THIRTY YEARS OF ACCESS AND PRIVACY SERVICE

2017 ANNUAL REPORT

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

1987 TO 2017

Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

June 14, 2018

The Honourable Dave Levac
Speaker of the Legislative Assembly of Ontario

Dear Speaker,

I have the honour to present the 2017 Annual Report of the Information and Privacy Commissioner of Ontario to the Legislative Assembly.

This report covers the period from January 1 to December 31, 2017.

Please note that additional reporting from 2017, including the full array of statistics, analysis and supporting documents, may be found within our online Annual Report section at www.ipc.on.ca.

Sincerely yours,

Brian Beamish
Commissioner

2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel/Tél: (416) 326-3333
1 (800) 387-0073
Fax/Téléc: (416) 325-9195
TTY/ATS: (416) 325-7539
Web: www.ipc.on.ca

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE 1

ABOUT US 9

OUR WORK 10

ACCESS TO INFORMATION 14
- MUNICIPAL LEGISLATION 15
- DELETION OF EMAILS 15
- PROMOTING UNDERSTANDING OF ACCESS ISSUES 16
- SIGNIFICANT ACCESS DECISIONS 16
- MEDIATED APPEALS 19
- JUDICIAL REVIEWS 20

PROTECTION OF PRIVACY 22
- DATA PRIVACY DAY 23
- *CHILD, YOUTH AND FAMILIES SERVICES ACT, 2017* 24
- IPC'S DE-IDENTIFICATION PUBLICATION WINS AT INTERNATIONAL CONFERENCE 24
- PRIVACY IN EDUCATION 24
- *POLICE SERVICES ACT* 25
- *ANTI-RACISM ACT* 25
- BIG DATA 25
- OPEN GOVERNMENT AND PRIVACY 26
- PRIVACY INVESTIGATIONS 26

CONSULTATIONS 30

HEALTH 32
- NEW CODE OF PROCEDURE FOR MATTERS UNDER *PHIPA* 34
- THREE-YEAR REVIEWS OF PRESCRIBED HEALTH ENTITIES AND PERSONS 34
- SIGNIFICANT *PHIPA* DECISIONS 35

30 YEARS OF ACCESS AND PRIVACY SERVICE 40

GUIDANCE AND FACT SHEETS 44

COMMISSIONER'S RECOMMENDATIONS 46

STATISTICS 50

FINANCIAL SUMMARY IBC

What has not changed in all of these years…is our unwavering pursuit of privacy protection within a more open, transparent and accountable Ontario.

Thirty Years of Access and Privacy Service

COMMISSIONER'S MESSAGE

2017 WAS A MILESTONE YEAR FOR THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER (IPC), ONE IN WHICH MY OFFICE PROUDLY CELEBRATED 30 YEARS OF ACCESS AND PRIVACY SERVICE TO ONTARIANS. For more than three decades, protecting and advancing access to information and personal privacy rights has been at the forefront of our work.

Much has changed since we first opened our doors in 1987. In 1988, the *Freedom of Information and Protection of Privacy Act (FIPPA)* came into force, followed by its municipal counterpart, *MFIPPA*, in 1991. The IPC has seen its mandate expand a number of times since then. In 2004, the *Personal Health Information Protection Act (PHIPA)* ushered in a new era of health privacy rights for Ontarians, and has since become the gold standard against which other health privacy statutes are measured. The IPC's mandate grew yet again in 2006 when universities were brought under *FIPPA*, and again in 2012 when hospitals followed suit. Soon, our mandate will undergo another historic expansion when, for the first time ever, children's aid societies and other child and family service providers will become subject to the IPC's oversight.

What has not changed in all of these years, however, is our unwavering dedication to privacy protection while pursuing a more open, transparent and accountable Ontario. Each expansion of our mandate has brought greater access to information, more government transparency and increased privacy rights for Ontarians.

Included in this annual report is a special anniversary retrospective, highlighting our 30-year legacy—from our extensive advocacy work to the major milestones and many successes we have

achieved as an oversight agency. The last three decades have been productive and rewarding for the IPC and 2017 unfolded in very much the same vein.

