. Subsequently, AHS decided the nursing home operators were public bodies under the FOIP Act, and that section 16 could not apply, but section 25 (disclosure harmful to economic and other interests) did apply. The union asked the Commissioner to review this decision.

At inquiry, the Adjudicator found that AHS and the nursing home operators had failed to establish that interference to their negotiating positions was reasonably likely to result from disclosure of the information in the audited financial returns under either section 16 or section 25 of the FOIP Act. The Adjudicator ordered disclosure of the withheld information.

On judicial review, the Court applied the reasonableness standard of review to the Adjudicator's decision.

The various applicants raised numerous grounds for judicial review, but the main issue before the Court was the application of the harm test under sections 16 and 25 of the FOIP Act. The Court stated, at paragraph 138:

> ...It is clear from the [Adjudicator's] decision, and other decisions from the Office of the Privacy Commissioner as well as Court of Queen's Bench decisions on review applications that it takes evidence, not arguments to support exemption claims. Mere assertions or opinions, without more, are insufficient.

The Court held the Adjudicator's decision in Order F2014-35 was reasonable; that is, it fell within the range of possible, acceptable and defensible outcomes and the reasons provided were justifiable, transparent and intelligible. The Court dismissed the application for judicial review.

Calgary (Police Service) v. Alberta (Information and Privacy Commissioner)

2017 ABQB 656 – Interim Decision regarding production of new evidence in the Judicial Review of Order F2016-35

An applicant made an access request under the FOIP Act to a public body, the Calgary Police Service (CPS), for all records relating to the processing of a previous access request under the FOIP Act.

A law firm responded on behalf of CPS, stating that responsive records had been located, but were being withheld under sections 24(1)(a), 24(1)(b)(i), 27(1)(a) and 27(1)(b)(i) of the FOIP Act (advice from officials and privileged information). At inquiry, CPS indicated it had applied sections 24(1)(a) and (b) and 27(1)(a) and (b) to sever information from the responsive records. CPS elected to not provide the records to the Adjudicator for review, on the basis that it was asserting solicitor-client privilege over the records.

After submissions were exchanged, the Adjudicator expressed concern regarding the sufficiency of CPS' evidence and asked it to either provide the records or provide more detailed evidence regarding the information to which it had applied the exceptions to disclosure. CPS provided an additional affidavit. Given the involvement of in-house counsel in the matter, the Adjudicator

determined that the principles set out in *Pritchard v. Ontario (Human Rights Commission),* [2004] 1 SCR 809, applied to the inquiry. This case states:

> Owing to the nature of the work of in-house counsel, often having both legal and non-legal responsibilities, each situation must be assessed on a case-by-case basis to determine if the circumstances were such that the privilege arose. Whether or not the privilege will attach depends on the nature of the relationship, the subject matter of the advice, and the circumstances in which it is sought and rendered.

The Adjudicator found CPS' evidence as to the nature of the relationship between those it described as lawyers and itself was insufficient evidence in most cases to enable her to understand the relationships. The Adjudicator also found that CPS' evidence regarding the subject matter of the advice and the circumstances in which any advice may have been sought and rendered was also insufficient in many cases to establish that the records were solicitor-client privileged communications. Finally, the Adjudicator found that CPS' application of multiple exceptions to the same information, all of which require a different factual foundation to apply, had the effect of giving CPS' evidence of the facts an ambiguous quality.

The Adjudicator ordered the disclosure of most of the records to the applicant.

CPS applied for judicial review. Because CPS had refused to provide the records over which it had asserted solicitor-client privilege to the Adjudicator, these records did not form part of the Certified Record of Proceedings. CPS asked the Court to review the records in any event.

The Court distinguished between a public body asserting privilege over a record, and the Commissioner's duty to determine whether, in fact, a record is privileged.

The initial issue before the Court was whether it could review the actual records over which solicitor-client privilege had been asserted by CPS, even though the records had not been before the Adjudicator. The Court issued an interim decision which created an exception to the general rule that new evidence is not allowed on judicial review. The Court stated at paragraph 30:

> I find, therefore, that there is an exception to the rule respecting introduction of new evidence, where the question before the Court on judicial review is solicitor-client privilege, and where the documents in question have not been reviewed by the Administrative Tribunal.

The Court issued this interim decision finding that it could review the records over which solicitor-client privilege had been asserted.

Calgary (Police Service) v. Alberta (Information and Privacy Commissioner)

2018 ABCA 114, which upheld Calgary (Police Service) v. Alberta (Information and Privacy Commissioner), 2017 ABQB 656

The Commissioner appealed the Court of Queen's Bench Interim Decision which created an exception to the general rule preventing new evidence on judicial review. The Court of Appeal upheld the lower Court's decision, in a succinct four-paragraph decision, stating at paragraphs 2 and 3:

> The question before us today is limited. We are not dealing with a range of possible issues, including whether a different statutory regime might be adopted in light of observations made by the Supreme Court of Canada. Instead, it is whether, on a judicial review application under the *Freedom of Information and Protection of Privacy Act,* a Court is entitled to review documents over which claims of solicitor-client privilege have been made even though those documents were not reviewed by the Privacy Commissioner and are not "formally" part of the certified record.
>
> We are satisfied that on a judicial review application where the dispute centres on whether the documents in question are subject to solicitor-client privilege, those documents should be put before the reviewing Court. It is this simple. The issue – whether solicitor-client privilege exists with respect to the disputed documents – cannot be properly determined in these circumstances without examining the documents themselves. This approach is consistent with the supervisory role of the Court.

The Court dismissed the appeal of the lower Court's Interim Decision. Accordingly, the judicial review of Order F2016-35 is ongoing before the Court of Queen's Bench of Alberta.

Gowrishankar v. JK

2018 ABQB 70 – Judicial Review of Order H2016-06, currently under appeal

An individual complained that two physicians accessed her health information from Alberta Netcare in contravention of HIA in both 2008 and 2012. The 2008 Netcare accesses occurred for the purpose of addressing a complaint made to the Department Chair about care the physicians had provided to the complainant and the 2012 Netcare accesses occurred for the purpose of the physicians defending themselves in a related hearing conducted by the Alberta College of Physicians and Surgeons (College). The two physicians also disclosed the health information they had obtained to the College.

