Office of the Information and
Privacy Commissioner of Alberta

ANNUAL REPORT
2016-17

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

www.oipc.ab.ca

NOVEMBER 2017

Office of the Information and
Privacy Commissioner of Alberta

November 2017

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, 2016 to March 31, 2017.

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 6

About the Office 9
Mandate 10
Organizational Structure 12
The Process: Request for Review/Complaint 13
OIPC as a Public Body 14
- FOIP Requests to OIPC 14
- OIPC Privacy Matters 14
- Proactive Travel and Expenses Disclosure 16
- Public Sector Compensation Transparency Act 16
- Public Interest Disclosure (Whistleblower Protection) Act 16

Financial Overview 17

Trends and Issues 19
Access and Privacy Education for Children and Youth 20
Solicitor-Client Privilege 21
Ethical Assessments in Big Data Initiatives 22
The Internet of Things, Implications for Connected Healthcare Technology 23
PIPA Review 24

By the Numbers 25
Graph A: Total Cases Opened 27
Graph B: Total Cases Closed 27
Table 1: Cases Opened by Case Type 28
Table 2: Cases Closed by Case Type 29
Table 3: Percentages of Cases Closed by Resolution Method 30
Graph C: Percentages of Cases Closed by Resolution Method 31
Table 4: General Enquiries 31

Regulation and Enforcement 33
Deemed Refusals to Respond to Access Requests 34
Requests for Time Extensions under FOIP 35
Investigation Reports 36
Privacy Breaches 39
Offence Investigations 42
Mediation and Investigation 43
Privacy Impact Assessment Reviews 45
Summary of Significant Decisions 47
Judicial Reviews and Other Court Decisions 51

Education and Outreach 57
Presentations, Forums and Workshops 58
Collaboration with Other Jurisdictions 61
Media Awareness 62

Financial Statements 65

Appendices 77
Appendix A: Cases Opened Under FOIP, HIA, PIPA by Entity Type 78
Appendix B: Cases Closed Under FOIP, HIA, PIPA by Entity Type 81
Appendix C: Orders and Public Investigation Reports Issued 84

Commissioner's Message

In my 2015-16 Annual Report message, I said "access to information in Alberta is fast approaching a crisis situation."

A number of factors led me to make this statement, including:

- A significant increase in the number of time extension requests made to my office;
- A significant increase in the number of deemed refusal files in my office[1];
- The increasingly widespread practice of refusing to provide records to my office for independent reviews and investigations;
- Court challenges by public bodies to my ability to compel the production of records when necessary to complete independent reviews and investigations;
- No concrete action to update and modernize Alberta's access to information legislation;
- Out of date statistics from Service Alberta on the operations of the FOIP Act.

The situation continued into 2016-17.

The OIPC received 253 time extension requests under the FOIP Act – a 150% increase over the 101 submissions received in 2015-16.

We issued 57 deemed refusal orders, 90% of which involved provincial government departments including 44 between Alberta Justice and Solicitor General and Alberta Environment and Parks alone.

The Supreme Court of Canada issued its decision in *Alberta (Information and Privacy Commissioner) v. University of Calgary* in November 2016, finding that the language in Alberta's *Freedom of Information and Protection of Privacy Act* (FOIP Act) was not sufficiently specific to empower me to compel the production of records alleged to be subject to solicitor-client privilege.[2] This decision affected some 80 – 90 cases already before the office.

Public bodies (and provincial government public bodies in particular) continued to withhold information and records requested by my office for reviews and investigations.[3]

In February 2017, I released investigation reports concerning allegations of delay by three provincial government public bodies: Alberta Justice and Solicitor General, Public Affairs Bureau, and Executive Council.

These reports focused attention on what has become an entrenched problem within the Government of Alberta. The reports found the public bodies had seen a significant increase in the volume and complexity of access requests received over a number of years, but process issues and a lack of resources had led to significant delays in responding. Among the most concerning findings were comments relayed to the investigator about the lack of respect for access to information across the Government of Alberta. In a news release associated with the release of the reports, I said "While process management is important, senior leadership must lay the groundwork for a culture that trusts and respects access to information as a cornerstone to good governance."

Overall, 2016-17 was not a good year for access to information in Alberta. However, I am optimistic that 2017-18 will see improvements. I am aware that, during the investigations just mentioned, public bodies adjusted their processes and hired additional staff. Other public bodies have contacted my office to discuss how to improve their administration of the FOIP Act, or have completed internal reviews and are taking steps towards fixing these entrenched problems.

Given this, I am hopeful that next year's Annual Report message will be more positive. But I am also aware that these improvements have occurred only after significant, sustained effort to draw attention to the problem, and there is a great deal more work to be done. Without the culture change I previously spoke of, and a clear commitment to principles of access and openness, it is far too easy to be complacent while access to information – a value that is foundational to informed, engaged democracy – is degraded. There must be a loud and strong commitment, without which these nascent steps will remain fragile and tenuous.

The next five years...

In February 2017, I was honored to be appointed to a second five-year term as Information and Privacy Commissioner of Alberta.

I am very proud of what my colleagues in the office have accomplished over the last five years, which has been a time of significant change. We are acutely aware of the role and importance of data and information in today's economy and society, and the myriad of challenges – including those posed by technology, changing social norms, economic and budgetary constraints, and citizen expectations.

In 2011-12, the office opened 1,288 files, closing 1,320. In 2016-17, we opened 2,239 – a 74% increase – and closed 2,061, an increase of 56%. We are clearly more efficient, though we are not able to stay ahead of demand. Over the last five years we have, among other things, restructured the office and reviewed processes from the ground up. We introduced a new case management system, updated and modernized our website, and have embarked on other multi-year initiatives to, for example, improve our records and information management systems and processes to support and facilitate a shift toward providing improved electronic services to the public and regulated stakeholders.

We will continue to review and refine our processes over the next few years, and will revisit our Strategic Business Plan to make sure we are on the right path. In the meantime, I would like to thank my colleagues at the OIPC for their hard work, patience and dedication. It is a real privilege and profoundly rewarding to work with you to uphold Alberta's access and privacy rights.

Jill Clayton
Information and Privacy Commissioner

[1] A deemed refusal is when an applicant has made an access request and has not received any response within the legislated timelines.

[2] In April 2017, I tabled *Producing Records to the Commissioner: Restoring Independent and Effective Oversight under the FOIP Act, A Special Report and Request for Legislative Amendment* in the Legislative Assembly, requesting specific amendments to the FOIP Act to address the court's concerns. To date, I have not received any formal response to the Special Report.

[3] In April 2017, I tabled the report of my investigation into alleged delays in the Government of Alberta's handling and response to access requests. Due to the challenges of obtaining information for the investigation, and the role Alberta Justice played in the investigation, I said the report's findings were "unreliable".

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 approximately 1,116 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 Netcare, the provincial electronic health record system.

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 individuals to have their 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 of requests to review 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 research purposes, record linkages or for the purpose of performing data matching

VISION

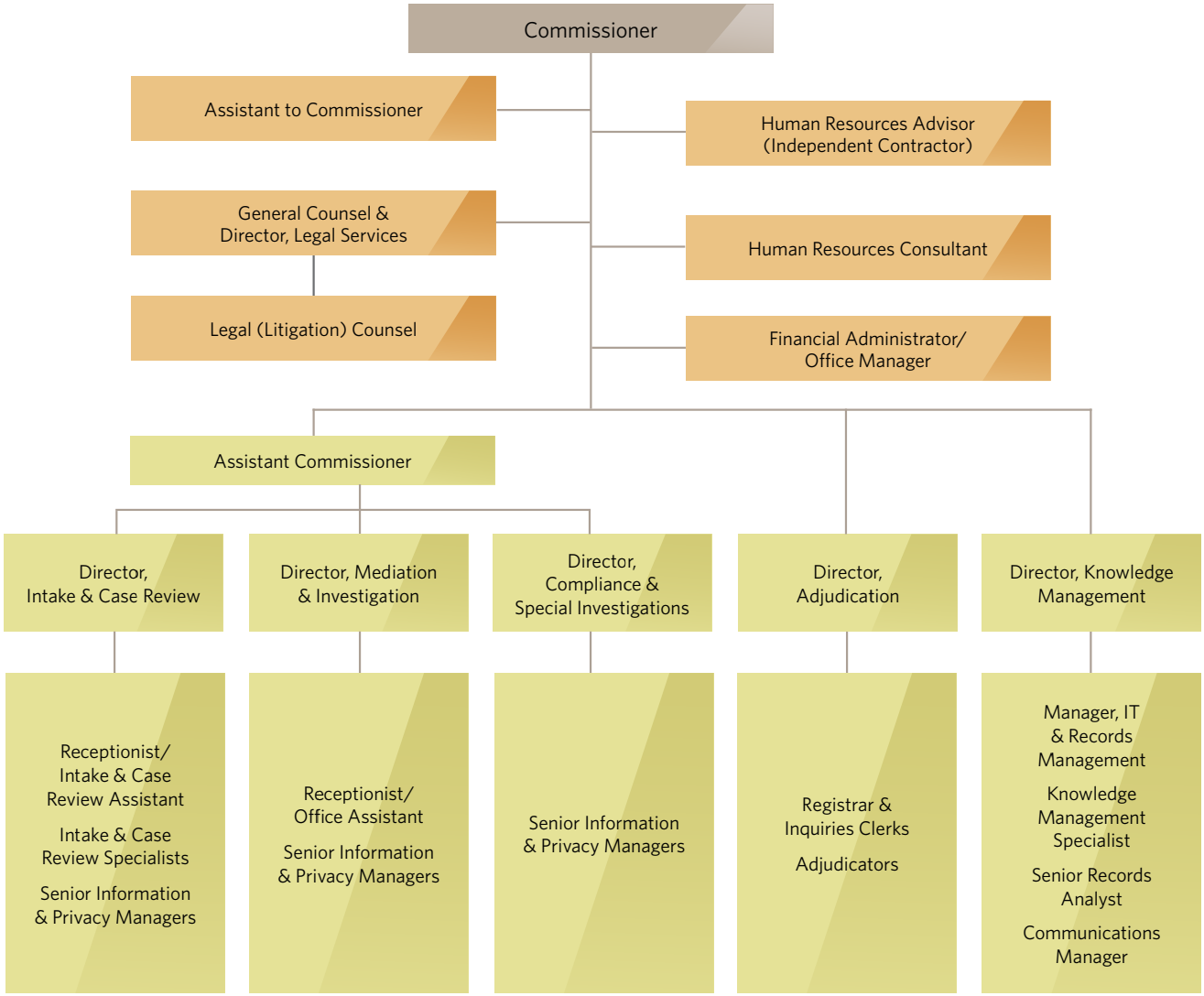
A society that values and respects access to information and personal privacy.

MISSION

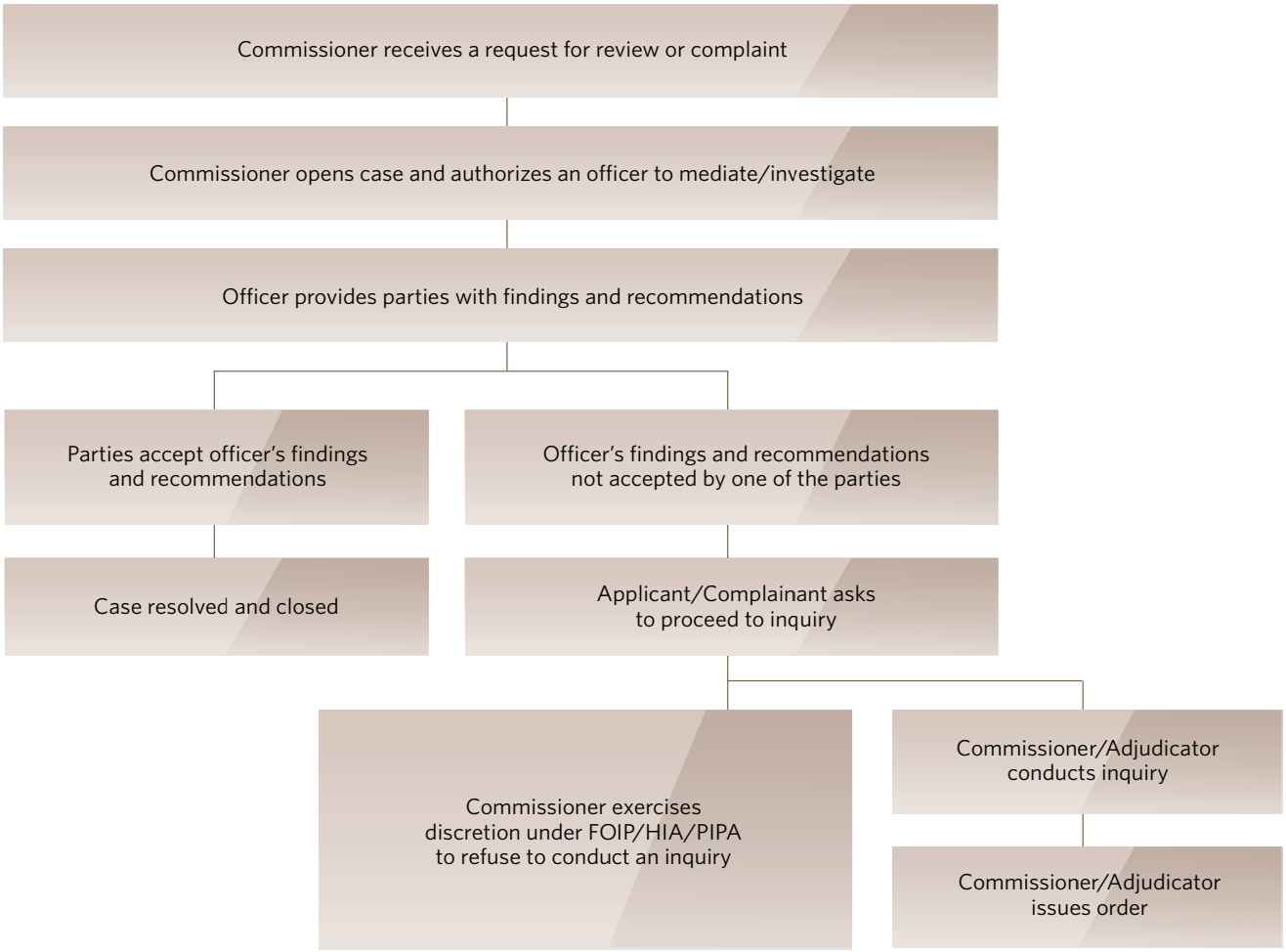
Our work toward supporting our vision includes:

- Advocating for the privacy and access 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 2016-17



The Process: Request for Review/Complaint



OIPC as a Public Body

FOIP REQUESTS TO THE OIPC

As a public body under the FOIP Act, the OIPC on occasion receives access requests from applicants. 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)).

In 2016-17, the OIPC received five general information requests under the FOIP Act, and one informal request for information. The OIPC responded to all of the requests within 30 days.

There is one outstanding matter related to a general information request made to the OIPC. An External Adjudicator has been designated by Order-in-Council to determine whether the OIPC properly excluded records subject to an access request after the applicant requested a review of the OIPC's decision.

Another matter was resolved by Adjudication Order No. 10 which was issued on June 28, 2016, and is available at www.oipc.ab.ca. The External Adjudicator determined that the OIPC had properly excluded records because the requested records related to the exercise of the Commissioner's functions under the FOIP Act.

OIPC PRIVACY MATTERS

In 2016-17, the OIPC conducted seven investigations into internal incidents involving potential privacy breaches.

Incident 1

Courier mail was delivered to the OIPC front reception desk. Following standard procedure, the mail was opened, date stamped and logged. During this process it was realized that one piece of mail was a confidential letter addressed to the Commissioner that should not have been opened. The OIPC investigation determined that while the contents of the letter had been viewed, there was no use or disclosure of the information. To further mitigate the risk of inappropriate disclosure, staff involved signed a letter attesting that they had not disclosed the contents of the letter and committing to not disclosing the contents of the letter in the future.