Privacy Day and Big Data

2017 began on a high note with our signature Privacy Day event, this year focusing on the theme of *Government and Big Data*. We welcomed privacy and big data experts who engaged in a lively discussion about the various privacy challenges that governments face in the era of big data. I used this special occasion to call on the Ontario government to modernize our access and privacy laws to ensure that public institutions harness data analytics in a privacy-protective manner. *FIPPA* and *MFIPPA* were designed almost 30 years ago, prior to the emergence of big data analytics as tools to identify trends, detect patterns and gather other valuable findings from the massive amount of information available to government institutions. With more organizations relying on data to develop evidence-based programs and policies, the need for legislative reform in this area has never been greater. My office will continue to work closely with institutions to ensure that the great promise of big data respects and protects their privacy rights.

Joint Resolution on Solicitor-Client Privilege

In 2017, I represented the IPC at the annual federal, provincial and territorial meeting of Information and Privacy Commissioners in Iqaluit, Nunavut. At the top of the agenda was a discussion about the Supreme Court of Canada's (SCC) 2016 decision in *Alberta (Information and Privacy Commissioner) v. University of Calgary*. In this decision, the court ruled that Alberta's IPC did not have the power to compel the production of records over which solicitor-client privilege is claimed. This ruling raises serious concerns for Canada's IPCs, who require this power to independently review appeals of access decisions and properly fulfil our respective mandates as the nation's access and privacy regulators.

This SCC decision was the impetus for passing a joint resolution, in which we called on governments to amend access and privacy laws to ensure that IPCs across Canada are expressly authorized to compel the production of records over which solicitor-client privilege is claimed. This is critical if we are to safeguard the independent review of such claims and verify that institutions are properly applying this exemption.

Student Privacy

My office collaborated with our federal counterparts on another important front in 2017. This time we partnered with the Office of the Privacy Commissioner of Canada in a joint research effort to evaluate online educational services. Our work was part of a larger, annual initiative coordinated by the Global Privacy Enforcement Network, made up of over 60 privacy enforcement authorities around the world who work to strengthen privacy protections in an increasingly data-rich landscape.

As part of this privacy initiative, our offices evaluated a number of online educational services to determine what personal information is collected, how it is used and disclosed, and what control users have over their personal information.

Our review included best practices for protecting student privacy and recommended that educators carefully examine privacy policies and terms of service to understand how students' information may be collected, used, and disclosed. We also urged educators to consult with school officials before selecting online educational services to ensure they comply with Ontario privacy laws.

Prescribed Health Entities and Registries

Every three years, my office reviews the privacy-related practices and procedures of prescribed entities and registries in the health sector. In 2017, the IPC conducted this review to determine whether they continue to meet the requirements under *PHIPA*.

As part of this year-long process, each of the four prescribed entities* and six prescribed registries** submitted detailed written reports and sworn affidavits to my office, attesting that their respective information practices and procedures are consistent with Ontario's health privacy law.

Based on our comprehensive reviews, my office was pleased to confirm that all prescribed entities and registries continue to have in place practices and procedures that protect the health privacy of Ontarians, and sufficiently maintain the confidentiality of their information.

* Cancer Care Ontario, Canadian Institute for Health Information, Institute for Clinical Evaluative Sciences, Pediatric Oncology Group of Ontario ** Cardiac Care Network of Ontario, INSCYTE, Cancer Care Ontario, Children's Hospital of Eastern Ontario, Ontario Institute for Cancer Research, Hamilton Health Sciences Corporation.

Global Privacy Award for IPC De-identification Guidelines

In 2017, our *De-identification Guidelines for Structured Data* won the inaugural International Conference of Data Protection and Privacy Commissioners' (ICDPPC) award for excellence in research. The ICDDPC awards attracted 90 entries from data protection and privacy authorities around the world and were announced at the 39th ICDPPC conference in Hong Kong.