Alberta Health Services (AHS) operated the facilities in which the Netcare accesses occurred and was the custodian. The two physicians were acting as affiliates of AHS. The Adjudicator determined that affiliates may use or disclose health information only at the direction of, under the authority of or on behalf of the custodian with whom they are affiliated. The Adjudicator found the physicians had accessed the complainant's health information for their own personal purposes, rather than those of AHS and therefore, AHS had, by operation of section 62(2) of HIA, contravened section 25 of HIA (prohibition regarding use of health information) by accessing the complainant's health information in Netcare.

The Adjudicator also determined that the complainant's health information had been disclosed to the College by the two physicians for the purpose of defending themselves in a complaint. She found that affiliates may disclose health information only under the authority of, or on behalf of the custodian with whom they are affiliated and are subject to the same limitations to which the custodian is subject when they do so. She determined that AHS would have had no authority to disclose the complainant's health information in the circumstances in which the two affiliates disclosed it, as AHS was not a party to the complaint conducted by the College, and had not received a formal demand for the records. The Adjudicator concluded that these accesses and disclosures caused AHS to contravene sections 25 and 31 of HIA.

The Adjudicator determined that AHS' policies and procedures were not adequate to protect the complainant's health information from the risks of unauthorized use and disclosure, as they appeared to permit affiliates to use and disclose health information for their own personal purposes, rather than purposes of AHS that are authorized by sections 27 and 35 of HIA. While the Adjudicator found that use and disclosure of the complainant's health information by the two physicians had led AHS to contravene HIA, it appeared that the two physicians had not contravened AHS policies and procedures when they used and disclosed the complainant's health information for their own personal purposes because the policies and procedures were not sufficient.

Although the Adjudicator ordered the two physicians to meet their duty to comply with HIA and its regulations when they use and disclose health information, the Adjudicator decided that she could not order the two physicians to comply with AHS' policies and procedures, given that doing so would not ensure the confidentiality of the complainant's health information. The Adjudicator ordered AHS to cease using and disclosing the complainant's health information in contravention of HIA. She suggested that compliance with the order could be achieved by revising the policies and procedures for affiliates.

The Adjudicator also determined that AHS should review its policies to ensure that they create enforceable obligations for affiliates to collect, use or disclose health information under the authority of AHS, in compliance with HIA, such that section 62(4)(b) is engaged should an affiliate use or disclose health information in a way that contravenes HIA.

On judicial review, the Court generally applied the reasonableness standard of review to the Adjudicator's interpretation of a home statute, in this case, HIA; however, the Court stated that a correctness standard of review applies when a decision strays into an arena of contractual interpretation outside the Adjudicator's area of expertise.

The Court held the Adjudicator's determination that the 2008 Netcare accesses were not for the purpose of providing health care services was reasonable; however, the Court further held that the Adjudicator's determination that the 2008 Netcare accesses were done for their own personal benefit was unreasonable. With respect to the physicians' 2012 Netcare accesses, the Court held the physicians were implicitly authorized to do so under the College's consent form and therefore, the Adjudicator's finding was unreasonable.

The Court quashed Order H2016-06. The complainant has appealed the Court's decision.

Alberta Energy Regulator v. Information and Privacy Commissioner and Jennie Russell

Oral decision of Horner J., Action No. 1601-15874, February 21, 2018 – Judicial Review of Order F2016-39

A journalist requested access for all records in the custody or control of a public body, the Alberta Energy Regulator (AER), relating to "broad industry initiatives". The broad industry initiatives refer to a practice that was discontinued in 2014 by which AER collected money from producers and provided this money to two industry associations: the Canadian Association of Petroleum Producers (CAPP) and the Small Explorers and Producers Association of Canada (SEPAC). The applicant requested a fee waiver on the basis that the records related to the public interest. AER denied the applicant's request for a fee waiver and required her to pay $1,218.50 for the services it had provided in processing her access request.

The Adjudicator determined that AER had not properly calculated the fees for providing services, as it had included 40 hours at a rate of $27 per hour for manually entering data in order to create records for the applicant. AER also did not establish that $0.25 per page reflected its actual costs for photocopying the records. The Adjudicator determined that the fees should have been calculated at $81.

The Adjudicator determined that the records relate to the functioning of a statutory entity responsible for regulating such things as oil and gas, energy and surface rights in Alberta, and its distribution of public funds. The Adjudicator determined that the records requested by the applicant related to a matter of public interest and that the applicant had requested them in order to write an article for the purpose of promoting public debate and awareness regarding this matter. The Adjudicator decided that the fees should be waived in the public interest and reduced the fees to zero.

On judicial review, the Court applied a reasonableness standard of review to the order. The Court held that the findings of the Adjudicator were reasonable and further ordered AER to pay costs to the applicant in the amount of $1,250. The judicial review was dismissed.

Chief of Police of the Calgary Police Service v. Criminal Trial Lawyers' Association, Information and Privacy Commissioner and Minister of Justice and Attorney General for the Province of Alberta

Oral decision of Nation J., Action No. 1501-05251, January 12, 2017 – Judicial Review of Order F2015-08; appeal discontinued.

This judicial review was reported on in the 2016-17 Annual Report. The appeal was discontinued on January 30, 2018. Order F2015-08 was upheld by the Court of Queen's Bench on January 12, 2017.

EDUCATION & OUTREACH

Survey: Access to Information and Privacy Rights Matter to Albertans

Albertans believe strongly in the importance of protecting privacy and the right to access information. The OIPC commissioned a public opinion survey, conducted in October 2017, which showed that 95% of respondents believe it is important to protect the privacy of personal information, but only 27% felt more secure about the privacy of their own personal information today than they did five years ago. More than 90% of respondents felt it is important to protect their right to access information, although only 39% were confident about their ability to exercise that right.

The survey also asked Albertans to identify the access and privacy issues of most importance. A list of 24 topics was provided and respondents identified the following as the most significant:

- Identity theft and fraud
- Hacking, malware, ransomware and email phishing
- Inappropriate employee access (also referred to as employee "snooping")
- Mobile device security
- Child and youth privacy

Since 2013, when the OIPC last commissioned a general population survey, the number of access requests submitted to government departments and other local public bodies has increased significantly. Additionally, privacy breaches caused by hacking, phishing or malware in the private sector are more frequently reported to the OIPC, as are "snooping" cases in the health sector. These and other realities continue to bring access and privacy issues to the fore in Alberta.