The steps taken to contain and mitigate the incident reduced the risk to a level that did not present a real risk of significant harm to any individual; therefore no notification was provided. Staff were reminded of the importance to ensure confidential mail is only opened by the person to whom it is addressed.

Incident 2

A memory stick a public body said it sent to the OIPC could not be located. The memory stick contained records related to an access request and an OIPC request for review file. The public body said that it included the memory stick in a letter (contained within an envelope) sent to the OIPC's office in Calgary. The letter was received and logged in the OIPC mail log. The log did not note whether the envelope contained a memory stick. The staff that opened the letter and made the mail log entry did not see a memory stick.

The documents contained on the missing memory stick included personal information, with a low to moderate level of risk if the information was accessed outside of the OIPC. The investigation concluded that the memory stick was either not provided to the OIPC, or if it was, it would have been securely destroyed as all envelopes received by the OIPC are securely shredded, thus limiting the risk of a privacy breach.

Incident 3

A fax regarding an OIPC request for review file was sent to a fax machine at a complainant's place of work rather than her home. OIPC staff assumed that the fax number provided on the form was the complainant's personal fax number when it was actually her work fax number. The fax included the name and address of the complainant and revealed that she had made a complaint to the OIPC and that her complaint was being held in abeyance.

The investigation determined that the affected individual was at low risk of hurt and humiliation. The personal information was sent to the individual's place of work where she received the only copy. Despite the low risk, notification was provided to the individual via phone call.

Incident 4

A security company brought a Government of Alberta (GoA) courier bag containing the OIPC's outgoing mail to the OIPC front reception desk. The bag had been found in the alley behind the OIPC's office building.

Surveillance video confirmed that the GoA courier dropped the bag where it was found and drove off without loading it into the vehicle. The video was not able to confirm whether anybody accessed the bag while it was in the alley.

The contents of the bag were reviewed, and on a balance of probabilities, it was determined that no correspondence was missing. There was no log of what was placed in the bag so there was no certainty whether correspondence was missing, but given the small amount of time the bag was in the alley, and the OIPC review of the returned bag's contents, the risk that something was missing was deemed to be minimal.

The GoA courier supervisor was contacted and advised of the incident. Individuals were not notified as there was no real risk of significant harm.

Incident 5

Correspondence was sent to a complainant's address listed in the OIPC electronic case management system. When the complainant's submission was not received by the due date, OIPC staff called the complainant and learned that the notice had been sent to the complainant's former address and therefore had not been received. The complainant was not concerned as he believed the mail would still sit in the locked community mail box. All attempts made by both the complainant and Canada Post to retrieve the notice were unsuccessful.

The notice contained detailed personal and health information about the complainant. There is no reason to believe the envelope containing the notice was opened and the information exposed, but if the information was exposed, there is risk that an individual with intent to cause harm could use the information for purposes of identity theft or fraud, or possibly hurt or humiliation.

The complainant was informally notified as soon as the incident was discovered and was engaged with the OIPC in addressing this matter from the outset. The investigation concluded that the breach presented a real risk of significant harm, and notification was formally provided to the complainant.

The OIPC also reviewed its procedures for updating the electronic system, with a view to mitigate the risk of a similar incident recurring.

Incident 6

An individual asked the OIPC a question relating to a fax. In order to respond, the OIPC followed up with a third party service provider and inadvertently included the name of the individual and their email address in an email communication to the service provider. This error was quickly recognized and steps were taken on the same day to ensure the service

provider deleted the email and did not act on it. The service provider subsequently confirmed to the OIPC that the email was deleted from its system.

The investigation concluded that the risk to the individual was low. The breach was contained and there was no real risk of harm. Therefore, no notification was provided to the individual.

Incident 7

The OIPC sent an email containing an inquiry submission extension request response letter to an incorrect email address. The individual who received the email in error contacted the OIPC to advise that it should not have been sent to him. The individual was asked to delete the email and on that same day he verbally confirmed that he had deleted the email.

The error was made as a result of using the Microsoft Outlook auto-complete list feature that remembers email addresses, and the OIPC staff did not notice that an incorrect address had been posted in the "To" field.

The information sent with the email included the individual's name and mailing address, revealed he had a matter before the OIPC, and to whom the matter related. The risk was partly mitigated by verbal confirmation from the recipient that the email was deleted; nonetheless, the information was viewed. Although the investigation concluded that there was no real risk of significant harm, formal notification was provided to the individual.

The incident was addressed at a staff meeting to remind staff of OIPC policies and to ensure correct email addresses are used.

PROACTIVE TRAVEL AND EXPENSES DISCLOSURE

The OIPC continues to publicly disclose 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

By June 30, 2016, the *Public Sector Compensation Transparency Act* required public sector bodies, including the OIPC, to publicly disclose compensation and severance provided to an employee if it was more than $125,000 in the 2015 calendar year. In addition, other non-monetary employer-paid benefits and pension were to be reported.

In preparation for the disclosure requirements, the OIPC completed its first access impact assessment, which helped to develop *Access Impact Assessment Guidelines for Proactive Disclosure* published in September 2016.

The compensation disclosure, access impact assessment, and guidelines are available at www.oipc.ab.ca.

This disclosure will be made annually by June 30 and the threshold for disclosure will be adjusted annually, according to legislation.

PUBLIC INTEREST DISCLOSURE (WHISTLEBLOWER PROTECTION) ACT

No disclosures under the *Public Interest Disclosure (Whistleblower Protection) Act* were received by the OIPC's designated officer in 2016-17.

Financial Overview

For the 2016-17 fiscal year, the total approved budget for the OIPC was $6,857,391, including $35,000 for capital asset purchases. The actual total cost of operating expenses and capital purchases was $6,716,346. The OIPC returned $141,045 (2.06% of the total approved budget) to the Legislative Assembly.

TOTAL ACTUAL COSTS COMPARED TO BUDGET

	VOTED BUDGET	ACTUAL	DIFFERENCE
Operating Expenses*	$ 6,822,391	$ 6,644,235	$ 178,156
Capital Purchases	35,000	72,111	-37,111
Total	$ 6,857,391	$ 6,716,346	$ 141,045

*Amortization is not included

Salaries, wages, and employee benefits make up approximately 80% of the OIPC's operating expenses budget. In 2016-17, payroll related costs were approximately $4,700 over budget. Legal fees were under budget approximately $210,000 due to a Supreme Court of Canada hearing which was unexpectedly scheduled on April 1, 2016 (as a result, costs were incurred in the 2015-16 fiscal year, not 2016-17 as budgeted). Other contract services were under budget $32,000, and various supplies and services were under budget a net of approximately $13,000. External adjudication for three inquiries was over budget approximately $72,000 due to additional records provided for review. Capital purchases were $37,111 over budget due to purchasing a new network storage device that was approaching end of life.

TOTAL ACTUAL COSTS COMPARED TO PRIOR YEAR

	2016-17	2015-16	DIFFERENCE
Operating Expenses	$ 6,644,235	$ 6,838,446	$ -194,211
Capital Purchases	72,111	0	72,111
Total	$ 6,716,346	$ 6,838,446	$ -122,100

Total costs for operating expenses and equipment purchases, including capital assets, decreased by approximately $122,000 from the prior year. The reduction was primarily due to a decrease in legal fees of approximately $325,000 as well as costs for technology services, hosting/working sessions, travel and advertising. These decreases were offset by an increase in salaries, wages, and employee benefits of $36,555, and other contract services, including external adjudication. There was also an increase of $72,111 for capital expenditures in the current year.

TRENDS & ISSUES

This section highlights provincial, national and international issues and trends that shape and influence the access and privacy landscape in Alberta.

Access and Privacy Education for Children and Youth

In 2016-17, there was significant discussion in a variety of forums on the topic of educating students about access and privacy issues and rights. A general consensus seems to have emerged: students require skills and knowledge to safely navigate their networked world, and to understand how to uphold information and privacy rights in the digital economy. While the solutions are less clear, a few initiatives to enhance education and raise awareness are gaining momentum.

One example is The eQuality Project, which entered its second year in 2016-17. The eQuality Project is a seven-year research project with a number of objectives, including to create new knowledge about commercial data practices and their impact on youth as well as the ways in which young people conceptualize privacy, to share this new knowledge with policy makers and the public, and to create educational materials to help young Canadians make the most of their digital media experiences.

The project was granted funding from the Social Sciences and Humanities Research Council of Canada, and is a partnership of scholars, research and policy groups, community organizations, educators, policymakers and youth. The OIPC supports The eQuality Project by helping to inform stakeholders about research findings and raising awareness of information and privacy rights. This included co-hosting an event in January 2017 with The eQuality Project and the Alberta Teachers' Association – an official partner of the project – to discuss "Privacy Implications of the Networked Classroom" with researchers, Alberta school administrators and teachers, and access and privacy professionals.

At an international level, the "Personal Data Protection Competency Framework for School Students" was adopted by data protection authorities at the 38th International Data Protection and Privacy Commissioners' conference in Morocco in October 2016. Based on nine foundational principles, the framework is a set of learning principles and competencies specifically dedicated to data protection, for use in official school programs and in training courses for educators. The framework was deliberately designed to have an international dimension and is intended to be adapted to address specific educational purposes, laws and data protection approaches relevant to each country. The framework is available at www.oipc.ab.ca.

In Alberta, the provincial government has announced a six-year curriculum review process. Alberta Education has committed to a public consultation process to help determine the learning outcomes for Alberta's students. The OIPC believes it is important to inform the curriculum working groups about the initiatives Information and Privacy Commissioners across Canada and worldwide have undertaken to educate students on privacy rights as they grow and live in the digital economy. As of March 31, 2017, plans were being discussed for the Commissioner to present to Alberta's curriculum working groups.

Solicitor-Client Privilege

On November 25, 2016, the Supreme Court of Canada issued its decision in *Alberta (Information and Privacy Commissioner) v. University of Calgary,*[4] finding that the FOIP Act does not empower the Commissioner to compel production of records in order to determine whether solicitor-client privilege has been properly claimed over records sought in an access to information request.[5]

In 2016-17, the OIPC issued five orders that dealt with claims of solicitor-client privilege. In one case (P2017-02), the respondent organization provided the record claimed to be subject to solicitor-client privilege to the Adjudicator for her review. The Adjudicator found the organization had properly claimed solicitor-client privilege as an exception to access and did not have to disclose the record.

In two other cases (F2016-63 and F2017-28, involving Alberta Human Services, and what is now Alberta Children's Services, respectively), the respondent public bodies did not provide copies of the records at issue; however, they provided sufficient evidence and argument to support their claims that solicitor-client privilege applied. In both cases, the Adjudicator found the public bodies properly claimed solicitor-client privilege. In Order F2017-28 in particular, the Adjudicator noted that information provided by Alberta Children's Services was a good example of how to support a claim for privilege without providing the records to the Adjudicator or revealing the legal advice.

In two other cases (F2016-31 and F2016-35, involving Alberta Justice and Solicitor General and Calgary Police Service, respectively) the public bodies did not provide the records at issue to the Adjudicators for review, but did provide argument and affidavit evidence to support claims that solicitor-client privilege applied. In both cases, the Adjudicators found that evidence provided by the public bodies was insufficient to establish that the exception applied. Alberta Justice and Solicitor General was ordered to review the relevant records at issue and respond to the applicant and the Adjudicator without relying on solicitor-client privilege. Calgary Police Service was ordered to disclose the records to the applicant. Calgary Police Service has applied for judicial review of Order F2016-35.

These cases are a reminder that, under the FOIP Act and PIPA, the burden rests with a public body or organization to demonstrate that exceptions apply to information in records that are the subject of an access request, such that they might be withheld from an applicant. As per the OIPC's *Solicitor-Client Privilege Adjudication Protocol,* published in 2008, the OIPC will accept evidence about the records, in lieu of the records themselves, where that evidence is sufficient to support a claim of solicitor-client privilege.

In December 2016, following the decision by the Supreme Court of Canada, the OIPC published an updated "Privilege Practice Note". The Practice Note states that claims of solicitor-client privilege or litigation privilege will require an affidavit of records, including a schedule listing the records (or bundle of records) for which privilege is claimed, along with the description for each record or bundle. The Practice Note also sets out the test to be met for each claim of privilege. The description for each record (or each bundle) must be sufficient to meet that test, without revealing the privileged information.

[4] 2016 SCC 53

[5] In April 2017, the Commissioner tabled *Producing Records to the Commissioner: Restoring Independent and Effective Oversight under the FOIP Act, A Special Report and Request for Legislative Amendment* in the Legislative Assembly, requesting specific amendments to the FOIP Act to empower the Commissioner to compel the production of records when necessary to perform legislative functions (such as when a public body does not provide enough evidence to satisfy the Commissioner that the records are privileged).

Ethical Assessments in Big Data Initiatives

Beyond information and privacy laws, important questions concerning the ethics of big data initiatives are being discussed, debated, and acted upon. A number of initiatives in 2016-17 illustrate this trend and suggest that current conversations are just the beginning.

In February 2017, the Information Accountability Foundation (IAF) released its *Report for the Big Data Assessment for Canadian Private Sector Organizations Project.* The IAF received a grant from the 2016-17 Contributions Program of the Office of the Privacy Commissioner of Canada "to create for the Canadian context an assessment process … to determine whether big data undertakings are legal, fair and just … and to identify the elements necessary for an assessment framework to fit into a code of conduct or practice that might be enforceable by Canadian governmental regulatory agencies…".

The purpose of the framework is in part to raise "additional considerations that may not be covered in a typical privacy impact assessment" by looking more broadly at human rights and interests when mitigating individuals' risks in a big data project, such as limiting algorithmic discrimination against certain individuals or groups of people.

While the legal framework discussed within the assessment framework is the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), the values it espouses are applicable in other private sector privacy legal frameworks, or may be applied in the public and health sectors, depending on the purpose and scope of a project.

The OIPC Alberta submitted comments on the draft framework and the Commissioner participated in a multi-stakeholder session held in Toronto in December 2016 at which the draft framework was evaluated, along with representatives from academia, civil society, and participating companies. The framework is available at www.informationaccountability.org.

Also on the topic of the ethics of Big Data initiatives, as of the end of the 2016-17 fiscal year, the Commissioner had accepted an invitation from the United Nations Initiative Global Pulse and the IAPP to participate as a panelist at an expert meeting on *"Building a Strong Privacy and Data Ethics Program: From Theory to Practice"* at the UN Headquarters in New York. The meeting's focus will be the implementation of privacy and data ethics in international organizations, as well as public-private sector data access for humanitarian and development causes.

In 2016, the United Nations' Global Pulse initiative published its "Data Innovation for Development Guide: Data Innovation Risk Assessment Tool", which is the first step in a two part data privacy, ethics and data protection compliance mechanism for understanding and managing risks, harms and benefits associated with big data use in development and humanitarian contexts. The tool is a checklist meant primarily for projects led by international development and humanitarian organizations, but may be applicable in other contexts as well.

The Internet of Things, Implications for Connected Healthcare Technology

In October 2016, a "massive and sustained internet attack" caused outages and network congestion for much of the east coast of the United States. The attack was "launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders".[6]

In some ways, the attack was not a surprise. One article noted that "people have been worried for a long time about the security implications of networking more and more physical devices."[7] Another reported "[w]e're at the frontier of an era in which everyday objects — baby monitors, home appliances and even medical devices — come with built-in web connections".[8] Further, "...the problem is quickly expanding: Cisco estimates that the number of such devices could reach 50 billion by 2020, from 15 billion today. Intel puts the number at roughly 200 billion devices in the same time frame. (Assuming the global population is around 7.7 billion people in 2020, that would be about six to 26 devices per person.)"[9]

The health care sector could be particularly at risk. As health custodians continue to promote, invest in and move towards health information portals that allow patients to access their own information, and more personal health devices are networked and available to consumers, questions regarding information flows and device security are front and centre. For example, health information collected by network-connected pacemakers, blood pressure monitors or exercise trackers may be transferred to patient health portals in order for doctors and patients to monitor progress or to identify certain medical interventions for different conditions. Closing vulnerability loopholes when, unlike a computer or phone, users are not prompted to update devices and the onus to secure these devices is on the individual who may not have the technical awareness to do so, are among the issues to be addressed.