Our guidelines are the first of their kind in Canada to use plain language to explain sophisticated de-identification concepts for the process of removing personal information from a record or data set. I was honoured to accept this award on behalf of the IPC and it was especially gratifying to have our efforts recognized on the global stage.

The IPC's *Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to US Border Officials via CPIC* was also recognized as a finalist in the dispute resolution, enforcement and compliance category. This report, and the subsequent court resolution, was the result of working collaboratively with the Toronto Police Service and privacy, mental health, and human rights stakeholders to develop privacy-protective measures that bring greater clarity and discipline to police disclosure practices.

An Ontario-Based Philadelphia Model for Sexual Assault Research

In 2017, my office engaged with the Kingston and Ottawa police, the Ottawa Rape Crisis Centre, and other policing and violence against women stakeholders on how to implement the US-based Philadelphia Model. This is a model where police

The success of our webinar series has helped us to overcome geographical barriers to delivering our mandate on behalf of all Ontarians, regardless of where they live or work.

and women's advocates regularly review closed sexual assault files to identify any investigative shortcomings related to, for example, biases or stereotypes. The centrepiece of our collaborative work was the development of a model Memorandum of Understanding (MOU) and confidentiality agreement, designed to set the terms for the review of sexual assault cases by police and external reviewers. Our Kingston-based model MOU and confidentiality agreement will help to ensure a privacy-protective framework is in place for other police services considering the use of the Philadelphia Model.

Outreach and Stakeholder Engagement

So much of what we do at the IPC involves educating public and health sector institutions—and the people they serve—about their access and privacy rights and obligations. In 2017, IPC staff delivered more than 100 presentations on leading and emerging access, privacy, and health privacy issues facing our public and health care sector stakeholders.

Our popular *Reaching Out to Ontario* series is a key element of our outreach program, with visits this past year to Thunder Bay and Windsor. These events featured a range of topics including the privacy risks of big data; the benefits of open contracting; how institutions can protect against ransomware attacks; recent developments in access to information laws; and the technical, physical and administrative safeguards that health care providers should implement to protect their patients' information.

My office continued to fulfil our commitment to increased engagement with audiences across the province through our interactive webinar series. One of the webinars we hosted this year focused on how the IPC interprets *FIPPA* and *MFIPPA* exemptions. This webinar exceeded all expectations, attracting more than 600 registrants who

mptions in *FIPPA* and *MFIPPA*

The Impact of Records and Information Management on Access and Privacy

watched the live presentation and participated in the Q&A session that followed. The webinar series has helped us to overcome geographical barriers to engaging with all Ontarians, regardless of where they live or work.

Annual Statistical Report Attestations of *FIPPA* Compliance

Every year, public institutions must submit an annual statistical report to the IPC – this responsibility forms an important part of their work and is required by law. One of my 2016 Annual Report recommendations was that all deputy ministers sign and submit an annual attestation to my office, indicating that their respective ministries are in compliance with the statistical reporting requirements set out in *FIPPA* and that their statistics are accurate.

This year my office received attestations from the deputy ministers of Ontario's 30 ministries, providing a strong level of accountability for the veracity of their 2017 statistical submissions.

Policy Consultations with Government

Much of the work at the IPC centres on providing advice on proposed legislation, programs and practices to ensure that they comply with Ontario's access and privacy laws. In 2017 alone, I provided my comments on four bills, including Bill 68, *Modernizing Ontario's Municipal Legislation Act, 2017*; Bill 84, the *Medical Assistance in Dying Statute Law Amendment Act, 2017*; Bill 89, the *Supporting Children, Youth and Families Act*; and Bill 160, the *Strengthening Quality and Accountability for Patients Act, 2017*. A common thread across all of my submissions was to urge the Ontario government to advance the basic tenets of open government and privacy protection and to ensure that these bills guard against the erosion of Ontarians' access to information and privacy rights.