Survey results show that while these issues continue to matter to Albertans, the public often struggles to understand how their own lives are impacted, and how they can exercise their legal rights under Alberta's access and privacy laws. Less than half of respondents were aware that they can file a complaint with the OIPC when they feel that their personal or health information has been improperly collected, used or disclosed. And only 32% were aware that they can ask the OIPC to review a response to an access request that they received from a public body, health care provider or private business.

The general population telephone survey of 800 randomly selected Albertans provides feedback about the public's awareness of access and privacy laws, their rights under those laws, and the role of the OIPC, as well as to identify the access and privacy issues of most importance to Albertans.

> "Albertans care about these issues, but new technologies, shifting economies and evolving social norms are challenging our ability to exercise these rights. This survey helps to inform my office and stakeholders about where to focus to improve Albertans' awareness of how they are impacted by these issues and how they can exercise their rights under Alberta's three access and privacy laws."
>
> *- Commissioner Jill Clayton, November 30, 2017* [18]

[18] OIPC news release, "Survey: Access to Information and Privacy Rights Matter to Albertans", is available at https://www.oipc.ab.ca/news-and-events/news-releases/2017/survey-access-to-information-and-privacy-rights-matter-to-albertans.aspx.

Presentations, Forums and Workshops

In 2017-18, the Commissioner and staff participated in 72 presentations, training sessions and speaking engagements. These events provide an opportunity for the office to increase awareness about access and privacy issues, and share the office's experiences.

The Legislative Assembly of Alberta's School at the Legislature program, in which the OIPC continued to participate, provides a great opportunity to connect OIPC staff with young Albertans to discuss access and privacy rights in the digital economy.

The OIPC also continues to host privacy impact assessment and privacy breach training workshops. The training sessions were held in Edmonton and Calgary in October 2017.

RIGHT TO KNOW WEEK FORUMS

The OIPC had a variety of speakers for the 2017 Right to Know Week Forums, covering a diverse and thoughtful range of topics.

In Calgary, Karen Meelker, Access and Privacy Officer for the University of Manitoba and the National Centre for Truth and Reconciliation (NCTR), discussed the NCTR's role in preserving residential school records, providing access to this information and protecting personal information. Ms. Meelker also provided a brief overview of a case that went to the Supreme Court of Canada in May 2017 that related to the disposition of records generated by the Independent Assessment Process, which is a settlement fund for claims of abuse and other wrongful acts committed at Canada's residential schools.

In Edmonton, Nicole Bresser, a lawyer, discussed the case that went to the Supreme Court and her role representing the Coalition to Preserve Truth, which was an intervener on the case. The coalition was formed to advocate for the preservation of the records created during the Independent Assessment Process.

At both events, a panel of different users of the access to information system in Alberta presented on some of the experiences they have in navigating the process. Sean Holman, Associate Professor of Journalism at Mount Royal University, was asked to form and moderate the panels in both Calgary and Edmonton. The panelists included journalists, a community activist, an academic and a researcher for the Official Opposition.

The Commissioner also presented on some of the things she heard during the International Conference of Information Commissioners in Manchester, United Kingdom, which she was invited to attend. The Commissioner presented as part of a panel discussion at the international conference which tackled the question, "What are progressive information rights?"

Right to Know Day is internationally recognized annually on September 28 to generate awareness about an individual's right to access public information and to promote freedom of information as a cornerstone to democracy and good governance. The United Nations Educational, Scientific and Cultural Organization (UNESCO) has proclaimed September 28 as the "International Day for the Universal Access to Information".

DATA PRIVACY DAY: ARTIFICIAL INTELLIGENCE

Artificial intelligence and machine learning continue to transform a variety of disciplines and professions in what were considered unimaginable ways not too long ago. These advancements have direct and at times unintended impacts on society's perceptions of privacy and data protection.

The Data Privacy Day event in Edmonton in January 2018 included three speakers – from theory to practice to assessment.

First, Professor Randy Goebel, Department of Computing Science from the University of Alberta, provided an overview of artificial intelligence and machine learning. He highlighted what it is, what it is not, some of the limitations and some of the ways it may impact our lives going forward.

Second, Colin McKay, Manager, Global Public Policy with Google Canada, outlined how Google has harnessed artificial intelligence and machine learning in the products it offers customers.

Finally, Martin Abrams, Executive Director, The Information Accountability Foundation, highlighted work that he has done with the private sector in developing an ethical assessment framework for big data and other processing of personal information that goes beyond traditional privacy impact assessments.

Data Privacy Day is internationally recognized on January 28 to promote the protection of personal information.

UNITED NATIONS GLOBAL PULSE DATA ETHICS PANEL

The Commissioner participated on a panel during the United Nations Global Pulse and International Association of Privacy Professionals joint event in New York on "Building a Strong Privacy and Data Ethics Program: From Theory to Practice".

The panel spoke about accessing data for the public good, and shared different strategies and considerations for sharing data for humanitarian and development causes.

In addition to the Commissioner, the panel included representatives from the International Committee of the Red Cross, Nielsen Market Research and the Alfred P. Sloan Foundation.

TEACHING STUDENTS ABOUT PRIVACY RIGHTS IN THE INFORMATION ECONOMY

The Commissioner was invited to present to five education groups or associations in Alberta during 2017-18, and encouraged the education sector to teach students about access and privacy rights in the information economy.

In advocating for privacy to be a component in education curriculum, the Commissioner said, "Students today and in the future will need the tools to succeed in a world where the leading international currency is data. But they need to use this currency ethically and with consideration of human rights."

The presentations promoted the International Privacy Competency Framework for School Students, The eQuality Project which the office supports, and educational resources that federal, provincial and territorial develop in collaboration.

Presentation to the Alberta Education Curriculum Review Working Groups

> "Privacy education is an area where everyone seems to be on the same page – we need more of it to teach students how to safely navigate their networked world. At the same time, it feels as though we're never catching up – new tools, games and gadgets keep coming up with new ways to collect and share information often without knowing exactly how that information is being collected, shared and monetized...
>
> I would like to see digital rights and responsibilities formalized in the curriculum so that these important discussions are facilitated by professional educators in classrooms, as well as at home with parents and guardians."
>
> *- Commissioner Jill Clayton, May 12, 2017*

Collaboration with Other Jurisdictions

The OIPC annually partners with Information and Privacy Commissioners and Ombudspersons in Canadian jurisdictions, as well as international counterparts, on a variety of initiatives.