These issues and others were the subject of discussion at the "Canada-US Connected Health Workshop" held in Washington, DC in December 2016. The Commissioner was invited to participate in a panel discussion with policymakers, regulators and representatives from the private sector that manufacture mobile health devices. The panel focused on the regulatory challenges posed by connected and mobile health technologies and big data, as well as identifying opportunities for cross-border regulatory cooperation.

[6] "Hacked Cameras, DVRs Powered Today's Massive Internet Outage", https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

[7] "The Lessons of the East Coast Cyberattack", http://www.slate.com/articles/technology/future_tense/2016/10/was_the_ddos_attack_on_dyn_actually_that_scary.html

[8] "Unregulated 'internet of things' industry puts us all at risk, security experts say", http://www.cbc.ca/news/technology/internet-ddos-attack-analysis-1.3820297

[9] "A New Era of Internet Attacks Powered by Everyday Devices", https://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html

PIPA Review

In June 2015, the Standing Committee on Alberta's Economic Future was given the task of reviewing the *Personal Information Protection Act* (PIPA) and its regulation. A comprehensive review of the legislation by an all-party special committee of the Legislative Assembly is a statutory requirement of PIPA.

During the review, which started in July 2015, the Committee issued a Discussion Guide, opened a consultation process and invited feedback from stakeholders and members of the public. The Committee received 36 written submissions and heard 11 oral presentations. The Commissioner appeared before the Committee three times and submitted a written report setting out ideas, suggestions and 10 recommendations for ensuring Alberta remains a leader in private sector privacy legislation across Canada and internationally. The report is available at www.oipc.ab.ca.

The Committee met on October 6, 2016 to deliberate the issues and proposals before it. As outlined in the Committee's October 2016 Final Report, the deliberations resulted in the following recommendation:

> That the Act be amended in section 56 to clarify the definition of a commercial activity.

No amendments have been proposed as of March 31, 2017.

BY THE NUMBERS

Totals Open/Closed

(excluding Intake cases)

2,239

FILES OPENED, 37% INCREASE OVER 2015-16

2,061

FILES CLOSED, 32% INCREASE OVER 2015-16

Self-Reported Breaches

342

FILES OPENED, 10% INCREASE OVER 2015-16

356

FILES CLOSED, 25% INCREASE OVER 2015-16

Requests for Review under FOIP

430

FILES OPENED, 69% INCREASE OVER 2015-16

352

FILES CLOSED, 21% INCREASE OVER 2015-16

Requests for Time Extensions under FOIP

253

150% INCREASE OVER 2015-16

Orders

105

ORDERS ISSUED, 64% INCREASE OVER 2015-16

57 OF WHICH WERE "DEEMED REFUSAL" ORDERS

Privacy Impact Assessments under HIA

583

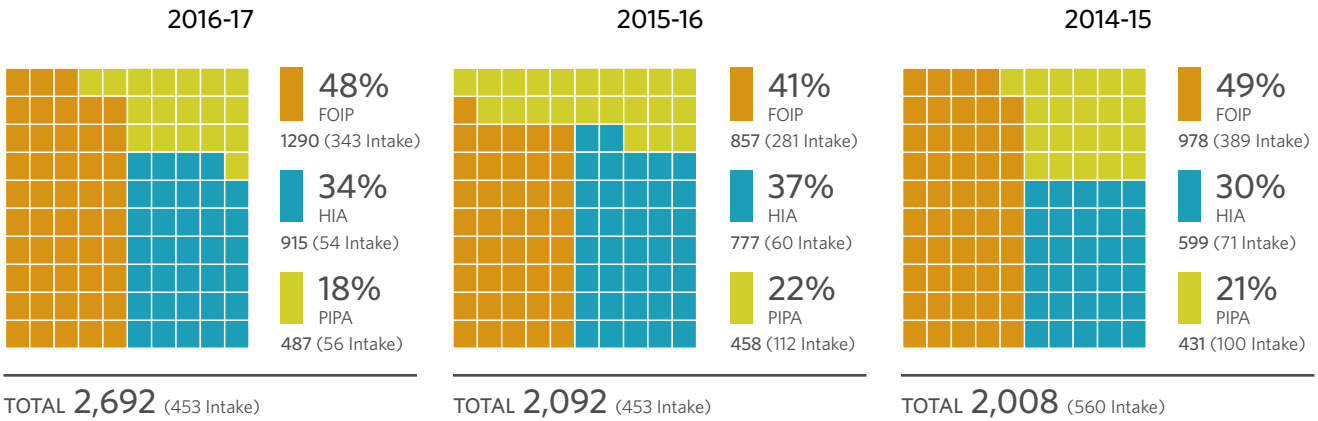
FILES OPENED, 37% INCREASE OVER 2015-16

548

ACCEPTED, 44% INCREASE OVER 2015-16

GRAPH A: TOTAL CASES OPENED

Three Year Comparison



GRAPH B: TOTAL CASES CLOSED

Three Year Comparison

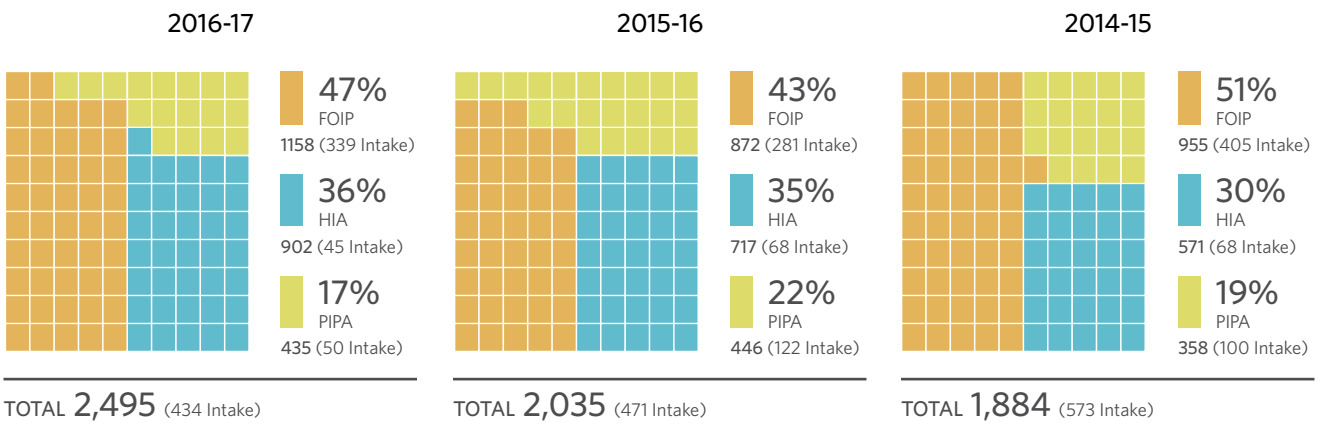


TABLE 1: CASES OPENED BY CASE TYPE

FOIP	2016-2017	2015-2016	2014-2015
Advice and Direction	2	0	0
Authorization to Disregard a Request	10	3	7
Complaint	92	78	85
Disclosure to Commissioner (Whistleblower)	0	0	1
Engage in or Commission a Study	0	0	0
Excuse Fees	10	10	7
Investigation Generated by Commissioner	27	13	23
Notification to OIPC	3	7	8
Offence Investigation	1	0	2
Privacy Impact Assessment	23	22	12
Request Authorization to Indirectly Collect	1	0	0
Request for Information	23	14	24
Request for Review	430	255	294
Request for Review 3rd Party	22	35	22
Request Time Extension	253	101	63
Self-reported Breach	50	38	41
Subtotal	**947**	**576**	**589**
Intake cases	343	281	389
Total	**1290**	**857**	**978**

HIA	2016-2017	2015-2016	2014-2015
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	1	1
Complaint	70	72	39
Engage in or Commission a Study	0	0	0
Excuse Fees	1	0	1
Investigation Generated by Commissioner	2	28	28
Notification to OIPC	0	0	0
Offence Investigation	7	1	2
Privacy Impact Assessment	583	427	341
Request for Information	37	33	24
Request for Review	30	26	16
Request Time Extension	1	0	0
Self-reported Breach	130	129	76
Subtotal	**861**	**717**	**528**
Intake cases	54	60	71
Total	**915**	**777**	**599**

PIPA	2016-2017	2015-2016	2014-2015
Advice and Direction	0	0	0
Authorization to Disregard a Request	2	2	0
Complaint	159	129	121
Engage in or Commission a Study	0	0	0
Excuse Fees	0	0	0
Investigation Generated by Commissioner	6	5	7
Notification to OIPC	0	0	0
Offence Investigation	2	1	0
Privacy Impact Assessment	5	3	3
Request for Advance Ruling	0	0	0
Request for Information	17	8	9
Request for Review	78	54	52
Request Time Extension	0	0	1
Self-reported Breach	162	144	138
Subtotal	**431**	**346**	**331**
Intake cases	56	112	100
Total	**487**	**458**	**431**

Notes

(1) See Appendix A for a complete listing of cases opened in 2016-17.

(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	2016-2017	2015-2016	2014-2015
Advice and Direction	2	0	0
Authorization to Disregard a Request	4	4	4
Complaint	69	76	117
Disclosure to Commissioner (Whistleblower)	0	0	0
Engage in or Commission a Study	0	0	0
Excuse Fees	8	6	25
Investigation Generated by Commissioner	15	4	7
Notification to OIPC	3	7	8
Offence Investigation	0	0	0
Privacy Impact Assessment	24	18	16
Request Authorization to Indirectly Collect	1	0	0
Request for Information	21	12	29
Request for Review	352	292	230
Request for Review 3rd Party	23	31	24
Request Time Extension	251	93	64
Self-reported Breach	46	48	26
Subtotal	**819**	**591**	**550**
Intake cases	339	281	405
Total	**1158**	**872**	**955**

HIA	2016-2017	2015-2016	2014-2015
Advice and Direction	0	0	0
Authorization to Disregard a Request	0	1	1
Complaint	48	39	42
Engage in or Commission a Study	0	0	0
Excuse Fees	0	1	0
Investigation Generated by Commissioner	25	16	18
Notification to OIPC	0	0	0
Offence Investigation	1	1	1
Privacy Impact Assessment	576	415	340
Request for Information	37	33	21
Request for Review	23	31	9
Request Time Extension	1	0	0
Self-reported Breach	146	112	71
Subtotal	**857**	**649**	**503**
Intake cases	45	68	68
Total	**902**	**717**	**571**

PIPA	2016-2017	2015-2016	2014-2015
Advice and Direction	0	0	0
Authorization to Disregard a Request	3	0	2
Complaint	121	111	114
Engage in or Commission a Study	0	0	0
Excuse Fees	0	0	0
Investigation Generated by Commissioner	9	6	12
Notification to OIPC	0	0	0
Offence Investigation	1	0	0
Privacy Impact Assessment	4	4	3
Request for Advance Ruling	0	0	0
Request for Information	16	8	6
Request for Review	67	70	44
Request Time Extension	0	0	1
Self-reported Breach	164	125	76
Subtotal	**385**	**324**	**258**
Intake cases	50	122	100
Total	**435**	**446**	**358**

Notes

(1) See Appendix B for a complete listing of cases closed in 2016-17.

(2) A listing of all privacy impact assessments accepted in 2016-17 is available on the OIPC website: 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 for those case types that can proceed to Inquiry (Request for Review, Request for Review 3rd Party, Request to Excuse Fees, and Complaint files).

RESOLUTION METHOD	NUMBER OF CASES (FOIP)	NUMBER OF CASES (HIA)	NUMBER OF CASES (PIPA)	TOTAL	%
Resolved by Mediation/Investigation	326	64	165	555	78%
Resolved by Order or Decision	95	3	7	105	15%
Resolved by Commissioner's Decision to Refuse to Conduct an Inquiry	8	3	10	21	3%
Withdrawn during Inquiry Process	4	0	5	9	1%
Discontinued during Inquiry Process	19	1	1	21	3%
Total	452	71	188	711	100%

FOIP Orders: 95 (99 cases); **HIA Orders:** 3 (3 cases); **PIPA Orders:** 7 (7 cases)

NOTES:

(1) This table includes only the Orders and Decisions issued that concluded/closed the file. No Decisions were issued in 2016-17. See Appendix C for a list of all Orders and Public Investigation Reports issued in 2016-17. A copy of all Orders, Decisions and Public Investigation Reports are available on the OIPC website www.oipc.ab.ca

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

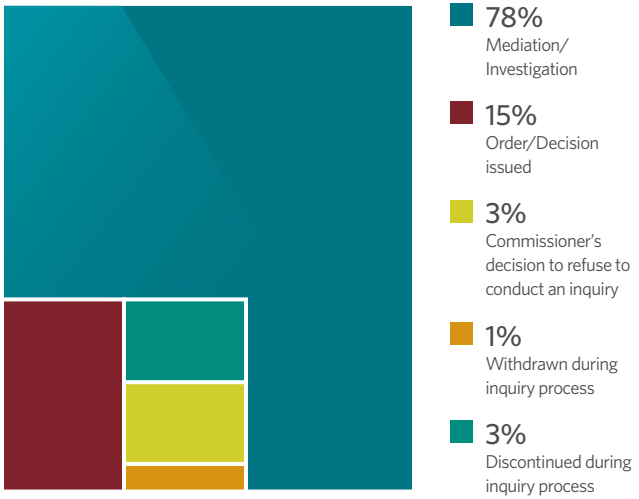
(3) Eight FOIP case files were closed by four Orders (i.e. two case files were closed per Order).

(4) Discontinued during the inquiry process includes three case files (FOIP, HIA, PIPA) that were discontinued before a decision was made to hold an inquiry.

(5) 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.

(6) This table does not include the Commissioner's decision to refuse to conduct an inquiry in relation to one of the two organizations named in the complainant's Request for Inquiry. As an inquiry was confirmed to proceed involving the other organization named in the complaint, the file was not closed by the decision to refuse to conduct an inquiry.

GRAPH C:
PERCENTAGE OF CASES CLOSED BY RESOLUTION METHOD



Of the **711** cases that could proceed to Inquiry:
19% were resolved within 90 days;
28% were resolved within 91-180 days;
53% were resolved in more than 180 days

TABLE 4: GENERAL ENQUIRIES

TELEPHONE CALLS		
FOIP	Number	Percentage
Public Bodies	178	31%
Individuals	389	69%
Total	567	100%

HIA	Number	Percentage
Custodians	295	48%
Individuals	324	52%
Total	619	100%

PIPA	Number	Percentage
Organizations	347	29%
Individuals	864	71%
Total	1211	100%

Emails FOIP/HIA/PIPA	259
Non-jurisdictional	188
Overall Total	2844

REGULATION & ENFORCEMENT

Deemed Refusals to Respond to Access Requests

Under a new process established in 2015-16, the OIPC streamlines requests for review to inquiry when a public body, custodian or organization acknowledges receipt of an applicant's access request but does not respond to the applicant within the time limits set out in the FOIP Act, HIA or PIPA, respectively.

There were five orders issued under this process in 2015-16 – four to Alberta Justice and Solicitor General and one to Alberta Environment and Parks.

The use of this process significantly increased in 2016-17. There were 57 deemed refusal orders issued by the OIPC. Nearly 90% (50) were issued to government departments, primarily Alberta Justice and Solicitor General and Alberta Environment and Parks which combined for 44 deemed refusal orders.

In each FOIP case, the public body acknowledged that it had not yet responded to the applicant. In a limited number of the orders, the public body responded during the inquiry. However, for the vast majority the Adjudicators ordered the public body to respond to the access request as required by the FOIP Act.