Throughout 2017 my office consulted extensively with the Ministry of Children and Youth Services, the Ontario Child Advocate and the child welfare sector to support the implementation of the *Child, Youth and Family Services Act* (*CYFSA*). When Part X of this law comes into force, on January 1, 2020, the IPC will mark an historic expansion of its responsibilities. For the first time, Ontarians will have the right to access their personal information held by children's aid societies and other service providers and file privacy complaints against them with my office. My staff and I look forward to our expanded oversight and believe it will usher in an era of greater public accountability in Ontario.

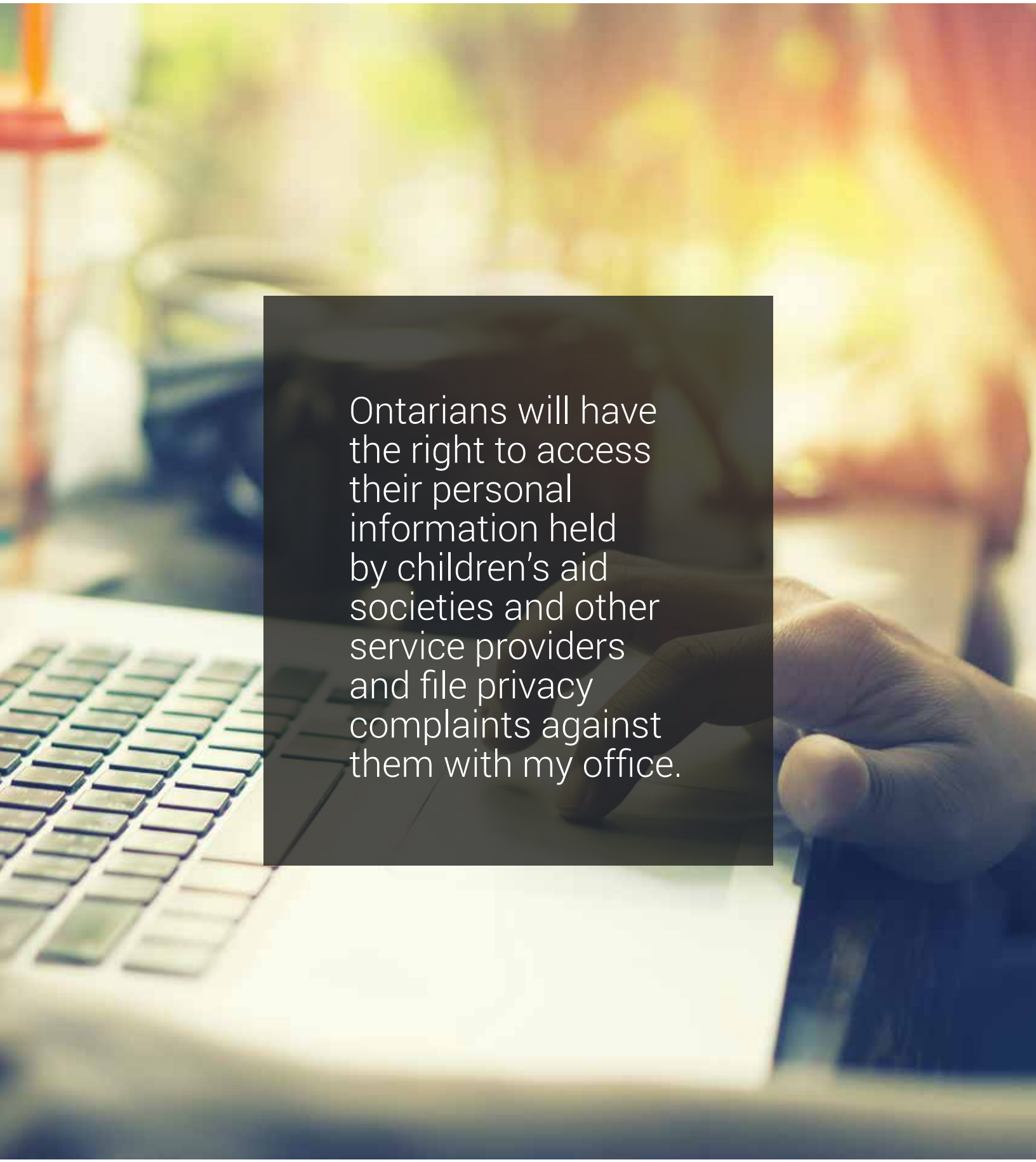
Mandatory Health Privacy Breach Reporting