JOINT RESOLUTION ON SOLICITOR-CLIENT PRIVILEGE

In a joint resolution, Canada's Information and Privacy Commissioners called on their respective governments to amend access to information and privacy legislation to ensure they are empowered to compel the production of records in order to independently review records over which public bodies claim solicitor-client privilege.

In *Alberta (Information and Privacy Commissioner) v. University of Calgary,* 2016 SCC 53, the Supreme Court of Canada determined that legislative language did not expressly permit the Commissioner to compel the production of records over which solicitor-client privilege had been claimed.

Canada's Commissioners were concerned with this decision as they require the power to compel these records in order to properly fulfil their mandate of providing independent review of public bodies' responses to requests for access to information.

The joint resolution was agreed upon by Canada's Information and Privacy Commissioners at their annual federal, provincial and territorial meeting in October 2017. The 2017 meeting was hosted by the Information and Privacy Commissioner of the Northwest Territories and Nunavut in Iqaluit, Nunavut.

The joint resolution and associated news release are available at www.oipc.ab.ca.

MINISTERS OF EDUCATION CALLED ON TO PRIORITIZE PRIVACY EDUCATION

Young Canadians growing up in an era of unprecedented technological change with profound impacts on privacy was the impetus for a joint letter written by Canada's federal, provincial and territorial privacy protection authorities to the Council of Ministers of Education, Canada. Commissioners urged Ministers of Education in their respective jurisdictions to include privacy education as a clear and concrete component in digital literacy curricula across the country.

In the November 2017 letter, Commissioners recognized that many schools currently teach digital literacy skills but privacy is not necessarily part of the courses offered. They also promoted the International Privacy Competency Framework for School Students, which was adopted at the 2016 International Conference of Data Protection and Privacy Commissioners.

The competency framework serves as a roadmap for teachers around the world, outlining nine foundational privacy principles students ought to know and understand. This includes being able to identify what constitutes personal information, being able to understand both the technical and economic aspects of the digital environment, knowing how to limit disclosure of personal information and how to protect oneself online. The framework also guides students in learning how to exercise their privacy rights and responsibilities.

The framework was developed with the flexibility to incorporate access to information and privacy laws in different jurisdictions.

In follow up to the letter, the Commissioner also wrote to Alberta's Minister of Education highlighting key privacy education initiatives undertaken by the OIPC to promote the importance of teaching privacy rights in Alberta's schools. The Commissioner also requested to meet with the Minister of Education to further make the case for the importance of teaching students about privacy rights in the digital economy. The Commissioner and Minister of Education met in January 2018.

Both letters are available at www.oipc.ab.ca.

JOINT POLICY STATEMENT ON GENETIC TESTING

In December 2017, the OIPC partnered with colleagues at the Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner for British Columbia in issuing an updated "Direct-to-Consumer Genetic Testing and Privacy" policy statement for private sector privacy laws.

The federal government passed the *Genetic Non-Discrimination Act* that prohibits an individual to undergo a genetic test or to disclose the existing results of genetic tests (e.g. an insurance company or employer cannot require an individual to take a genetic test and cannot require, if one has been taken, that the results be disclosed to them, unless the individual voluntarily provides written consent). That law came into effect in May 2017.

What Are the Potential Privacy Risks Associated with Genetic Testing?

"As direct-to-consumer genetic tests become increasingly available it is important to understand their privacy risks. Genetic information can be highly sensitive personal information. Combined with contact, health, lifestyle, and financial information, genetic information paints a very detailed picture of you, and potentially your family members."

- Direct-to-Consumer Genetic Testing

Available from www.oipc.ab.ca

GLOBAL PRIVACY SWEEP

The OIPC joined 23 other privacy regulators around the world to analyze how effectively privacy policies are communicated and how much control users have over the information they give to websites and apps. In total, 455 websites and apps were analyzed, including 20 Alberta-based websites. Generally, in Alberta, the results were positive and privacy issues and risks were adequately communicated.

Of the 20 Alberta websites reviewed, 20% did not have a privacy policy despite collecting personal information. Meantime, 65% of the websites failed to disclose to users in which country their information was stored, and more than half did not provide a clear means for deleting or removing their personal information, once collected by the website. Additionally, 40% of the websites failed to adequately explain whether personal information is shared with third parties and to whom that data is shared.

The results in Alberta are similar to those globally, as among the 455 websites and apps analyzed:

- Privacy communications across the various sectors tended to be vague, lacked specific detail and often contained generic clauses.
- The majority of organizations failed to inform the user what would happen to their information once it had been provided.
- Organizations generally failed to specify with whom data would be shared.
- Many organizations failed to refer to the security of the data collected and held – it was often unclear in which country data was stored or whether any safeguards were in place.
- Just over half the organizations examined made reference to how users could access the personal data held about them.

More positively, most organizations were generally quite clear on what types of information they would collect from the user and more than half of organizations provided users with a means to access the personal information that had been collected.

The annual privacy sweep is coordinated by the Global Privacy Enforcement Network, which was established in 2010 upon recommendation by the Organisation for Economic Co-operation and Development. Its aim is to foster cross-border cooperation among privacy regulators in an increasingly global market in which commerce and consumer activity relies on the seamless flow of personal information across borders. Its members seek to work together to strengthen personal privacy protections in this global context. As of October 2017, the informal network was comprised of over 60 privacy enforcement authorities in 39 jurisdictions around the world.

> "At the core of privacy laws is for individuals to have control over their own personal information; the information economy has eroded this principle. As more awareness is raised about these practices, all sectors would be well served to ensure control is given back to consumers and citizens for both legal and ethical reasons. These include having mechanisms in place for individuals to access, delete and better understand what is happening to their own personal information."
>
> *- Commissioner Jill Clayton, October 24, 2017* [19]

[19] OIPC news release, "Global Privacy Sweep Finds Websites, Apps Often Not Effectively Communicating Privacy Practices", is available at https://www.oipc.ab.ca/news-and-events/news-releases/2017/survey-access-to-information-and-privacy-rights-matter-to-albertans.aspx.