In addition, there were eight deemed refusal inquiries discontinued during the inquiry process because the public body responded to the access request. In each of these eight cases, applicants either advised the OIPC that they did not wish to continue with the inquiry or failed to respond to the OIPC's letter asking if they wanted the inquiry to continue only on the timeliness issue.

There was also one deemed refusal inquiry withdrawn by the applicant. In that case, the public body responded during the inquiry process and the applicant withdrew the request for an inquiry.

LIST OF DEEMED REFUSAL ORDERS ISSUED IN 2016-17

Alberta Justice and Solicitor General

1. ..... F2017-35
2. ..... F2017-34
3. ..... F2017-33
4. ..... F2017-32
5. ..... F2017-31
6. ..... F2017-26
7. ..... F2017-13
8. ..... F2017-09
9. ..... F2017-08
10. ..... F2017-07
11. ..... F2017-06
12. ..... F2017-05
13. ..... F2016-54
14. ..... F2016-53
15. ..... F2016-52
16. ..... F2016-50
17. ..... F2016-49
18. ..... F2016-48
19. ..... F2016-47
20. ..... F2016-46
21. ..... F2016-45
22. ..... F2016-44
23. ..... F2016-43
24. ..... F2016-42
25. ..... F2016-22
(related to F2016-23: Alberta Human Rights Commission)
26. ..... F2016-17
27. ..... F2016-12
28. ..... F2016-11

Alberta Environment and Parks

29. ..... F2017-30
30. ..... F2017-25
31. ..... F2017-24
32. ..... F2017-23
33. ..... F2017-22
34. ..... F2017-21
35. ..... F2017-20
36. ..... F2017-19
37. ..... F2017-18
38. ..... F2017-17
39. ..... F2017-16
40. ..... F2017-15
41. ..... F2016-38
42. ..... F2016-37
43. ..... F2016-36
44. ..... F2016-30

Executive Council

45. ..... F2017-12
46. ..... F2016-29
47. ..... F2016-28

Service Alberta

48. ..... F2017-11
49. ..... F2017-10

Alberta Economic Development and Trade

50. ..... F2017-29

Alberta Human Rights Commission

51. ..... F2016-23
(related to F2016-22: Alberta Justice and Solicitor General)

Edmonton Catholic Separate School District

52. ..... F2016-15
53. ..... F2016-14

City of Edmonton

54. ..... F2017-27

University of Calgary

55. ..... F2016-59

Dr. Adeleye Adebayo

56. ..... H2016-04

Lundgren & Young Insurance Ltd.

57. ..... P2016-04

Requests for Time Extensions under FOIP

The increase in deemed refusal orders aligned with a significant increase in requests for time extensions submitted by public bodies to the OIPC under the FOIP Act, most of which were also submitted by government departments.

There were 253 requests for time extensions received in 2016-17, representing a 150% increase from 2015-16 (101).

Of the 253 time extension requests received in 2016-17:

- 73% were made by provincial government departments
- 10% were made by other public bodies, including the Alberta Electric System Operator, Balancing Pool, Residential Tenancies Dispute Resolution Service and Alberta Motor Vehicle Industry Council
- 7% were made by municipalities
- 4% were made by post-secondary institutions
- 4% were made by school districts
- 2% were made by a regional health authority

These time extension requests were decided as follows:

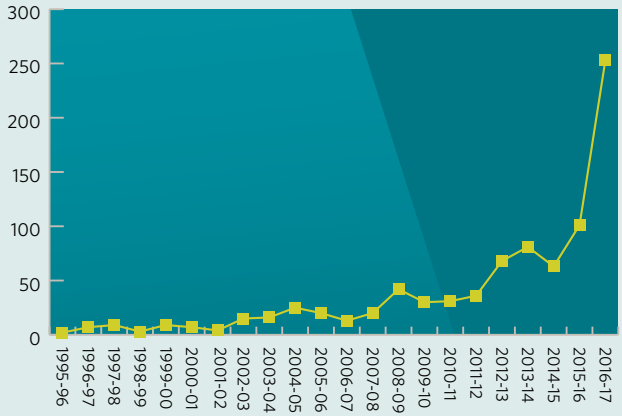
- 51% were granted
- 23% were partially granted (extension period permitted was less than what was requested by the public body)
- 18% were denied
- 8% were withdrawn by the public body

A public body must make every reasonable effort to respond to a request for access under the FOIP Act within 30 calendar days. A public body may ask the OIPC for a time extension in specific and limited situations set out in the FOIP Act (section 14).

In response to the influx of time extension requests, the OIPC updated its "Request for Time Extensions Form" and published a "Request for Time Extension Under Section 14" practice note to assist public bodies in understanding what the OIPC considers when granting or denying a time extension request. The updated form and new practice note were published in September 2016.

A LOOKBACK AT 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.



Investigation Reports

DELAYS IN RESPONDING TO ACCESS REQUESTS

Alberta Justice and Solicitor General

On September 1, 2016, the OIPC received a request from an applicant who alleged he had not received a response to any of the 14 access requests he had made to Alberta Justice and Solicitor General (JSG).

Upon review, the investigation found that there were 187 additional access requests outstanding for more than 30 days. The newest outstanding request was 109 days overdue while the oldest was more than 1,000 days overdue.

An investigation was initiated and identified a number of concerns with regard to process. During one exchange in a request to gather records responsive to an access request, the Assistant Deputy Minister of the Corporate Service Division was asked to provide records. Subsequently, seven reminders were required and it took JSG nearly six months to provide a response to the applicant.

Applying discretionary exceptions to access was also identified as contributing to delays, and the investigation emphasized that discretionary exceptions do not mean information must be withheld. The investigation recommended that staff responsible for managing access requests be trusted to use their own judgment and to generally increase trust in the professionalism of civil servants to provide sound advice even if information might be disclosed publicly.

The investigation recognized the time constraints within which employees responsible for managing access requests operate, particularly considering that staffing had not kept pace with the number of requests received. From 2011 to 2016, the number of access requests received by JSG increased 83% (from 224 in 2011 to 410 in 2016) while staffing levels in the FOIP Office ranged between eight to 11 employees. Additionally, the investigation found an increase in the number of complex or large requests.

Finally, anecdotal evidence provided during the investigation questioned the respect for access to information by senior management. One individual said that "FOIP wasn't taken seriously" by senior levels of the ministry when the Department of Justice merged with the Solicitor General's department in 2012, and again when the increase in access requests began. Senior leadership support is essential to set the tone for a culture that respects access to information.

In total, the investigation report made 19 recommendations to improve timeliness of responses.

> "The purpose of these investigations was to shed light on some of the systemic issues in the administration of access to information in Alberta. While process management is important, senior leadership must lay the groundwork for a culture that trusts and respects access to information as a cornerstone to good governance."
>
> *- Commissioner Jill Clayton, February 23, 2017*

Executive Council and Public Affairs Bureau

On June 29, 2016, the OIPC received 14 requests asking for a review of how Executive Council and the Public Affairs Bureau responded to access requests the applicant had made.

Of the 14 requests, nine were made to Executive Council and five to the Public Affairs Bureau. One FOIP Office handles access request processing for both public bodies.

The investigation focused on 12 of the requests. It was found that in each of the 12 cases the timelines to respond were not met under the FOIP Act. The longest delay was for more than six months beyond the 30-day time limit; the shortest was five days overdue.

The approval time was of concern for these 12 requests. The investigation noted the average approval time was 33 days, which alone is more than the legislated 30-day timeline to respond. The longest approval time was 85 days, while the shortest was 16 days.

Additionally, the investigation found that 257 access requests were made from August 2015 to October 2016. Of those, 105 requests were submitted by the applicant. A response was provided to the applicant for 82 of his 105 requests. The average length of time to respond was 78 days. However, the investigation noted that the average length of time to respond to other applicants was 64 days. In both cases, legislated timelines were not met but the response time to the applicant was 14 days longer than the average general response time, which could suggest that the applicant's requests were treated differently or were deliberately or intentionally delayed.

Disregarding very low numbers in 2011-12 (five access requests between both public bodies) there had been a 216% increase in the number of requests to 240 in 2015-16 from 64 in 2012-13.

The investigation recognized the time constraints within which those responsible for managing access requests operate, particularly considering that staffing had not kept pace with the number of requests being received. Staffing levels were adjusted during the course of the investigation, however.

Beyond the volume of requests, there were additional concerns in the process. Rather than an access request being sent to a FOIP Analyst upon receipt, the request was sent to the Senior Financial Officer (SFO) who sent it to the Deputy Secretary of Cabinet (DSC), who is the delegated authority for the public bodies with regard to access requests. Following reviews by the SFO and DSC, a request was then sent to the FOIP Office for retrieval and review of records prior to disclosure.

The investigation noted that this practice of preliminary review by the SFO and DSC impacted timelines, and that the process could be perceived as a form of interference by individuals who need not be involved until the records are retrieved and at least until an initial review had been completed. The public bodies changed the process during the investigation. Although the DSC continued to receive a copy of the request, the FOIP Analyst would receive it at the same time to not delay processing.

The investigation nonetheless recommended that only individuals with designated authority in the processing of requests be involved. Having more individuals involved not only delays the process, it also is contrary to the privacy protections in the FOIP Act. An individual who has no delegated authority in the processing of requests should not have access to the personal information contained in the records nor of applicants, if individuals are identifiable in the access request.

In total, there were nine recommendations made in the investigation.

LEAKED CELLPHONE RECORDS AT EXECUTIVE COUNCIL

An investigation of Service Alberta and Executive Council was launched on the Commissioner's own motion following a leak to the media in August 2014 of documents showing cellphone and data charges for four former Executive Council officials, including a former Deputy Premier.

The objectives of the investigation were to determine whether the public bodies:

- Used or disclosed personal information in contravention of the FOIP Act
- Implemented reasonable safeguards to protect the personal information at issue

The investigation found that, on a balance of probabilities, the documents were disclosed by Executive Council. Because the personal information was disclosed in an uncontrolled manner, without due consideration of all the circumstances (including the four affected individuals' privacy interests), the disclosure contravened the FOIP Act.

Executive Council was also found to have used personal information in contravention of the FOIP Act. In late 2012 and early 2013, the billing information was circulated within Executive Council as officials attempted to reduce the charges. The investigation determined this use of the information supported an understandable business purpose. However, the information was circulated again in March 2014 – two years after the cellphone charges were incurred. No one in Executive Council explained the purpose for this use of personal information and there was no evidence to support an authorized business purpose, which resulted in this second use being a contravention of the FOIP Act.

The investigation found that there were reasonable administrative, technical and physical safeguards to protect the information, which included public officials' names, business telephone numbers, data usage and related cellphone carrier charges. While the investigation recognized it would be unreasonable to expect public bodies to have extraordinary measures in place to protect this kind of information, the report noted that the government may store other more sensitive information in the same systems and recommended that Service Alberta and Executive Council review their security arrangements to prevent future leaks.

> "The FOIP Act provides an outlet for the controlled release of information about the operations of public bodies. While it is arguable that the release of information about cellphone charges may have been in the public interest, it was leaked in an uncontrolled manner – nobody's privacy interests were considered."
>
> *- Commissioner Jill Clayton, August 10, 2016*

Privacy Breaches

PIPA

There were 162 breaches reported under PIPA in 2016-17. This represented the highest number of self-reported breaches opened since mandatory breach reporting and notification provisions were enacted in 2010.

A total of 164 breach notification decisions were issued. In 102 decisions, the Commissioner decided there was a real risk of significant harm. There were 43 decisions where there was no real risk of significant harm found. There were 19 where the Commissioner decided PIPA did not apply.

Private sector organizations must report privacy breaches to the Commissioner in situations where a reasonable person would consider that a real risk of significant harm may result to an individual affected (section 34.1). This includes any loss, or unauthorized access or disclosure of personal information. The Commissioner has the power to require organizations to notify affected individuals when a privacy breach presents a real risk of significant harm (section 37.1).

Self-Reported Breaches Opened Per Year under PIPA

Mandatory Breach Reporting and Notification Provisions were enacted in 2010

2010-11: **49**
2011-12: **94**
2012-13: **84**
2013-14: **96**
2014-15: **138**
2015-16: **144**
2016-17: **162**

Hacking and Malware

The number of breach notification decisions involving hacking and malware continued to increase in 2016-17. More than 50 breach decisions were issued that found a real risk of significant harm to Albertans caused by unauthorized intrusions into computer systems. These incidents accounted for more than half of all breach decisions involving a real risk of significant harm. The breaches affect very few to millions of individuals. The most affected Albertans in one incident was approximately 109,000, while other incidents affected tens of thousands of Albertans. Many of the incidents are occurring due to the increased use of ecommerce.

The information at issue in many of these cases commonly includes email addresses, contact information, credit or payment card information, user credentials, and identification numbers.

There is no standard approach and the techniques by hackers vary depending on the attack – some are random attacks while others are targeted.

These stats highlight the need for organizations to remain vigilant to protect client and employee information.

Continuous employee training is critical to help limit the number of suspicious links from being clicked. In addition, business continuity plans must ensure that digital information is backed up and tested regularly to limit any productivity or material losses that may occur as a result of a cyberattack, especially intrusions or losses of personal information.

The decisions involving hacking or malware can be found at www.oipc.ab.ca.

Reusing Hacked or Common Passwords

Individuals are often reminded to use complex and different passwords on each website or app for which they have an account. When an individual reuses the same password for multiple accounts, if one is hacked then it makes all other accounts susceptible. Commonly used passwords pose a similar problem.

In one incident reported to the OIPC, an organization found there had been a brute force attack against its system whereby unauthorized third parties accessed member accounts using lists of email and password combinations to log into the systems and verify valid matches for accounts.

The organization confirmed that the attacker(s) knew the credentials of the members or used commonly-used passwords to gain access to accounts, and that the incident was not due to any data leaks or a weakness in its own systems. The unauthorized accesses allowed the attacker(s) to log in to user accounts and request the PIN in order to use the organization's services.

In another case, an organization operating a loyalty rewards program received several calls from program members reporting that rewards points had disappeared from their accounts.

The organization's investigation confirmed member accounts had been targeted by threat actors operating in the "dark web" of the internet. The organization believed that member accounts were accessed using usernames and/or passwords stolen from other sites.

A third breach occurred when an organization found that an unauthorized individual had gained access to 102 customer accounts using valid credentials. The organization reported that its own systems had not been compromised, and believed that the accounts were accessed using email address and password combinations obtained from a website that posts personal information from compromised applications.

The organization reported that the authentication credentials for accessing those accounts may have been obtained as a result of individuals using the same log in information across multiple ecommerce applications. Upon accessing an account, the unauthorized individual(s) changed the email address and then made purchases using gift and credit cards on the account.

car2go Canada Ltd., P2017-ND-42
Loblaw Companies Limited, P2017-ND-35
Indigo Books & Music Inc., P2017-ND-07

Rogue Employees

Current or former employees who have access to information systems then choose to snoop on personal information is a common type of breach reported to the OIPC

In one case, an organization was informed by another company that a former employee had accessed an electronic file, and confirmed that the information of 41 former and current independent sales agents was used to commit fraud by opening fake accounts for mobile phone services or to purchase smart phones. The former employee was not authorized to access the file while being employed by the organization.

In another incident, the organization learned that a recently departed employee hired through a staffing agency stole and used some credit card numbers without authorization. The former employee may have physically written down or copied credit card information that had been used.

A third matter involved an employee who had sent records to his personal email account. The records contained personal information of individuals who had completed occupational health screenings with the organization. The employee was terminated and retained the records as part of an employment dispute. It was reported that the former employee had used the records during a meeting with a third party organization.

EVO Payments International Corp. – Canada, P2017-ND-39
New England College of Optometry, P2017-ND-13
eScreen Canada ULC, P2017-ND-04

Senior Executive Phishing Scams

A number of organizations were victimized by phishing scams in which an employee of the organization is asked for information from an unauthorized individual who purports to be a senior executive or leadership member from the organization. The employee then provides the personal information at issue via email to the unauthorized individual(s).