PHIPA underwent a number of significant amendments in 2017, one of which requires that health care providers, such as hospitals, medical offices and others who deal with patient information, report certain health privacy breaches to my office. To help health care organizations and professionals understand and meet their new mandatory reporting requirements, the IPC published privacy breach reporting guidelines that outline reporting criteria and explain when and in what circumstances these bodies must notify the IPC of a breach. I was pleased to see this amendment come into effect on October 1, and believe it will better protect patient privacy and improve accountability and transparency across Ontario's health care system. Our front-line staff was certainly put to the test by the resulting increase in reports. The number of breaches reported to our office more than doubled for the last three months of 2017, compared to the same period in 2016. I was once again impressed by the agility with which our Tribunal Services staff responded to this dramatic increase in workload.

Final Thoughts

As I reflect on the IPC's 30-year history, I would like to thank our staff—past and present—for their professionalism in meeting the many pressures and demands we have faced as an organization. Our work would not be possible without their dedication to protecting and advancing Ontarians' access and privacy rights. Their ongoing commitment to excellence has helped to make the IPC one of the most respected oversight agencies in the country. I feel confident that in the years ahead my office will continue to build on the progress we made over the last 30 years.

Brian Beamish
Commissioner


Ontarians will have the right to access their personal information held by children's aid societies and other service providers and file privacy complaints against them with my office.

OUR VALUES

RESPECT | We treat all people with respect and dignity, and value diversity and inclusiveness.

INTEGRITY | We take accountability for our actions and embrace transparency to empower public scrutiny.

FAIRNESS | We make decisions that are impartial and independent, based on the law, using fair and transparent procedures.

COLLABORATION | We work constructively with our colleagues and stakeholders to give advice that is practical and effective.

EXCELLENCE | We strive to achieve the highest professional standards in quality of work and delivery of services in a timely and efficient manner.

OUR STRATEGIC GOALS

Uphold the public's right to know and right to privacy

Encourage open, accountable and transparent public institutions

Promote privacy protective programs and practices

Ensure an efficient and effective organization with engaged and knowledgeable staff

Empower the public to exercise its access and privacy rights

For three decades, protecting and advancing access to information and personal privacy rights has been at the forefront of our work.

ABOUT US

Established in 1987, the Office of the Information and Privacy Commissioner of Ontario (IPC) provides independent oversight of the province's access and privacy laws.

The *Freedom of Information and Protection of Privacy Act* (*FIPPA*) applies to over 300 provincial institutions such as ministries, provincial agencies, boards and commissions, as well as community colleges, universities, local health integration networks, and hospitals.

The *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) applies to over 1,200 municipal institutions such as municipalities, police services boards, school boards, conservation authorities, boards of health, and transit commissions.

The *Personal Health Information Protection Act* (*PHIPA*) covers individuals and organizations in Ontario that are involved in the delivery of health care services, including hospitals, pharmacies, laboratories, and Ontario's Ministry of Health and Long-Term Care, as well as health care providers such as doctors, dentists, and nurses.

Our Work

Commissioner

The Commissioner is appointed by the Legislative Assembly of Ontario and is independent of the government of the day. His mandate includes resolving access to information appeals and privacy complaints, educating the public about access and privacy issues, reviewing information practices and commenting on proposed legislation, programs, and practices.

In 2017, the IPC was mentioned more than 100 times in the media and made 103 presentations to stakeholder and public audiences.

Tribunal

Intake

The Registrar receives all access appeals and privacy complaints, including health privacy complaints, and directs them to the appropriate department. Intake can screen out or resolve appeals or complaints at an early stage. Our intake analysts also serve as our front-line response to privacy breaches.