Media Awareness

TRADITIONAL MEDIA

The OIPC received fewer media requests in 2017-18. There were 73 media requests compared to 108 in 2016-17.

There was only one investigation report issued that related to government departments which contributed to fewer media requests overall. Generally, the office receives more media requests when investigation reports about government departments are issued publicly.

The investigation report into allegations of delays and possible interference by the Government of Alberta in responding to access requests accounted for more than five media requests from online, print or radio outlets. That report was issued in conjunction with the special report on producing records to the Commissioner, which also received media attention.

Throughout the year, the topic of police services' disclosures of homicide victims' names was of media interest, particularly in Edmonton. Media noticed that some police services were no longer disclosing the names of homicide victims in all cases. Police services were basing these decisions on their interpretation of access and privacy laws, as noted in the media.

In response to this change in direction by some police services, the Alberta Association of Chiefs of Police (AACP) collaborated on a policy framework outlining how decisions to disclose or not disclose homicide victims' names would be released. The Commissioner was asked by the AACP in June 2017 to review their draft Decision Framework on Naming Homicide Victims. The Commissioner provided comments and recommendations on the framework. Police chiefs confirmed publicly that they considered the Commissioner's recommendations in the final framework, which is available on the AACP's website.

While the office does not often receive media requests in relation to high profile privacy breaches reported publicly, there was general interest in the sheer number of privacy breach notification decisions the OIPC rendered in the 2017 calendar year. Additionally, the breach notification decision related to Uber Canada Inc. garnered a few media requests.

The investigation into multiple alleged unauthorized accesses of health information at South Health Campus, and Official Opposition complaints about certain access to information issues also received media attention in 2017-18.

SOCIAL MEDIA

Twitter continues to be used by the OIPC to share orders, investigation reports, publications and news releases, and promote events or raise awareness about access and privacy laws. When appropriate, the OIPC will respond to questions or concerns on Twitter.

There were 213 tweets, replies and retweets in 2017-18. This was an increase of 22 tweets on the social media site compared to 2016-17.

The following five topics attracted the most attention on Twitter:

- A newspaper article that stated that no legislation prohibits school employees from telling parents what clubs students have joined was clarified in a tweet, which highlighted that students have legislated privacy rights under already-established laws and that schools can only disclose personal information of students without consent in specific situations.
- The special report and request for legislative amendment on producing records to the Commissioner.
- The promotion of privacy education for students in a number of related tweets.
- The joint guidance on direct-to-consumer genetic testing.
- The news release on the conviction of a pharmacist for unauthorized access to health information.

Robert C. Clark Award

Maryann Hammermeister was the recipient of the 2017-18 Robert C. Clark Award for her efforts in advancing access to information in Alberta. The award was presented to Ms. Hammermeister during an Edmonton Public School Board (EPSB) meeting in March 2018.

Ms. Hammermeister, the District FOIP Coordinator for EPSB, was selected unanimously by an independent, three-person panel of experts in the field of access to information. In making their selection, the panel noted that Ms. Hammermeister has "shown very strong leadership in access to information" and "obviously thinks from the perspective of the user." They were impressed by her outreach efforts, education initiatives and collaboration with other access to information and privacy professionals in Alberta.

The selection panel members were:

- Catherine Tully, Information and Privacy Commissioner for Nova Scotia
- Hank Moorlag, former Yukon Information and Privacy Commissioner
- Drew McArthur, former Acting Information and Privacy Commissioner for British Columbia

The award is named after Alberta's first Information and Privacy Commissioner, Robert (Bob) Clark, who served in that role from 1995 to 2001. Clark led the OIPC through the introduction and expansion of the FOIP Act, while also acting as an educator and advocate for the principles of access to information and privacy.

FINANCIAL STATEMENTS

Auditor General
OF ALBERTA

Independent Auditor's Report

To the Members of the Legislative Assembly:

Report on the Financial Statements

I have audited the accompanying financial statements of the Office of the Information and Privacy Commissioner, which comprise the statement of financial position as at March 31, 2018, and the statements of operations, change in net debt and cash flows for the year then ended, and a summary of significant accounting policies and other explanatory information.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these 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 financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

My responsibility is to express an opinion on these financial statements based on my audit. I conducted my audit in accordance with Canadian generally accepted auditing standards. Those standards require that I comply with ethical requirements and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements 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 entity's internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my audit opinion.

Opinion

In my opinion, the financial statements present fairly, in all material respects, the financial position of the Office of the Information and Privacy Commissioner as at March 31, 2018, and the results of its operations, its remeasurement gains and losses, its changes in net debt, and its cash flows for the year then ended in accordance with Canadian public sector accounting standards.

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

Auditor General
July 24, 2018
Edmonton, Alberta

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
STATEMENT OF OPERATIONS

Year ended March 31, 2018

	2018 Budget	2018 Actual	2017 Actual
Revenues			
Prior Year Expenditure Refund	$ -	$ 9,482	$ 25,375
Other Revenue	-	734	178
	-	10,216	25,553
Expenses – Directly Incurred (Note 3b)			
Salaries, Wages, and Employee Benefits	$ 5,559,817	$ 5,132,348	$ 5,501,760
Supplies and Services	1,313,474	1,536,055	1,142,475
Amortization of Tangible Capital Assets (Note 4)	55,000	47,003	53,900
Total Program-Operations	6,928,291	6,715,406	6,698,135
Net Cost of Operations	$ (6,928,291)	$ (6,705,190)	$ (6,672,582)

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

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

STATEMENT OF FINANCIAL POSITION

As at March 31, 2018

	2018	2017
Financial Assets		
Cash	$ 200	$ 200
Accounts Receivable	2,490	3,646
	2,690	3,846
Liabilities		
Accounts Payable and Accrued Liabilities	310,886	358,122
Accrued Vacation Pay	498,119	510,819
	809,005	868,941
Net Debt	(806,315)	(865,095)
Non-Financial Assets		
Tangible Capital Assets (Note 4)	114,206	141,177
Prepaid Expenses	13,606	10,737
	127,812	151,914
Net Liabilities	$ (678,503)	$ (713,181)
Net Liabilities at Beginning of Year	$ (713,181)	$ (782,585)
Net Cost of Operations	(6,705,190)	(6,672,582)
Net Financing Provided from General Revenues	6,739,868	6,741,986
Net Liabilities at End of Year	$ (678,503)	$ (713,181)