In all but one of the cases, the information sought by the unauthorized individuals included social insurance numbers, salary or tax information, and contact information of employees of the respective organizations.

In the remaining case reported to the OIPC, name, email address and membership status was sent to the unauthorized individual(s).

Marin Software Incorporated, P2017-ND-32
Sexsauer Ltd., P2016-ND-54
Matrix Service Company, P2016-ND-36
Canadian Medical Association, P2016-ND-35
Landstar System, Inc., P2016-ND-34

HIA

There were 130 self-reported breaches voluntarily submitted by custodians under HIA in 2016-17.

Reporting breaches under HIA remains voluntary despite amendments passed in 2014 that would require custodians to report certain breaches to the Commissioner. These amendments were not in force as of March 31, 2017, and there has been no timeline given for if or when the amendments will be enacted.

One of the leading causes of breaches in the health sector is employee "snooping" into electronic files. Snooping is often done out of curiosity or, at times, with malicious intent. Either way, these incidents are unauthorized accesses under HIA. These issues are not limited to Alberta as a number of jurisdictions struggle with health information snooping in electronic health record systems.

Like private sector organizations, custodians also face similar concerns related to malware, hacking and phishing attacks.

In addition to emerging issues with electronic medical information systems, the OIPC continues to see issues around unsecured or misdirected faxes of paper records as a leading cause of breaches in Alberta's health sector. These incidents continue to occur despite repeated warnings and guidance related to the transmission of health information via fax machines by employers, regulatory bodies and professional associations.

FOIP

Like custodians under HIA, public bodies do not have a legislated requirement to report privacy breaches to the OIPC or to notify affected individuals. The Commissioner has recommended mandatory breach reporting and notification requirements in a variety of forums since 2013.

Some public bodies do voluntarily report certain breaches to the OIPC. The OIPC reviews each incident and makes any necessary recommendations to respond to the breach, notify affected individuals and help prevent future incidents.

In 2016-17, public bodies reported 50 privacy breaches to the OIPC. This represented an increase of 32% (12) over 2015-16 during which 38 breaches were voluntarily reported by public bodies to the OIPC.

Among the incidents reported in 2016-17 were breaches caused by mailing or emailing errors (e.g. wrong mailing address or email address mistakenly autocompleted), system or website administration errors (e.g. personal information mistakenly posted in shared drives or on websites), records stolen from an office or an employee's vehicle or home, rogue employees (e.g. unauthorized database searches), and malware or ransomware. There were also incidents where personal information was disclosed during the processing of access requests by public bodies.

Offence Investigations

HIA

In 2016-17, three individuals were convicted for knowingly accessing health information in contravention of HIA. There have been seven convictions under HIA since it was enacted in 2001.

In one case, the individual pleaded guilty to accessing the health information of 26 people in contravention of HIA. The individual had been working at the Alberta Children's Hospital where she was responsible for entering and confirming data relating to newborns with congenital anomalies. The breach was discovered by Alberta Health Services in April 2014 while it conducted database audits, including Alberta Netcare, the provincial electronic health record. The judge issued a $5,000 fine on September 21, 2016.

A second case dealt with a former supervisor of health information management who was convicted for accessing individuals' health information in contravention of HIA. The judge issued a $5,000 fine on March 21, 2017 for 13 unauthorized accesses of health information. In June 2013, Alberta Health Services was notified that the individual had visited with her boyfriend in the health records room at the Tofield Health Centre in contravention of internal policy. AHS conducted an audit of the individual's accesses in medical information systems, including Alberta Netcare, the provincial electronic health record. The OIPC's investigation found that the health information of 14 individuals was improperly accessed on 25 occasions in Alberta Netcare.

In the third case, a former registration and staffing clerk pleaded guilty and was fined $3,000 for accessing individuals' health information in contravention of HIA on March 27, 2017. In 2015, Alberta Health Services identified 279 alleged unauthorized accesses of health information in electronic health record systems by the individual. The OIPC's investigation focused on 28 of the alleged unauthorized accesses of health information. For prosecution, that number was reduced to 21 as seven accesses were barred due to the limitation period under HIA. During the investigation, the individual resigned from her position where she had been working at the Athabasca Health Care Centre.

One additional case was before the courts as of March 31, 2017.

7 convictions under HIA for unauthorized access of health information since the Act was **enacted in 2001.**

Mediation and Investigation

Each year, hundreds of files work their way through the office's mediation and investigation processes – both 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. Seventy-eight percent (78%) of files that could proceed to inquiry are resolved by the OIPC's Mediation and Investigation unit.

There are themes and trends that become apparent when there are a number of similar requests for review or complaints being submitted to the OIPC in any given year.

EMPLOYEE REQUESTS FOR PERSONAL INFORMATION UPON TERMINATION

Under both the FOIP Act and PIPA, there was a noticeable increase in terminated employees asking for access to personal information in their personnel files.

Individuals may provide a written request to organizations for records, such as for pay stubs or for "my entire employee file." Sometimes organizations do not acknowledge the request, presumably not understanding that it is a request under PIPA, or will refuse to provide the records since the organization believes it does not need to as the requested records have previously been provided during the employment relationship.

PIPA requires that the request for personal information be in writing with sufficient detail to enable the organization to identify the record(s) being requested. "Personal information" and "personal employee information" are defined differently under PIPA and as such are treated differently, especially with respect to fees that can be charged to access the information.

There is no requirement for applicants to mention that the request is being made under PIPA specifically.

It is important for organizations to know that there is a legal obligation to respond within time limits and with sufficient explanation for providing or not providing access to records under PIPA. It would be beneficial to all parties that when an organization receives a request to clarify the expectations of the requestor and respond in accordance with the law.

REASONABLE COLLECTION AND DISCLOSURE OF PERSONAL EMPLOYEE INFORMATION

There have also been several privacy complaints about personal information disclosures during takeovers of one business by another. Complaints also occur regarding the amount and nature of information sharing between organizations, such as between contractor and subcontractor or when providing employment references.

The OIPC also receives complaints that too much personal information is disclosed for the intended purpose. For example, when one organization is asked about a former employee by another organization outside the purpose of a reference, the response "this person is no longer with us" is sufficient in most circumstances. However, some organizations also provide the rationale for why the person left or was terminated, which may be outside the authority to disclose without consent under PIPA.

The OIPC has also noticed an increase in complaints about the amount and type of personal information collected for disability claims and Workers' Compensation Board claims, as well as the necessity and quantity of information disclosed to an employer.

RIGHT TO BE FORGOTTEN

There have been a few files with respect to the availability of personal information on the internet concerning individuals' past involvement with legal proceedings or quasi-judicial bodies.

The concerns centre on what personal information is searchable on external search engines based on an individual's name. For example, as a party in a lawsuit, arbitration or a matter before a quasi-judicial tribunal.

The questions that arise in these cases include: Can individuals control the amount of personal information being scraped by search engines? Are there controls in the amount of personal information that search engines can find? Is it incumbent on the entity publishing the decisions to prevent external search engines from scanning personal information in publicly available records, such as names in court records? For example, by preventing the indexing of decisions using web robot exclusion protocols.

These are complex issues. They involve the balance of open court principles, public availability of information concerning certain tribunal decisions, and the ubiquity and permanence of information online, as well as an individual's right to privacy.

Balancing these interests will only become more challenging as information technologies continue to evolve and as people conduct searches for purposes beyond those originally contemplated by open court principles.

Privacy Impact Assessment Reviews

A privacy impact assessment (PIA) helps to identify and address potential privacy risks that may occur in the operation of a new or redesigned project. PIAs are meant to be used for proposed legislative schemes, administrative practices and/or information systems that relate to the collection, use or disclosure of individually identifying personal or health information.

A PIA describes the initiative and its benefits, analyzes legal authority to collect, use or disclose personal or health information, assesses privacy risk and mitigation plans, and explains the policy management structure in place.

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 information in a new or redesigned project or legislative scheme.

A listing of all PIAs accepted by the OIPC in 2016-17 is available at www.oipc.ab.ca.

PIA STATS

In 2016-17, the OIPC accepted 573 PIAs, which represented an increase of 44% over 2015-16 (399).

Considering mandatory PIA requirements under HIA (section 64), 96%, or 548, of accepted PIAs were submitted by custodians. The OIPC accepted 22 PIAs from public bodies subject to the FOIP Act and three PIAs were accepted under PIPA.

HIA

Of 548 accepted PIAs under HIA in 2016-17, there were several notable projects reviewed.

The OIPC accepted a PIA related to Alberta Health's Medical Assistance in Dying Regulatory Review Committee. The committee was developed in part to review, report and make recommendations to the Minister of Health on the regulatory framework and health services delivered in Alberta with respect to medical assistance in dying.

Of the **548** accepted PIAs under HIA, **75%** or 409, were from physicians **(208)** and pharmacists/ pharmacists **(201)**.

A PIA related to an online patient portal was also accepted in 2016-17. A PIA on the Carebook Patient Portal was submitted by a physician. The purpose of the portal is to provide individuals and families with access to their personal health record(s). Information can be entered into the portal and information can flow from outside sources, such as an individual's family doctor's electronic medical record system or laboratory testing facilities. The portal can also import data from home diagnostic equipment, such as blood pressure monitors.

The first Alberta Netcare PIA accepted from an optometrist was in May 2016. This was accepted during the pilot phase of a project to include optometrists as authorized custodians for Netcare, the province's electronic health record.

Relatedly, the first Netcare PIA from a dentist was accepted during the pilot phase of a project to include dentists as registered custodians for the purpose of accessing Netcare.

The full implementation of Netcare access for optometrists and dentists' access to Netcare had not occurred as of March 31, 2017.

FOIP ACT

Under the FOIP Act, it is not mandatory for public bodies to prepare or submit a PIA to the OIPC. However, public bodies voluntarily submit PIAs to the OIPC for review and comment. In 2016-17, there were noteworthy PIAs accepted by the OIPC that were submitted by public bodies.

Service Alberta submitted, and the OIPC accepted, a PIA on the MyAlberta Digital Identity project. The program was implemented by the Government of Alberta as a means to facilitate electronic delivery of services to Albertans. The intent of the project is to deliver services more efficiently while maintaining the security of personal information required for service delivery by government departments. The goal is for the program to be used by government departments, municipalities, post-secondary institutions, agencies, boards and commissions, and other public bodies as defined under the FOIP Act.

The Calgary Police Service (CPS) partnered with the Missing Children Society of Canada (MCSC) on a program that provides information about a missing child and any potential suspects to MCSC who then can direct it to the public through their search program which uses social media to engage the public in its search efforts. While the alerts use mobile devices and social media, the personal information related to a missing child case is securely stored by MCSC. Information shared through alerts is the same as was previously distributed through traditional media, but the search program now enhances the scope of coverage and allows for targeting certain locations to gather information to help with finding a missing child.

Summary of Significant Decisions

TRANSGENDER STUDENT PRIVACY

A female transgender student made a privacy complaint that the Edmonton Public School District No. 7 disclosed her personal information in contravention of the FOIP Act when teachers displayed or called out her legal name, which is a typically male name. The public body agreed that it had breached the FOIP Act and had not made proper security arrangements to protect the student's personal information.

The Adjudicator found that the public body disclosed the student's personal information – name, sex, and that her gender identity was different than her sex at birth – in contravention of the FOIP Act. The Adjudicator also found that it had failed to make proper security arrangements, but noted that the draft policy created after these breaches addressed the concerns raised by the student.

Edmonton Public School District No. 7, Order F2016-26

AFFILIATE OR CUSTODIAN RESPONSIBILITY UNDER HIA

An individual made a privacy complaint that two physicians gained access to her health information from Alberta Netcare in contravention of HIA.

The two physicians conceded that they had gained access to the complainant's health information in 2008 and 2012 for the purpose of addressing complaints that had been made about care they had provided to the complainant. The physicians also disclosed the health information they had obtained to the Alberta College of Physicians and Surgeons related to a complaint of the care they had given. Alberta Health Services operated the facilities at which the accesses occurred and also conceded that the two physicians had accessed the complainant's health information.

The Adjudicator made a number of determinations related to this complaint.

First, the Adjudicator determined that AHS was the custodian in this case, and that the two physicians were 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. Because of AHS being the custodian and the physicians were affiliates, the Adjudicator found that the physicians had gained access to the complainant's health information for their own personal purposes, rather than those of AHS, and that AHS had contravened HIA due to the physician's uses of health information for personal purposes.

Second, the Adjudicator determined that the complainant's health information had been disclosed by the physicians to the Alberta College of Physicians and Surgeons for the purpose of defending themselves in a complaint submitted to the College. AHS would not have had authority to disclose the complainant's health information in the circumstances in which the two physicians 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.

Third, while the Adjudicator found that the two physicians had caused AHS to contravene HIA, it appeared that the physicians had not contravened AHS policies. 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 allow affiliates to use and disclose health information for their own personal purposes, rather than purposes authorized by HIA.

The Adjudicator ordered AHS to cease using and disclosing the complainant's health information in contravention of HIA.

The Adjudicator also suggested that compliance could be achieved by revising the policies and procedures for affiliates to convey the following:

- Only AHS is the custodian and authorized custodian at sites it operates
- HIA authorizes only an "authorized custodian" to use or disclose health information via Alberta Netcare
- Affiliates may use or disclose health information via Alberta Netcare at AHS' sites only where AHS would have authority to use or disclose health information

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.

There were two applications for judicial review issued on this order – one by the physicians and one by AHS. As of March 31, 2017, the judicial reviews had not been heard.

Alberta Health Services, Order H2016-06

INFORMATION IN THE PUBLIC INTEREST OR DOMAIN

There were five cases that concluded at inquiry which involved information deemed to be in the public interest or information that was already in the public domain that was withheld in response to an access request.

In one case, the applicant made an access request to the Edmonton Police Service (EPS) for a disciplinary decision. The applicant submitted a copy of a newspaper article in which the conduct of a named police officer is outlined giving rise to the disciplinary decision that was requested. The Adjudicator decided that would be an absurd result if the applicant were to be denied access to the name and badge number of the EPS member when this information was inferable from information in the public domain. The information was also inferable based on the initial response by EPS to the applicant's request. However, the Adjudicator confirmed the decision of EPS to redact details about the EPS member's employment and volunteer history.

In a second case involving EPS, an access request was again made for a disciplinary decision. EPS provided the applicant with the disciplinary decision but redacted the names of the accused/complainant and third party officers and their badge numbers. The Adjudicator found that any need for public scrutiny of EPS' actions had been met but that the information was publicly available to such an extent that it was a factor that weighed heavily in favour of disclosure. EPS was ordered to disclose all of the redacted information.

In a third case involving EPS, an individual complained that EPS issued a media release about his release from prison. The Adjudicator found that EPS was permitted to disclose the complainant's personal information because EPS had reasonable grounds to believe that the public was in imminent danger or risk of harm. The FOIP Act permits disclosure of personal information in these circumstances.

In two separate cases, a journalist requested records from Alberta Energy and the Alberta Energy Regulator and fee estimates were issued prior to processing the request. In each case, the journalist requested a fee waiver, arguing the records being requested were in the public interest.

In the case involving the Alberta Energy Regulator, it was determined that the fee would be waived as the matter was of public interest and the applicant had requested the records in order to write an article for the purpose of promoting public debate and awareness regarding this matter.

In the case involving Alberta Energy, the Adjudicator decided that it was appropriate to grant a fee waiver in the public interest, as the records would contribute to the public understanding as to whether Alberta Energy had corrected

deficiencies noted by the Auditor General in two different reports, and whether the bioenergy program is serving to reduce emissions, and therefore, whether Alberta Energy is spending public money on the bioenergy program appropriately.

Edmonton Police Service, Orders F2016-20, F2016-32 and F2016-33
Alberta Energy Regulator, Order F2016-39
Alberta Energy, Order F2016-40

SOLICITOR-CLIENT PRIVILEGE

In five cases, Adjudicators considered whether solicitor-client privilege applied to records at issue. Three of these are discussed below.

In a matter involving the Calgary Police Service (CPS), the applicant requested records related to the processing of another access request he had submitted. The Adjudicator asked the law firm responding on behalf of CPS to provide additional evidence to demonstrate that some of the records at issue were subject to solicitor-client privilege.

The Adjudicator found that CPS' evidence as to the nature of the relationship between those it described as lawyers and itself was insufficient in most cases to understand the relationships. The Adjudicator also found that the 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, CPS' application of multiple exceptions to the same records, all of which require a different factual foundation to apply, had the effect of giving CPS' evidence as to the facts an ambiguous quality. The Adjudicator ordered the disclosure of most of the records to the applicant. CPS applied for a judicial review on this order. As of March 31, 2017, the judicial review had not been heard.

In a case involving Alberta Human Services, the Adjudicator found the evidence provided was sufficient and accepted that the records contained communications between a solicitor and client that entailed the seeking or giving of legal advice.

An individual had made a request to Alberta Human Services for a copy of his Assured Income for the Severely Handicapped investigation file. Alberta Human Services withheld some information based on a claim of solicitor-client privilege. The applicant requested a review.

A lawyer representing Alberta Human Services provided an affidavit stating the nature of the relationship and a chart indicating how many pages comprised each record, the type of record, the date of the record and who created the record, and to whom the record was provided and/or copied. The Adjudicator found that Alberta Human Services properly withheld the records from the applicant based on the affidavit evidence and detailed chart of records.

In the third case, an applicant requested records about him and his employment from Alberta Children's Services. The Adjudicator made a number of determinations related to records withheld under various exceptions. With regard to records withheld due to claims of solicitor-client privilege, the Adjudicator upheld Alberta Children's Services decision.

The Adjudicator noted that the final affidavit and additional evidence (chart) provided by Alberta Children's Services regarding solicitor-client privilege was a good example of how to support a claim for that privilege without providing the information in the records to the Adjudicator or revealing the legal advice.

The Adjudicator also noted that having the relevant dates for the correspondence and the position titles of the correspondents was valuable for supporting the claim of solicitor-client privilege with respect to emails between Alberta Children's Services employees who are not counsel (i.e. determining the likelihood that those employees were discussing legal advice that was provided by counsel).

Calgary Police Service, Order F2016-35
Alberta Human Services, Order F2016-63
Alberta Children's Services, Order F2017-28

INTERNAL REVIEW AND CONSULTATION PROCESSES UNDER THE FOIP ACT

An applicant made a request to Executive Council for copies of polling paid for by the Government of Alberta, and copies of deliverables completed as a result of polling. Executive Council informed the applicant that it was extending the time to respond because it needed to search a large volume of records. The applicant did not receive a response and requested a review.

Executive Council responded to the applicant during the inquiry. However, at the inquiry, Executive Council attributed its failure to respond to the applicant within the time limits set out in the FOIP Act due to an influx of access requests, the large volume of records, internal and third party consultation requirements, and the extensive review and approval period to which it subjected the request. Executive Council had also provided notice to third parties of a decision to disclose information in the records and waited for the appeal period to end before releasing the records.

The Adjudicator found that Executive Council failed to comply with its duty to make reasonable efforts to respond to the applicant within 30 days. This failure was due in part to Executive Council's internal review and consultation process. The Adjudicator noted that duties under the FOIP Act are statutory while internal procedures are not. As Executive Council had responded to the applicant during the inquiry, the Adjudicator did not make an order but requested that it review its processes to align them with requirements under the FOIP Act to respond within time limits.

Executive Council, Order F2017-12

Judicial Reviews and Other Court Decisions

Alberta (Information and Privacy Commissioner) v. University of Calgary

2016 SCC 53, [2016] 2 S.C.R. 555, which upheld 2015 ABCA 118, which reversed 2013 ABQB 652, which upheld an Adjudicator's Notice to Produce Records alleged to be subject to solicitor-client privilege

An individual, a former employee of the University of Calgary, made an access request for information held by various other employees of the public body, a Wellness Centre and a doctor associated with the Wellness Centre. The public body provided some of the information, but withheld other information under various exceptions to disclosure contained in the FOIP Act, including section 27(1)(a) (solicitor-client privilege). The individual requested that the Commissioner review the public body's decisions to withhold information.

In an inquiry under the FOIP Act, the public body chose not to provide the Adjudicator with a copy of the records for which it claimed that solicitor-client privilege applied, in accordance with the OIPC's "Solicitor-Client Privilege Adjudication Protocol". In accordance with the protocol, the Adjudicator requested additional argument and evidence from the public body so that he could decide whether it properly applied section 27(1)(a) to the records. The public body provided a minimal amount of additional information, which was insufficient for the Adjudicator to decide the issue. The Adjudicator sent the public body a notice under section 56(2) of the FOIP Act to produce the records so that he could decide whether the public body had the authority to withhold those records.

The public body applied for judicial review of the Adjudicator's Notice to Produce Records. The Court of Queen's Bench held that the standard of review was correctness, that the FOIP Act gave the Commissioner authority to issue a Notice to Produce in relation to records that were alleged to be subject to solicitor-client privilege, and upheld the Adjudicator's decision to issue the Notice to Produce as being correct. On appeal, the Court of Appeal reversed the lower court's decision, holding that the FOIP Act did not authorize the Commissioner to order a public body to produce to her records over which it had asserted solicitor-client privilege. The Commissioner obtained leave to appeal the Court of Appeal's decision to the Supreme Court of Canada.

The primary issue before the Supreme Court of Canada was whether section 56(3) of the FOIP Act, which requires a public body to produce to the Commissioner records "[d]espite … any privilege of the law of evidence", allows the Commissioner to review documents that a public body claims are protected by solicitor-client privilege. Three separate sets of partially concurring reasons were issued.

Speaking for the majority, Justice Côté held that the issue was one of central importance to the legal system as a whole and outside the Commissioner's area of expertise. Therefore, the applicable standard of review was correctness. She held (at paragraph 28) that to give effect to solicitor-client privilege as a fundamental policy of the law, legislative language purporting to abrogate it, set it aside or infringe it must be interpreted restrictively and must demonstrate a clear and unambiguous legislative intent to do so. She explained that solicitor-client privilege was a substantive rule, rather than merely an evidentiary rule and concluded that "any privilege of the law of evidence" was not sufficiently clear and precise to set aside or permit an infringement of solicitor-client privilege. Justice Côté stated:

> [57] Solicitor-client privilege is clearly a "legal privilege" under s. 27(1), but not clearly a "privilege of the law of evidence" under s. 56(3). As discussed, the expression "privilege of the law of evidence" is not sufficiently precise to capture the broader substantive importance of solicitor-

client privilege. Therefore, the head of a public body may refuse to disclose such information pursuant to s. 27(1), and the Commissioner cannot compel its disclosure for review under s. 56(3). This simply means that the Commissioner will not be able to review documents over which solicitor-client privilege is claimed. This result is consistent with the nature of solicitor-client privilege as a highly protected privilege.

The majority acknowledged that subject to constitutional limitations, legislatures can pierce solicitor-client privilege by statute. However, the language of the provision must be explicit and evince a clear and unambiguous legislative intent to do so.

Justice Cromwell, although he agreed with the result reached by the majority (that production of the records at issue in this case should not have been ordered), disagreed with the majority's interpretation that the FOIP Act did not allow the Commissioner to order production of records over which solicitor-client privilege had been claimed. He stated:

> [73] Whatever other principles and presumptions of statutory interpretation are engaged, statutory interpretation must be anchored in the words chosen by the legislature, read in their full context. In my respectful view, to hold as my colleague Justice Côté would that solicitor-client privilege is a "legal privilege", but not a "privilege of the law of evidence" in *FOIPP* is not justified by the text or context of the legislation or by the principle of interpretation that the legislature must use clear language to authorize any abrogation of solicitor-client privilege. Rather, the words of the enactment, read in context, evince a clear intention to permit the Commissioner, subject to judicial review, to order production for inspection of records over which solicitor-client privilege is claimed. To hold otherwise abandons the modern approach to statutory interpretation repeatedly endorsed by the Court and, under the guise of "restrictive" interpretation, undermines legislative policy choices which, absent constitutional constraint, legislatures are entitled to make.

Finally, in her own separate, but partially concurring reasons, Justice Abella disagreed with the majority's conclusion on the standard of review, and held that the standard of review should have been reasonableness.

The appeal was dismissed.

Edmonton (City) v. Alberta (Information and Privacy Commissioner)

2016 ABCA 110, which overturned in part Edmonton (City) v. Alberta (Information and Privacy Commissioner), 2015 ABQB 246, which upheld Order F2013-53

An individual made a request under the FOIP Act to the City of Edmonton for access to all records relating to herself or her property for a certain time period. The public body informed the Applicant that her request was for general information, not personal information, and was therefore subject to a $25 initial fee.

At inquiry, the Adjudicator found that the public body did not meet the timelines required under the FOIP Act, and that it did not meet its duty to assist the applicant because it failed to properly define her request. The Adjudicator also determined that the applicant's request was for bylaw complaints about the applicant. As such, it was a request for "personal information" and was therefore not subject to the $25 initial fee. Finally, the Adjudicator found that the public body did not consider all relevant factors in withholding information in the responsive records under section 17 of the FOIP Act. The Adjudicator ordered the public body to consider all relevant circumstances in making the decision to disclose or withhold personal information in the responsive records.

On judicial review, the main issue before the Court of Queen's Bench was the Adjudicator's interpretation of "personal information" in the FOIP Act. The court upheld Order F2013-53 as reasonable and dismissed the public body's judicial review application.

The public body appealed the Court's decision. On appeal, the Court of Appeal agreed with the lower court that the Adjudicator's interpretation of personal information was reasonable, stating:

> [25] In general terms, there is some universality to the conclusion in *Leon's Furniture* that personal information has to be essentially "about a person", and not "about an object", even though most objects or properties have some relationship with persons. As the adjudicator recognized, this concept underlies the definitions in both the *FOIPP Act* and the *Personal Information Protection Act.* It was, however, reasonable for the adjudicator to observe that the line between the two is imprecise. Where the information related to property, but also had a "personal dimension", it might sometimes properly be characterized as "personal information."

Because the request was for personal information, the Court held it was reasonable to find that no fee was payable. The Court also held it was reasonable for the Adjudicator to request an explanation of the redactions the public body made under section 17.

The Court of Appeal, however, found that the Adjudicator's decision with respect to section 10, the duty to assist, was unreasonable, stating:

> [42] The requirement of s. 10 that the public body must assist the applicant cannot reasonably mean that the public body must be right in law every time. The requirement that disclosures must be "accurate" reasonably relates to the thoroughness of the search, the production of the documents requested, and the minimization of production of un-requested documents. Further, just because the Commissioner subsequently decides that the public body has not properly responded to the request does not automatically mean that there has been a failure to apply "every reasonable effort."

With respect to the scope of production of the records requested, the Court of Appeal stated:

> [52] As the adjudicator noted, the City's search was "thorough, if overbroad, given the Applicant's clarified request". It is unreasonable and unrealistic to expect that every search for requested documents will be perfectly focused. Given the general nature of the request made in this case, even a diligent search might have failed to discover some documents, and may have produced some other documents that were not of interest to [the applicant]. Given the objectives of the *FOIPP Act,* obviously the latter is preferable to the former. Unless third-party interests are engaged, it is much more in keeping with the spirit of the *FOIPP Act* to have the public body produce some documents that turn out not to be of interest, rather than to miss some documents that are genuinely of interest. Criticizing a search for being unhelpful or inaccurate because it is "overbroad" is an unreasonable conclusion. An overbroad production could only be characterized as inaccurate if the production was so unfocused that the documents of genuine interest are effectively hidden in a haystack.

The Court of Appeal allowed the public body's appeal in part, and set aside the portion of the Adjudicator's order that found the public body had not complied with section 10 of the FOIP Act. The Adjudicator's conclusions on the scope of the term "personal information", the resulting payment of fees and the need for further particulars about the application of section 17 were all reasonable.

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, currently under appeal

The Criminal Trial Lawyers' Association (applicant) requested records from the Calgary Police Service relating to: money spent in 2011 on lawyers other than in-house counsel, money spent by the public body on in-house counsel, excluding any counsel

who work on litigation or claims involving police vehicles, and money spent on in-house counsel who do FOIP Act work. The public body denied access to the information on the basis that it was subject to solicitor-client privilege. At inquiry, the public body stated responsive records did not exist, but acknowledged that if solicitor-client privilege did not attach to the requested information, it had a duty under section 10(2) of the FOIP Act to create the records.

The Adjudicator determined it was necessary for the public body to respond to the applicant's access request either by creating records or by producing severed records that would enable the applicant to determine the amounts specified in its request.

On judicial review, the Court held that the appropriate standard of review was correctness, and that the Adjudicator had provided a correct statement of the law regarding the application of the FOIP Act, stating at page 8 of the transcript:

> The decision of the delegate started in the analysis by outlining the issue and then turned to the case of *Solosky v. Queen,* [1980] 1 SCR 821, which outlined what solicitor privilege is. The decision accepted and outlined the position in *Maranda*. The delegate pointed out that the request here is not for actual billings, but an aggregate number or total sums of payment. The decision of the delegate considered the request, not fees on a particular matter, but rather the adding up of fees with no requirement that the firm or how many files or topics were covered was disclosed. The request in relation to the salaries of the in-house counsel, again, it recognized, would reveal money spent in relation to particular job descriptions but nothing about the content of the file or the topics that were dealt with.
>
> The delegate then came to the conclusion that the global amount sought could not possibly be subject to solicitor/client privilege as this revealed nothing about the particulars of the matters. This would not reveal communications between the solicitor and the client or the nature of the advice or from whom the advice is sought or given. In the application of the assiduous inquirer test, the delegate dealt with the concerns raised by the applicant that the assiduous inquirer would gain access to how big a legal war chest the CPS has or gain insight into how often or how much access the CPS has to legal advice. The delegate, in a logical fashion, went through why she did not accept those assertions. The delegate held the presumption in *Maranda* was rebutted and in a reasoned and detailed decision, she found that creating a record or records to satisfy the applicant's access request would not reveal solicitor/client communications and therefore she made an order that the applicant comply with its duty.

The Court held that Order F2015-08 correctly stated the law and applied it to the facts, and that it withstood review at the correctness level. The application for judicial review was dismissed.

The public body has appealed the Court's decision.

Selim v. Alberta (Information and Privacy Commissioner)

2016 ABQB 562 – Judicial Review of the Commissioner's decision to refuse to conduct an inquiry under the FOIP Act, section 70

The applicant spent approximately seven months communicating with a member of the Calgary Police Service about a woman, "JC", whom he had been trying to contact. The police officer had led the applicant to believe he was directly communicating with JC, including fabricating a letter from JC to the applicant. After the police officer informed the applicant he would no longer communicate with him, the applicant made a request under the FOIP Act to the public body for information about JC. The public body responded to the applicant, informing him it had no records.

The applicant requested a review of the public body's response and the Commissioner authorized an investigation and mediation which was unsuccessful. The applicant requested an inquiry. In order to decide whether an inquiry would be conducted, the Commissioner asked the public body to provide a sworn document outlining the specific steps it had taken to identify and locate responsive records. The public body provided the Commissioner with a declaration to the effect that it had made inquiries of the police officer in question who had asserted that all communications had been conducted only in

a personal capacity, that no police records existed relative to JC and that all information the police officer had provided the applicant was "to attempt to assuage a person suffering from delusional thinking".

The Commissioner relied on the declaration from the public body. The applicant was notified that the Commissioner refused to conduct an inquiry because the police officer had never been in contact with JC, and therefore there could be no records relating to JC. The applicant requested a judicial review of the Commissioner's decision to refuse to conduct an inquiry.

After reviewing the circumstances of the case, the Court concluded the Commissioner's decision to refuse to conduct an inquiry was reasonable and the judicial review was dismissed.