Contractual obligations (Note 6)

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

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
STATEMENT OF CHANGES IN NET DEBT

Year ended March 31, 2018

	2018		2017
	Budget	Actual	Actual
Net Cost of Operations	$ (6,928,291)	$ (6,705,190)	$ (6,672,582)
Acquisition of Tangible Capital Assets (Note 4)	-	(20,032)	(72,111)
Amortization of Tangible Capital Assets (Note 4)	55,000	47,003	53,900
Change in Prepaid Expenses	-	(2,869)	(3,701)
Net Financing Provided from General Revenue	6,873,291	6,739,868	6,741,986
Decrease in Net Debt	-	58,780	47,492
Net Debt, Beginning of Year	-	(865,095)	(912,587)
Net Debt, End of Year	$ -	$ (806,315)	$ (865,095)

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

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

STATEMENT OF CASH FLOWS

Year ended March 31, 2018

	2018	2017
Operating Transactions		
Net Cost of Operations	$ (6,705,190)	$ (6,672,582)
Non-cash Items Included in Net Cost of Operations		
Amortization of Tangible Capital Assets (Note 4)	47,003	53,900
	(6,658,187)	(6,618,682)
Decrease (Increase) in Accounts Receivable	1,156	(365)
(Increase) in Prepaid Expenses	(2,869)	(3,701)
(Decrease) in Accounts Payable and Accrued Liabilities	(59,936)	(47,027)
Cash Applied to Operating Transactions	(6,719,836)	(6,669,775)
Capital Transactions		
Acquisition of Tangible Capital Assets (Note 4)	(20,032)	(72,111)
Financing Transactions		
Net Financing Provided from General Revenues	6,739,868	6,741,986
Cash, Increase	-	100
Cash, at Beginning of Year	200	100
Cash, at End of Year	$ 200	$ 200

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

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

March 31, 2018

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 of the Information and Privacy Commissioner 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

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.

The Office has prospectively adopted the following standards from April 1, 2017: PS 2200 Related Party Disclosures, PS 3420 Inter-Entity Transactions, PS 3210 Assets, PS 3320 Contingent Assets and PS 3380 Contractual Rights which are reflected in Note 4 and Schedule 2.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2018

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

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.

a) Revenue

All revenues are reported on the accrual basis of accounting.

b) Expenses

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.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2018

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:

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

Non-financial assets of the Office are limited to tangible capital assets and prepaid expenses.

f) 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.

g) Net debt

Net debt indicates additional cash that will be required from General Revenues to finance the Office's cost of operations to March 31, 2018.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2018

Note 4 Tangible Capital Assets

	Office equipment and furniture	Computer hardware and software	Total
Estimated Useful Life	5 years	5 years	
Historical Cost			
Beginning of Year	$ 83,318	$ 432,311	$ 515,629
Additions	-	20,032	20,032
	$ 83,318	$ 452,343	$ 535,661
Accumulated Amortization			
Beginning of Year	$ 72,280	$ 302,172	$ 374,452
Amortization Expense	3,679	43,324	47,003
	$ 75,959	$ 345,496	$ 421,455
Net Book Value at March 31, 2018	$ 7,359	$ 106,847	$ 114,206
Net Book Value at March 31, 2017	$ 11,038	$ 130,139	$ 141,177

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2018

Note 5 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 $671,822 for the year ended March 31, 2018 (2017 – $762,215).

At December 31, 2017, the Management Employees Pension Plan reported a surplus of $866,006,000 (2016 - surplus $402,033,000) and the Public Service Pension Plan reported a surplus of $1,275,843,000 (2016 – surplus $302,975,000). At December 31, 2017 the Supplementary Retirement Plan for Public Service Managers had a deficit of $54,984,000 (2016 - deficit $50,020,000).

The Office also participates in a multi-employer Long Term Disability Income Continuance Plan. At March 31, 2018, the Management, Opted Out and Excluded Plan reported an actuarial surplus of $29,805,000 (2017 – surplus $31,439,000). The expense for this plan is limited to employer's annual contributions for the year.

Note 6 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.

	2018	2017
Obligations under operating leases and contracts	$ 23,399	$ 17,419

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

	Total
2018-19	$ 11,586
2019-20	6,821
2020-21	4,992
	$ 23,399

Note 7 Comparative Figures

Certain 2017 figures have been reclassified to conform to the 2018 presentation.

Note 8 Approval of Financial Statements

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

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 1 - SALARY AND BENEFITS DISCLOSURE

Year ended March 31, 2018

	2018			2017
	Base Salary [a]	Other Non-cash Benefits [b][c]	Total	Total
Senior Official				
Information and Privacy Commissioner	$ 242,743	$ 63,659	$ 306,402	$ 483,291

[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, tuition fees.

[c] Other non-cash benefits for the Information and Privacy Commissioner paid by the Office includes $8,185 (2017: $7,298) being the lease, fuel, insurance and maintenance expenses for an automobile provided.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 2 - ALLOCATED COSTS

Year ended March 31, 2018

	2018					2017
	Expenses - Incurred by Others					
Program	Expenses [a]	Accommodation Costs [b]	Telephone Costs [c]	Business Services [d]	Total Expenses	Total Expenses
Operations	$ 6,715,406	$ 482,077	$ 18,723	$ 52,000	$ 7,268,206	$ 7,242,985

[a] Expenses - Directly Incurred as per Statement of Operations.
[b] Costs shown for Accommodation (includes grants in lieu of taxes), allocated by square meters.
[c] Other costs are for telephone land line charges.
[d] Business services includes charges for shared services, finance services, technology services, IMAGIS, and Corporate Overhead.