Davis v. Alberta (Information and Privacy Commissioner)

2016 ABQB 578 – Judicial Review of Order F2015-36

An applicant made an access request to a school board for all of the information it had gathered in relation to a bullying complaint the applicant had made. The applicant also requested records containing information provided by individuals who had provided references for her. The public body conducted a search for responsive records, but was unable to locate anything relating to the bullying complaint other than a written decision dismissing the complaint, which it had already provided to the applicant. The public body provided records relating to the applicant's references.

The Adjudicator reviewed the public body's response and found that the public body had conducted a reasonable search for responsive records and had responded openly, accurately, and completely. The public body was unable to produce records relating to the bullying complaint, as no such records had been created.

On judicial review, the Court noted the applicant was self-represented, and that although the originating application was styled as a judicial review, it was based on, and sought remedies for, matters that were clearly outside the scope of a judicial review application. With respect to matters that were properly the subject of judicial review, the Court found the standard of review was reasonableness. The Court held it was reasonable for the Adjudicator to conclude the public body had complied with the FOIP Act in its response to the applicant's request, and that it was reasonable for the Adjudicator to conclude that certain remedies sought by the applicant were outside the Adjudicator's jurisdiction.

The Court dismissed the application for judicial review.

Steven Grove v. Office of the Information and Privacy Commissioner

Oral decision of Read J., Action No. 1403-02800, June 10, 2016 – Judicial Review of Order H2013-04

The applicant had been referred by his family physician for a psychiatric assessment. The psychiatrist, a custodian under the *Health Information Act,* met the applicant and prepared a consultation report which was sent to the applicant's family physician. The applicant wrote to the custodian, objecting to several statements in the report. The custodian agreed to correct two factual errors in the report, but informed the applicant he would not make any additional changes to the report on the basis that the report was the custodian's professional opinion. The custodian provided the applicant's family physician with an addendum to the report that noted and corrected the factual errors.

The Applicant requested a review of the custodian's decision. The Adjudicator held that most of the applicant's letter to the custodian was not sufficiently clear to constitute a request for correction under HIA, and that the custodian properly refused to correct or amend the items for which the applicant had requested a correction, other than the two factual items that were amended by the custodian prior to the inquiry.

On judicial review, the Court of Queen's Bench stated that HIA did not compel custodians to resolve differences of opinion by forcing physicians to change their opinion under the guise of correction. The Court held that the proper standard of review to be applied to the Adjudicator's decision was reasonableness, and that the order under review was reasonable. The application for judicial review was dismissed.

EDUCATION & OUTREACH

The mandate of the OIPC includes a strong commitment to education and outreach. From publications to presentations, the office raises public awareness of access to information and privacy rights under the FOIP Act, HIA and PIPA; provides guidance and direction to stakeholders to enhance compliance; and facilitates opportunities for the public and stakeholders to comment on the administration of the Acts, OIPC processes, and access and privacy trends and issues.

Presentations, Forums and Workshops

In 2016-17, the Commissioner and staff participated in 70 presentations, training sessions and speaking engagements. These local, national and international events provide an opportunity for the office to promote its educational mandate, increase awareness about access and privacy issues, and share the office's experiences.

SCHOOL AT THE LEGISLATURE

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.

DATA PRIVACY DAY: PRIVACY IMPLICATIONS IN THE NETWORKED CLASSROOM

The OIPC took a slightly different approach to its annual Data Privacy Day celebration by co-hosting a workshop with The eQuality Project and the Alberta Teachers' Association. The workshop, titled "Privacy Implications in the Networked Classroom: A Workshop", brought together researchers and leaders of The eQuality Project with school district administrators, access and privacy professionals, principals and teachers from across Alberta.

The topics presented were the use of technology in schools, educational software, social media monitoring of students, education law and policy on cyberbullying, and tools to help educators promote privacy in the classroom and board of education policy.

In addition, there were breakout group discussions throughout the day that in part served as an opportunity for The eQuality Project to develop a base of "on the ground" research for understanding the privacy implications in Alberta's networked classrooms.

Data Privacy Day is internationally recognized on January 28 to promote the protection of personal information. The OIPC hosts annual events on or during the week of January 28.

RIGHT TO KNOW WEEK FORUMS

The focus of the OIPC's 2016 Right to Know Week Forums was on access impact assessments. Half-day forums were hosted in Calgary and Edmonton.

In June 2016, the OIPC completed and published its first access impact assessment as part of its mandated disclosure of compensation information under the *Public Sector Compensation Transparency Act*. To follow up on that assessment, the office published *Access Impact Assessment Guidelines for Proactive Disclosure,* which was released during Right to Know Week.

In addition to a presentation by the OIPC on the guidelines, the City of Calgary presented its approach to access impact assessments. The forums also included a chat with the Commissioner and OIPC staff, which provided an opportunity for participants to ask questions and discuss access to information issues and trends.

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 also proclaimed

September 28 as the "International Day for the Universal Access to Information". The OIPC hosts forums in Calgary and Edmonton annually during the week of September 28 to recognize Right to Know Day.

FEDERAL STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

The Commissioner presented to the House of Commons' Standing Committee on Access to Information, Privacy and Ethics in February 2017 as part of that Committee's review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

PIPEDA is the federal private sector privacy law that applies to a federal work, undertaking or business or to businesses carrying on a commercial activity in provinces that do not have a private sector privacy law deemed substantially similar to PIPEDA. Alberta, British Columbia and Quebec each have private sector privacy laws deemed substantially similar to PIPEDA.

The Commissioner provided evidence to the Committee, including on aspects where Alberta's PIPA differs from PIPEDA, such as mandatory breach reporting and notification provisions, and the Commissioner's order-making powers (i.e. the Privacy Commissioner of Canada has an ombudspersons function).

The Commissioner also commented on global considerations for private sector privacy law, namely the European Union's *General Data Protection Regulation* that comes into force in May 2018.

Finally, the Commissioner spoke to the issues around meaningful consent, "I seldom hear that consent and notice should be done away with entirely, but there does seem to be concern that in this age of big data, predictive analytics, and complex information systems, consent and notice may not be adequate in all cases and may stifle innovation as well as initiatives that are in the public interest... In any event, I believe any solution to the problem, if there is a problem in this area, would involve a mix of legislative, regulatory, and voluntary options, and I certainly support discussion of these issues, including consultations such as the exercise the federal Privacy Commissioner recently undertook."

The presentation follows an earlier (March 2016) appearance by the Commissioner before the Committee during its review of the federal *Access to Information Act*. The Commissioner shared the office's experiences with Alberta's public sector access to information legislation, the FOIP Act.

Transcripts of ETHI Committee meetings are available at www.ourcommons.ca/Committees/en/ETHI.

PIA AND BREACH WORKSHOPS

The OIPC continued to host privacy impact assessment and privacy breach training workshops in 2016-17, including:

- Two Privacy Breach Response and Reporting Workshops in Edmonton, May 2016 and October 2016
- Two Privacy Breach Response and Reporting Workshops in Calgary, June 2016 and October 2016
- Two Privacy Impact Assessment Workshops in Edmonton, June 2016 and October 2016

The Privacy Breach Response and Reporting Workshop starts with the premise, "It's not a matter of if you will have a privacy breach, it's when." The workshop comments on trends in the type and magnitude of breaches reported to the OIPC. The presenters give participants practical guidance from a regulator's perspective, based on successful – and unsuccessful – strategies organizations have used to respond to breaches.

The Privacy Impact Assessment Workshop provides participants with the essentials for completing a PIA, and assists stakeholders in understanding how to review the impact that a new project may have on individual privacy.

CYBERA'S CYBER SUMMIT

The Commissioner was invited to deliver a keynote presentation at Cybera's annual Cyber Summit in October 2016. The title of the presentation was "Cybersecurity from a Privacy Regulator's Perspective".

Topics addressed during the speech included the internet of things, privacy breaches, privacy education and privacy law from a European context, specifically how the European Union's *General Data Protection Regulation* may change the privacy law landscape globally.

CANADA-US CONNECTED HEALTH WORKSHOP

This workshop in Washington, DC focused on the alignment of concerns and priorities related to the emergence of mobile and connected health devices.

The Commissioner participated in a panel discussion with regulators from Canada and the United States. Discussion focused on the extent to which Canada and the United States have commonalities in regulatory oversight and identifying areas where cross-border collaboration could be achieved.

Other panelists included representatives from the United States' Food and Drug Administration, Federal Trade Commission, Department of Health and Human Services, and the Office of the National Coordinator for Health Information Technology, as well as participation from Health Canada, Canada Health Infoway and the multinational corporation, Johnson & Johnson.

Resources

- Guidance for Electronic Health Record Systems (June 2016)
- Review of the Personal Information Protection Act: Global Considerations (September 2016)
- Access Impact Assessment Guidelines for Proactive Disclosure (September 2016)
- Our Right to Know What Governments Know About Us Op-Ed (September 2016)
- Cybersecurity from a Privacy Regulator's Perspective Speech (October 2016)
- Privilege Practice Note (December 2016)

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.

NATIONAL SECURITY FRAMEWORK

All federal, provincial and territorial Privacy Commissioners and Ombudspersons signed onto a formal submission to the federal government's public consultation on Canada's national security framework.

Canada's Privacy Commissioners and Ombudspersons recognized the importance of providing law enforcement and national security agencies with adequate tools and measures to protect Canadians, but cautioned that these measures should not infringe on privacy rights of individuals who are not suspected of criminal or terrorist activities.

The submission addressed issues such as collection and use of metadata by national security agencies and law enforcement, encryption, and information sharing by government.

GLOBAL PRIVACY SWEEP

The OIPC, along with 24 privacy regulators around the world, looked at internet-connected devices to consider how well organizations communicate privacy matters to their customers. In Alberta, the review focused on smart meters used by utility companies for billing and insurance companies' usage-based insurance (UBI) programs for vehicles.

The Alberta results were generally positive and privacy issues and risks were adequately communicated.

Internationally, the report showed that of the more than 300 devices reviewed:

- 59% failed to adequately explain to customers how their personal information was collected, used and disclosed
- 68% failed to properly explain how information was stored
- 72% failed to explain how customers could delete their information off the device
- 38% failed to include easily identifiable contact details if customers had privacy concerns

The sweep was coordinated by the Global Privacy Enforcement Network, and follows previous sweeps on online services for children, website privacy policies and mobile phone apps.

The Global Privacy Enforcement Network was established in 2010 upon recommendation by the Organization for Economic Co-operation and Development. It aims 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. The informal network is comprised of 51 privacy enforcement authorities in 39 jurisdictions around the world.

SOCIAL SMARTS: PRIVACY, THE INTERNET AND YOU

The Office of the Privacy Commissioner of Canada republished its graphic novel aimed to help young Canadians improve their understanding of privacy and to help navigate their online worlds. Each provincial and territorial office had their logo included in the latest edition to increase distribution across Canada.

Media Awareness

TRADITIONAL MEDIA

While newsrooms across the country continue to face setbacks and cuts in light of declining advertising revenue, the OIPC continues to receive approximately the same number of media requests each year. In 2016-17, there were 108 media requests received compared to 105 in 2015-16.

The vast majority of requests came from reporters who work for print and/or online media outlets. Other requests came from radio and TV outlets and from professional subscription-based newsletter writers.

Topics of media interest varied – from privacy breaches affecting casinos, colleges and universities to delays in responding to access requests by government departments.

Similar to previous years, investigation reports related to government departments received the most media interest. These included the investigation reports on the leaking of a cellphone bill of a former Deputy Premier, delays in responding to access requests by Alberta Justice and Solicitor General, Executive Council and the Public Affairs Bureau, and delays in responding to access requests by numerous government departments and allegations of political interference in the processing of access requests.

Related to law enforcement, there were a handful of media requests related to a change in the frequency of disclosing homicide victims' names by some police services, while the privacy considerations associated with police street information checks, or "carding", were discussed in 2016-17.

While no one breach received overwhelming attention, there were several calls throughout the year on different breaches. These included a ransomware incident at the University of Calgary, computer system breaches at some Alberta-based casinos, a rogue employee incident at a college that had occurred more than one year prior to being made public, and health information breaches. There were a few media requests related to convictions for the unauthorized access of health information under HIA.

In addition, despite being a fairly complex topic, the Supreme Court of Canada's decision on the Commissioner's power to compel records claimed to be subject to solicitor-client privilege garnered several media requests.

Finally, the Commissioner submitted an op-ed to the Calgary Herald and Edmonton Journal titled "Our Right to Know What Governments Know About Us" to align with and recognize Right to Know Week. The focus of that op-ed was to dispel, in part, the myth that the access to information system in Alberta is only used by the media and opposition when, in fact, the majority of requests are made by individuals for their own information or for information about public programs and services.

SOCIAL MEDIA

There were 191 tweets, replies and retweets on the OIPC's Twitter account, @ABoipc, in 2016-17. This was a reduction of 53 total posts, or 22%, on the social media site compared to 2015-16.

The OIPC's social media presence is used to share recent decisions or orders issued by the office, publications, news releases or investigation reports, promote events, respond to questions, and where appropriate weigh in on a topic to inform Albertans about access to information and privacy laws.

The following three topics attracted the most attention on Twitter:

- A one-on-one interview the Commissioner did with Alberta Primetime on the investigation reports related to access to information request delays in Alberta.
- The news release on the Commissioner's response to the Supreme Court of Canada's decision related to the Commissioner's power to compel production of records over which a claim of solicitor-client privilege has been made.
- Promotion of the Data Privacy Day event on "Privacy Implications in the Networked Classroom: A Workshop", which was co-hosted with The eQuality Project and the Alberta Teachers' Association.

In addition, the Commissioner's Right to Know Week op-ed and the Commissioner's Message from the 2015-16 Annual Report received plenty of views through tweets.

FINANCIAL STATEMENTS

Independent Auditor's Report....66
Statement of Operations....67
Statement of Financial Position....68
Statement of Changes in Net Debt....69
Statement of Cash Flows....70
Notes to the Financial Statements....71
Schedule 1 – Salary and Benefits Disclosure....75
Schedule 2 – Allocated Costs....76

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, 2017, 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, 2017, 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
Merwan N. Saher, FCPA, FCA

Auditor General
July 10, 2017
Edmonton, Alberta

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
STATEMENT OF OPERATIONS

Year ended March 31, 2017

	2017		2016
	Budget	Actual	Actual
Revenues			
Prior Year Expenditure Refund	$ -	$ 25,375	$ 25,004
Other Revenue	-	178	1,745
	-	25,553	26,749
Expenses – Directly Incurred (Note 3b)			
Salaries, Wages, and Employee Benefits	$ 5,497,061	$ 5,501,760	$ 5,465,185
Supplies and Services	1,325,330	1,142,475	1,373,261
Amortization of Tangible Capital Assets (Note 4)	74,000	53,900	79,553
Total Expenses	6,896,391	6,698,135	6,917,999
Net Cost of Operations	$ (6,896,391)	$ (6,672,582)	$ (6,891,250)

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, 2017

	2017	2016
Financial Assets		
Cash	$ 200	$ 100
Accounts Receivable	3,646	3,281
	$ 3,846	$ 3,381
Financial Liabilities		
Accounts Payable and Accrued Liabilities	$ 358,122	$ 403,737
Accrued Vacation Pay	510,819	512,231
	$ 868,941	$ 915,968
Net Debt	$ (865,095)	$ (912,587)
Non-Financial Assets		
Tangible Capital Assets (Note 4)	$ 141,177	$ 122,967
Prepaid Expenses	10,737	7,035
	$ 151,914	$ 130,002
Net Liabilities	$ (713,181)	$ (782,585)
Net Liabilities at Beginning of Year	(782,585)	(739,851)
Net Cost of Operations	(6,672,582)	(6,891,250)
Net Financing Provided from General Revenues	6,741,986	6,848,516
Net Liabilities at End of Year	$ (713,181)	$ (782,585)

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, 2017

	2017		2016
	Budget	Actual	Actual
Net Cost of Operations	$ (6,896,391)	$ (6,672,582)	$ (6,891,250)
Acquisition of Tangible Capital Assets (Note 4)	-	(72,111)	-
Amortization of Tangible Capital Assets (Note 4)	74,000	53,900	79,553
Change in Prepaid Expenses	-	(3,701)	(6,740)
Net Financing Provided from General Revenue	6,822,391	6,741,986	6,848,516
Decrease in Net Debt	-	47,492	30,079
Net Debt, Beginning of Year	-	(912,587)	(942,666)
Net Debt, End of Year	$ -	$ (865,095)	$ (912,587)

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, 2017

	2017	2016
Operating Transactions		
Net Cost of Operations	$ (6,672,582)	$ (6,891,250)
Non-cash Items Included in Net Cost of Operations		
Amortization of Tangible Capital Assets (Note 4)	53,900	79,553
	(6,618,682)	(6,811,697)
(Increase) in Accounts Receivable	(365)	(10)
(Increase) in Prepaid Expenses	(3,701)	(6,740)
(Decrease) in Accounts Payable and Accrued Liabilities	(47,027)	(30,069)
Cash Applied to Operating Transactions	(6,669,775)	(6,848,516)
Capital Transactions		
Acquisition of Tangible Capital Assets (Note 4)	(72,111)	-
Financing Transactions		
Net Financing Provided from General Revenues	6,741,986	6,848,516
Cash, Increase	100	-
Cash, at Beginning of Year	100	100
Cash, at End of Year	$ 200	$ 100

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, 2017

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 of the Information and Privacy Commissioner 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 of the Information and Privacy Commissioner 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.