APPENDICES

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

Statistics are from April 1, 2017 to March 31, 2018

FOIP Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Disclosure to Commissioner (Whistleblower)	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request Authorization to Indirectly Collect	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies																	**0**
Boards		1	12						1		1	7		2			**24**
Colleges			4						1				2	2	3		**12**
Commissions			2				1		1			4		7	1		**16**
Committees												1					**1**
Crown Corporations												2					**2**
Federal Departments			1								1						**2**
Foundations												1					**1**
Government Ministries/Departments	1	13	31			5	6		2	6		6	158	50	145	21	**444**
Health Quality Council of Alberta																	**0**
Hospital Board (Covenant Health)																1	**1**
Law Enforcement Agencies		2	9			1		3				1	77		9	1	**103**
Legislative Assembly Office													1				**1**
Local Government Bodies			2							1			2				**5**
Long Term Care Centres																1	**1**
Municipalities		2	14			3	1			1		3	98	8	16	9	**155**
Nursing Homes																	**0**
Office of the Premier/ Alberta Executive Council							1						13	1	2	1	**18**
Officers of the Legislature					1							1					**2**
Panels																	**0**
Regional Health Authorities (Alberta Health Services)		2	11				1			4			42	1	24		**85**
School Districts			5							1		2	13		1	7	**29**
Universities		1	4									1	26	2	15	4	**53**
Other			1						1	2		6	9	1	5	1	**26**
Total	**1**	**21**	**96**	**0**	**1**	**9**	**10**	**3**	**3**	**18**	**0**	**22**	**454**	**65**	**228**	**50**	**981**

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2017 to March 31, 2018

HIA

Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fees	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			2		**5**
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians														**0**
Chiropractors								24	3			2		**29**
Dental Hygienists								14						**14**
Dentists								76		2		3		**81**
Denturists														**0**
Government Ministries/Departments								1						**1**
Health Professional Colleges & Associations			1						2					**3**
Health Quality Council of Alberta								1						**1**
Hospital Board (Covenant Health)			5					2		3		4		**14**
Long Term Care Centres												1		**1**
Midwives														**0**
Minister of Health (Alberta Health)								18	3			53		**74**
Nursing Homes										1		2		**3**
Opticians														**0**
Optometrists								60						**60**
Pharmacies/Pharmacists			3					277				9		**289**
Physicians			20					224	1	13		30		**288**
Podiatrists								1						**1**
Primary Care Networks								17	5			5		**27**
Regional Health Authorities (Alberta Health Services)			19			1		35	1	12		15		**83**
Registered Nurses								19	2			3		**24**
Research Ethics Boards									1					**1**
Researchers														**0**
Subsidiary Health Corporations			6					2				2		**10**
Universities/Faculties of Medicine														**0**
Other			2				3		2			2		**9**
Total	**0**	**0**	**56**	**0**	**0**	**1**	**0**	**3**	**771**	**23**	**31**	**0**	**133**	**1018**

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2017 to March 31, 2018

PIPA Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request for Advance Ruling	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Accommodation & Food Services			2								2		21		**25**
Admin & Support Services			1								1		6		**8**
Agriculture, Forestry, Fishing & Hunting													1		**1**
Arts, Entertainment & Recreation			3			3					1		9		**16**
Child Day-care Services			2								2		3		**7**
Collection Agencies													2		**2**
Construction			4								2		1		**7**
Credit Bureaus			2								1		1		**4**
Credit Unions			1							1	1		10		**13**
Dealers in Automobiles			2			1					5		4		**12**
Educational Services													2		**2**
Finance		1	7							1	7		35		**51**
Health Care & Social Assistance			11						1	1	9		15		**37**
Information & Cultural Industries			5							2			8		**15**
Insurance Industry			6								5		11		**22**
Investigative & Security Services			1												**1**
Legal Services			9							1	2		7		**19**
Management of Companies & Enterprises		1											1		**2**
Manufacturing			2								3		8		**13**
Medical & Diagnostic Laboratories											1				**1**
Mining, Oil & Gas			6								11		7		**24**
Motor Vehicle Parts & Accessories		3	17						1	4					**25**
Nursing Homes/Home Health Care			1							1			1		**3**
Private Healthcare & Social Assistance															**0**
Professional, Scientific & Technical			6						1	1	4		21		**34**
Public Administration			1			1				2	1				**5**
Real Estate, Rental, Leasing			17								13		8		**38**
Retail			5							2	2		30		**39**
Trades/Contractors			1								1		2		**4**
Transportation			2			1					5		3		**11**
Utilities			2												**2**
Wholesale Trade			3										5		**8**
Other											8		9		**17**
Total	**0**	**5**	**119**	**0**	**0**	**6**	**0**	**0**	**3**	**1**	**16**	**87**	**0**	**231**	**468**

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2017 to March 31, 2018

FOIP

Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Disclosure to Commissioner (Whistleblower)	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request Authorization to Indirectly Collect	Request for Information	Request for Review	Request for Review 3rd Party	Request Time Extension	Self-reported Breach	Total
Agencies																	**0**
Boards			11						1		1	6	1	2			**22**
Colleges			2			1			1			4		1	3		**12**
Commissions			1									2		6	1		**10**
Committees												1					**1**
Crown Corporations												1					**1**
Federal Departments			1								1						**2**
Foundations												1					**1**
Government Ministries/Departments	1	3	24	1		3	18		3		5	145	21	142	20		**386**
Health Quality Council of Alberta																	**0**
Hospital Board (Covenant Health)															1		**1**
Law Enforcement Agencies		1	7			1		3				66		9	1		**88**
Legislative Assembly Office																	**0**
Local Government Bodies			2						1			3					**6**
Long Term Care Centres																	**0**
Municipalities		1	18			1			2		2	82	6	17	12		**141**
Nursing Homes																	**0**
Office of the Premier/ Alberta Executive Council							1					15	1	1			**18**
Officers of the Legislature					1												**1**
Panels																	**0**
Regional Health Authorities (Alberta Health Services)		2	9			1			6			17	6	25			**66**
School Districts			4								3	11		1	6		**25**
Universities			3									14	1	16	5		**39**
Other			1			1			3		6	4	1	5	1		**22**
Total	**1**	**7**	**83**	**1**	**1**	**8**	**19**	**3**	**0**	**17**	**0**	**18**	**372**	**37**	**225**	**50**	**842**