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

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2017

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

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 Schedule 2.

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) 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 major enhancements to existing systems is $250,000 and new systems development is $100,000.

d) 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, 2017.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2017

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	$ 360,200	$ 443,518
Additions	-	72,111	72,111
	$ 83,318	$ 432,311	$ 515,629
Accumulated Amortization			
Beginning of Year	$ 63,756	$ 256,796	$ 320,552
Amortization Expense	8,524	45,376	53,900
	$ 72,280	$ 302,172	$ 374,452
Net Book Value at March 31, 2017	$ 11,038	$ 130,139	$ 141,177
Net Book Value at March 31, 2016	$ 19,562	$ 103,404	$ 122,967

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

NOTES TO THE FINANCIAL STATEMENTS *(continued)*

March 31, 2017

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 $762,215 for the year ended March 31, 2017 (2016 – $808,135).

At December 31, 2016, the Management Employees Pension Plan reported a surplus of $402,033,000 (2015 - surplus $299,051,000) and the Public Service Pension Plan reported a surplus of $302,975,000 (2015 - deficit $133,188,000). At December 31, 2016, the Supplementary Retirement Plan for Public Service Managers had a deficit of $50,020,000 (2015 - deficit $16,305,000).

The Office also participates in a multi-employer Long Term Disability Income Continuance Plan. At March 31, 2017, the Management, Opted Out and Excluded Plan reported an actuarial surplus of $31,439,000 (2016 – surplus $29,246,000). 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.

	2017	2016
Obligations under operating leases and contracts	$ 17,419	$ 27,463

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

	Total
2017-18	$ 11,692
2018-19	5,727
	$ 17,419

Note 7 Approval of Financial Statements

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

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 1 - SALARY AND BENEFITS DISCLOSURE

Year ended March 31, 2017

	2017				2016
	Base Salary [a]	Other Cash Benefits [b]	Other Non-cash Benefits [c][d]	Total	Total
Senior Official					
Information and Privacy Commissioner	$ 235,809	$ 144,177	$ 103,304	$ 483,290	$ 258,521

[a] Base salary is comprised of pensionable base pay.
[b] Prior years compensation adjustments duly approved by the Standing Committee, were processed in June, 2016
[c] Other non-cash benefits include the government'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, and professional memberships and tuition fees.
[d] Other non-cash benefits for the Information and Privacy Commissioner includes $7,238 (2016: $8,811) being the lease, fuel, insurance and maintenance expenses for an automobile provided by the Office.

Financial Statements

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

SCHEDULE 2 - ALLOCATED COSTS

Year ended March 31, 2017

	2017				2016
	Expenses - Incurred by Others				
Program	Expenses [a]	Accommodation Costs [b]	Telephone Costs [c]	Total Expenses	Total Expenses
Operations	$ 6,698,135	$ 471,657	$ 16,193	$ 7,185,985	$ 7,397,628

[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] Telephone Costs is the line charge for all phone numbers.

APPENDICES

Appendix A: Cases Opened under FOIP, HIA, PIPA by Entity Type ..78
Appendix B: Cases Closed under FOIP, HIA, PIPA by Entity Type 81
Appendix C: Orders and Public Investigation Reports Issued 84

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

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

FOIP Entity Type	Advice and Direction	Authorization to Disregard 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			8									7	2				**17**
Colleges			4			1			1			6	1	4	2		**19**
Commissions			3									5		1	3		**12**
Committees																	**0**
Crown Corporations												1					**1**
Foundations			1									2					**3**
Government Ministries/Departments		3	14			6	20		1	10		9	168	10	184	12	**437**
Health Quality Council of Alberta																	**0**
Hospital Board (Covenant Health)										1							**1**
Law Enforcement Agencies			10					3		1		2	65			2	**83**
Legislative Assembly Office																	**0**
Local Government Bodies			1									1	1				**3**
Long Term Care Centres																	**0**
Municipalities		2	29			1	1			4		4	85	3	18	16	**163**
Nursing Homes																1	**1**
Office of the Premier/ Alberta Executive Council			1				2						29		1		**33**
Officers of the Legislature	2											1				1	**4**
Panels																	**0**
Regional Health Authorities (Alberta Health Services)		4	7			1				2			17	5	4	1	**41**
School Districts			5				2			1		2	18		9	8	**45**
Universities		1	5				1			1	1		21	1	7	4	**42**
Other			4			1	1			2		4	5		25		**42**
Total	**2**	**10**	**92**	**0**	**0**	**10**	**27**	**3**	**1**	**23**	**1**	**23**	**430**	**22**	**253**	**50**	**947**

Note: The statistics do not include Intake cases.

APPENDIX A: CASES OPENED 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 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)									4			1		**5**
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians														**0**
Chiropractors								29						**29**
Dental Hygienists								3						**3**
Dentists			1					7		1		1		**10**
Denturists														**0**
Government Ministries/Departments														**0**
Health Professional Colleges & Associations			1					1	6					**8**
Health Quality Council of Alberta			1					4	1					**6**
Hospital Board (Covenant Health)								1		2		4		**7**
Long Term Care Centres								1						**1**
Midwives														**0**
Minister of Health/Alberta Health			1					12	1	1	1	47		**63**
Nursing Homes								1				1		**2**
Opticians														**0**
Optometrists								6						**6**
Pharmacies/Pharmacists			3					198	1			2		**204**
Physicians			12			1	2	237	3	11		32		**298**
Primary Care Networks								14	1			5		**20**
Registered Nurses								21	1			1		**23**
Regional Health Authorities (Alberta Health Services)			50		1	1		44	3	13		31		**143**
Researchers														**0**
Research Ethics Boards									1					**1**
Subsidiary Health Corporations			1					3	1			2		**7**
Universities/Faculties of Medicine									2			2		**4**
Other							5	1	12	2		1		**21**
Total	**0**	**0**	**70**	**0**	**1**	**2**	**0**	**7**	**583**	**37**	**30**	**1**	**130**	**861**

Note: The statistics do not include Intake cases.

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

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

PIPA Entity Type	Advice and Direction	Authorization to Disregard 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			10								1		7		**18**
Admin & Support Services			4										5		**9**
Arts, Entertainment & Recreation			5			1		1					7		**14**
Child Day-care Services											5				**5**
Construction			5								4		2		**11**
Collection Agencies											1		1		**2**
Credit Bureaus											1				**1**
Credit Unions			1							1	1		4		**7**
Dealers in Automobiles			4								1				**5**
Educational Services			3							1	1		5		**10**
Finance			3					1	2		1		22		**29**
Health Care & Social Assistance			8						2	2	3		9		**24**
Information & Cultural Industries			1						1		1		9		**12**
Insurance Industry			4								6		7		**17**
Investigative & Security Services			1								1				**2**
Legal Services		2	15								2		9		**28**
Manufacturing			3			2					3		3		**11**
Medical & Diagnostic Laboratories			2								2		1		**5**
Mining, Oil & Gas			7								11		7		**25**
Nursing Homes/Home Health Care			3								5		5		**13**
Professional, Scientific & Technical			6			1				2	3		9		**21**
Public Administration			1							2					**3**
Real Estate, Rental, Leasing			21							1	8		4		**34**
Retail			12			1				1	6		25		**45**
Trades/Contractors			2							1			1		**4**
Transportation			1							1	2		3		**7**
Utilities			4												**4**
Wholesale Trade			2							1					**3**
Other			31			1				4	9		17		**62**
Total	**0**	**2**	**159**	**0**	**0**	**6**	**0**	**2**	**5**	**0**	**17**	**78**	**0**	**162**	**431**

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

FOIP

Entity Type	Advice and Direction	Authorization to Disregard 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			3				1					12	3		1		**20**
Colleges									1			2		4	3		**10**
Commissions			3				1					8		1	3		**16**
Committees																	**0**
Crown Corporations																	**0**
Foundations			1														**1**
Government Ministries/Departments			18			4	6		12		6	147	2	183	10		**388**
Health Quality Council of Alberta																	**0**
Hospital Board (Covenant Health)									1				3				**4**
Law Enforcement Agencies			9			1	3	3	2		2	52		2	3		**77**
Legislative Assembly Office																	**0**
Local Government Bodies											1						**1**
Long Term Care Centres																	**0**
Municipalities			16			2	1		4		4	55	9	18	9		**118**
Nursing Homes															1		**1**
Office of the Premier/ Alberta Executive Council							2				1	21		1			**25**
Officers of the Legislature	2										2				1		**5**
Panels																	**0**
Regional Health Authorities (Alberta Health Services)		3	8						1			21	5	2	1		**41**
School Districts			5				1		1		1	17		9	12		**46**
Universities			6						2	1		13	1	6	1		**30**
Other		1				1					4	4		25	1		**36**
Total	**2**	**4**	**69**	**0**	**0**	**8**	**15**	**3**	**0**	**24**	**1**	**21**	**352**	**23**	**251**	**46**	**819**

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 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			1	9				**13**
Associations, Boards, Councils, Committees, Commissions, Panels or Agencies, created by Custodians										1				**1**
Chiropractors									45					**45**
Dental Hygienists									3				1	**4**
Dentists			1						6				1	**8**
Denturists													1	**1**
Government Ministries/Departments														**0**
Health Professional Colleges & Associations									1	7				**8**
Health Quality Council of Alberta			1						3					**4**
Hospital Board (Covenant Health)									1				2	**3**
Long Term Care Centres			1						1					**2**
Midwives														**0**
Minister of Health/Alberta Health						1			18	2	2	1	53	**77**
Nursing Homes													1	**1**
Opticians														**0**
Optometrists									2					**2**
Pharmacies/Pharmacists			1			1			202	1	1		2	**208**
Physicians			13			6		1	216	2	8		25	**271**
Primary Care Networks									19				6	**25**
Registered Nurses									21	1				**22**
Regional Health Authorities (Alberta Health Services)			31			11			34	3	11		47	**137**
Researchers										1				**1**
Research Ethics Boards										2				**2**
Subsidiary Health Corporations									2	1			5	**8**
Universities/Faculties of Medicine									1	3			2	**6**
Other						3				4	1			**8**
Total	**0**	**0**	**48**	**0**	**0**	**25**	**0**	**1**	**576**	**37**	**23**	**1**	**146**	**857**

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

PIPA Entity Type	Advice and Direction	Authorization to Disregard 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			7								2		10		**19**
Admin & Support Services			3			1							3		**7**
Arts, Entertainment & Recreation			6					1					5		**12**
Child Day-care Services											5		3		**8**
Collection Agencies													1		**1**
Construction			6								1		3		**10**
Credit Bureaus			2								2				**4**
Credit Unions													4		**4**
Dealers in Automobiles			2								1		2		**5**
Educational Services			2			2				1	1		2		**8**
Finance									1				24		**25**
Health Care & Social Assistance			2						2	2			7		**13**
Information & Cultural Industries			2						1		1		10		**14**
Insurance Industry			2			1				1	5		10		**19**
Investigative & Security Services											2				**2**
Legal Services		1	5								4		7		**17**
Manufacturing			3			2					4		6		**15**
Medical & Diagnostic Laboratories			1								1		1		**3**
Mining, Oil & Gas		2	2								6		8		**18**
Nursing Homes/Home Health Care			1								4		1		**6**
Private Healthcare & Social Assistance											5		1		**6**
Professional, Scientific & Technical			4							2	3		7		**16**
Public Administration			1							3			1		**5**
Real Estate, Rental, Leasing			28								5		2		**35**
Retail			7			1				1	4		28		**41**
Trades/Contractors			2							1					**3**
Transportation			4							1	1		2		**8**
Utilities			4										1		**5**
Wholesale Trade			3							1			2		**6**
Other			22			2				3	10		13		**50**
Total	**0**	**3**	**121**	**0**	**0**	**9**	**0**	**1**	**4**	**0**	**16**	**67**	**0**	**164**	**385**

Note: The statistics do not include Intake cases.

APPENDIX C: ORDERS AND PUBLIC INVESTIGATION REPORTS ISSUED

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

FOIP Respondent	Orders	Public Investigation Reports	Total
Alberta Children's Services	1		1
Alberta Economic Development and Trade	1		1
Alberta Energy	1		1
Alberta Energy Regulator (AER)	1		1
Alberta Environment and Parks	18		18
Alberta Health Services	7		7
Alberta Human Rights Commission	1		1
Alberta Human Services	2		2
Alberta Justice and Solicitor General	31	1	32
Alberta Transportation	1		1
Athabasca University	1		1
Calgary Police Service	6		6
City of Calgary	2		2
City of Edmonton	1		1
City of St. Albert	1		1
Edmonton Catholic School District No. 7	2		2
Edmonton Police Service	3		3
Edmonton Public School District No. 7	1		1
Elk Island Public Schools Regional Division No. 14	1		1
Mount Royal University	1		1
Office of the Premier/Executive Council	2	2	4
Public Affairs Bureau	1	1	2
Service Alberta	3	1	4
Town of High River	1		1
Town of St. Paul	1		1
University of Calgary	2		2
University of Lethbridge	1		1
Workers' Compensation Board	1		1
Subtotal	95	5	100

HIA Respondent	Orders	Public Investigation Reports	Total
Alberta Health Services	2		2
Dr. Adeleye Adebayo	1		1
Subtotal	3	0	3

PIPA Respondent	Orders	Public Investigation Reports	Total
Accessible Accessories Ltd.	1		1
Alberta Assessors' Association	1		1
CLFN Sawmill & Training Centre Ltd.	1		1
G4S Secure Solutions Canada Ltd.	1		1
Ludgren & Young Insurance Ltd.	1		1
McLeod Law	1		1
REDI Enterprises Society	1		1
Subtotal	7	0	7

Total	**105**	**5**	**110**

No Decisions were issued under FOIP, HIA or PIPA in 2016-17.
No Investigation Reports were issued under HIA or PIPA in 2016-17.

FOIP Orders: 95 (99 cases)
FOIP Investigation Reports: 3 (5 cases)
HIA Orders: 3 (3 cases)
PIPA Orders: 7 (7 cases)

Notes:

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

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

Orders are recorded by the date the Order was signed, rather than the date the Order was publicly released. Investigation Reports are recorded by the date the Investigation Report was publicly issued.

A copy of all Orders, Decisions and Investigation Reports are available on the OIPC web site www.oipc.ab.ca.

www.oipc.ab.ca