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2016 to March 31, 2017

HIA

Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fees	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 & Information Managers (Electronic Medical Record Vendors, Consultants)									3			1		**4**
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians														**0**
Chiropractors								23	3			1		**27**
Dental Hygienists								13						**13**
Dentists								37		1		2		**40**
Denturists														**0**
Government Ministries/Departments								1						**1**
Health Professional Colleges & Associations			1						2					**3**
Health Quality Council of Alberta								1	1					**2**
Hospital Board (Covenant Health)			4			1		1		3		2		**11**
Long Term Care Centres												1		**1**
Midwives														**0**
Minister of Health (Alberta Health)			2					10				55		**67**
Nursing Homes								1				1		**2**
Opticians														**0**
Optometrists								53						**53**
Pharmacies/Pharmacists			5			10		256				9		**280**
Physicians			13			2		241	3	10		38		**307**
Podiatrists								1						**1**
Primary Care Networks								11	6			4		**21**
Regional Health Authorities (Alberta Health Services)			30		1	3		36	1	33		21		**125**
Registered Nurses								17	1			3		**21**
Research Ethics Boards									1					**1**
Researchers														**0**
Subsidiary Health Corporations			3					4				1		**8**
Universities/Faculties of Medicine														**0**
Other							4	1	5	1		3		**14**
Total	**0**	**0**	**58**	**0**	**1**	**16**	**0**	**4**	**707**	**26**	**48**	**0**	**142**	**1002**

Note: The statistics do not include Intake cases.

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

Statistics are from April 1, 2017 to March 31, 2018

PIPA / Entity Type	Advice and Direction	Authorization to Disregard a Request	Complaint	Engage in or Commission a Study	Excuse Fees	Investigation Generated by Commissioner	Notification to OIPC	Offence Investigation	Privacy Impact Assessment	Request Advanced Ruling	Request for Information	Request for Review	Request Time Extension	Self-reported Breach	Total
Accommodation & Food Services			6								4		20		**30**
Admin & Support Services			3								1		6		**10**
Agriculture, Forestry, Fishing & Hunting													1		**1**
Arts, Entertainment & Recreation			5			3		1					7		**16**
Child Day-care Services			2								1		3		**6**
Collection Agencies											1		1		**2**
Construction			5								2		1		**8**
Credit Bureaus			1												**1**
Credit Unions			2								1		14		**17**
Dealers in Automobiles			1								2		2		**5**
Educational Services			2										4		**6**
Finance		1	3					1	1		1		30		**37**
Health Care & Social Assistance			5						1	1	5		10		**22**
Information & Cultural Industries			2							2			10		**14**
Insurance Industry			3								4		22		**29**
Investigative & Security Services			1								1		1		**3**
Legal Services		1	9							1	1		9		**21**
Management of Companies & Enterprises													1		**1**
Manufacturing			4								1		3		**8**
Medical & Diagnostic Laboratories			2								1				**3**
Mining, Oil & Gas			9								6		10		**25**
Motor Vehicle Parts & Accessories													1		**1**
Nursing Homes/Home Health Care										1	1		3		**5**
Private Healthcare & Social Assistance			2										5		**7**
Professional, Scientific & Technical			6						1	1	1		19		**29**
Public Administration										1					**1**
Real Estate, Rental, Leasing			19							1	11		7		**38**
Retail			7							2			27		**36**
Trades/Contractors			4										3		**7**
Transportation											2		3		**5**
Utilities			1												**1**
Wholesale Trade			2										4		**6**
Other			20						1	5	7		15		**48**
Total	**0**	**2**	**126**	**0**	**0**	**3**	**0**	**2**	**4**	**15**	**54**	**0**	**242**	**449**	

Note: The statistics do not include Intake cases.

APPENDIX C: ORDERS AND PUBLIC INVESTIGATION REPORTS ISSUED

Statistics are from April 1, 2017 to March 31, 2018

FOIP Respondent	Orders	Decisions	Public Investigation Reports	Total
Alberta Emergency Management Agency	1			1
Alberta Gaming and Liquor Commission			1	1
Alberta Health Services	5			5
Alberta Occupational Health and Safety Council	1			1
Calgary Police Service	3			3
Children's Services	1			1
City of Calgary	1	1		2
City of Edmonton	1			1
City of Grande Prairie	1			1
Community and Social Services	1			1
Edmonton Police Service	6			6
Environment and Parks	1			1
Executive Council	5			5
Government of Alberta*			1	1
Health	1			1
Justice and Solicitor General	11			11
Keyano College	1			1
Kroll Associates	1			1
Labour	3			3
Peace River School Division No. 10	2			2
Regional Municipality of Wood Buffalo	1			1
Royal Canadian Mounted Police	1			1
Summer Village of West Cove	2			2
Treasury Board and Finance	6			6
University of Alberta	1			1
University of Calgary	3	1		4
Workers' Compensation Board	3			3
Subtotal	63	2	2	67

HIA Respondent	Orders	Decisions	Public Investigation Reports	Total
Alberta Health Services	1		1	2
Dr. Justin C. Sebastia			1	1
Subtotal	1	0	2	3

PIPA Respondent	Orders	Decisions	Public Investigation Reports	Total
Acosta Canada Corporation	1			1
Ascot Garden	1			1
Bishop & McKenzie LLP	1			1
Castledowns Bingo Corporation	1			1
Co-op Taxi	1			1
Harcourt Personnel Inc.	1			1
Kroll Associates	1			1
VitalAire Canada Inc.	1			1
Subtotal	8	0	0	8

Total	72	2	4	78

FOIP Orders: 63 (70 cases)
FOIP Decisions: 2 (2 cases)
FOIP Investigation Reports: 2 (20 cases)
HIA Orders: 1 (25 cases)
HIA Investigation Reports: 2 (4 cases)
PIPA Orders: 8 (8 cases)

*Refers to Investigation Report F2017-IR-03 involving the following Government of Alberta departments: Service Alberta; Executive Council; Aboriginal Relations; Agriculture and Rural Development; Culture and Tourism; Education; Energy; Environment and Sustainable Resource Development; Health; Human Services; Infrastructure; Innovation and Advanced Education; International and Intergovernmental Relations; Jobs, Skills, Labour and Training; Justice and Solicitor General; Municipal Affairs; Seniors; Transportation; Treasury Board and Finance.

Notes:

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

A single Order, Decision or Investigation Report can relate to more than one entity and more than one file.

The number of Orders, Decisions and Investigation Reports are counted by the number of Order, Decision or Investigation Report numbers assigned.

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.

Only those Investigation Reports that are publicly released are reported.

Copies of Orders, Decisions and public Investigation Reports are available on the OIPC web site www.oipc.ab.ca.

www.oipc.ab.ca