In 2017, our Registrar received:

- 1,392 access appeals
- 629 health complaints
- 268 privacy complaints

We closed 246 privacy and 538 health complaints at intake in 2017.

Investigation and Mediation

Our team of investigators gather information and resolve privacy complaints, including health

privacy complaints, while our team of mediators work to resolve or narrow the issues in access appeals with a view to a mutually agreeable solution. While our decisions attract the most attention, the majority of access appeals and privacy complaints are resolved through mediation.

In 2017, 686 access to information appeals were fully resolved at the mediation stage. Ten privacy complaints moved to Mediation and Investigation and six were closed. One was resolved through mediation and five resulted in an investigative report. Our *PHIPA* investigators also issued four decisions, closing breach investigations.

Adjudication

When a resolution cannot be found through mediation, access appeals and health complaints are forwarded to an adjudicator who will decide whether to conduct a formal inquiry. The adjudicator collects and reviews evidence and arguments and issues a final and binding decision. A court review of IPC decisions is available in some limited circumstances.

TRIBUNAL SERVICES OVERVIEW

- 1,392 ACCESS APPEALS RECEIVED
- 686 ACCESS APPEALS SETTLED AT THE MEDIATION STAGE
- 1,414 ACCESS APPEALS CLOSED
- 268 PRIVACY COMPLAINTS RECEIVED
- 273 PRIVACY COMPLAINTS CLOSED
- 629 HEALTH COMPLAINTS RECEIVED
- 617 HEALTH COMPLAINTS CLOSED
- 140 PROVINCIAL ORDERS ISSUED
- 135 MUNICIPAL ORDERS ISSUED
- 26 *PHIPA* DECISIONS ISSUED

In 2017, our adjudicators closed 140 provincial access to information appeals through orders, 135 municipal appeals through orders and 22 *PHIPA* decisions.

Legal

Our legal department works in close collaboration with and provides legal advice and support to the Commissioner and other departments. Our lawyers frequently provide advice and comments with respect to proposed legislation, programs and technologies in the government and health sectors. They also represent the Commissioner in judicial reviews and appeals of the IPC's decisions and in other court cases regarding access to information and privacy issues.

In 2017, our Legal Services Department made more than 32 presentations and represented the Commissioner in six court hearings. Legal Services also represented the IPC as an intervener in a case before the Supreme Court of Canada.

Policy

Our policy analysts research, analyze, and provide advice on current, evolving and emerging access and privacy issues. Public organizations will frequently ask our policy analysts to examine and review their access and privacy practices. They also examine and provide comments on any proposed legislation that may affect the rights of Ontarians.

In 2017, our Policy Department released nine guidance documents, fact sheets and reports, and provided consultations and advice to a variety of public sector organizations and made more than 21 presentations where they provided information and insight on privacy and access issues.

Health Policy

Our health policy team researches privacy issues relating to personal health information and provides guidance through education, consultation, and comment on health policy and legislation. They also conduct reviews of the information practices of prescribed entities and persons on a tri-annual basis.

In 2017, Health Policy issued eight publications, helped develop amendments to health privacy legislation, and consulted with and presented to numerous organizations.

Communications

Communications promotes the work of the IPC and engages in public information campaigns and outreach initiatives to inform and empower both the public and public servants about matters of access and privacy. Our communications team also manages the IPC website, social media channels, media relations, and public events.

In 2017, Communications fielded more than 76 media calls, developed two webinars, and oversaw three major events that attracted over 800 people, in person and via webcast. Communications responds to thousands of calls and emails from the public through our public enquiry lines each year.

Corporate Services and Technology

From overseeing organizational operations such as human resources and monitoring expenditures to providing technical support, our Corporate Services and Technology department provides the day-to-day operational support and infrastructure needed for the Commissioner and IPC staff to do their jobs effectively and efficiently.

The IPC has long been a champion for increased transparency as a means to support accountability and civic engagement.

ACCESS TO INFORMATION

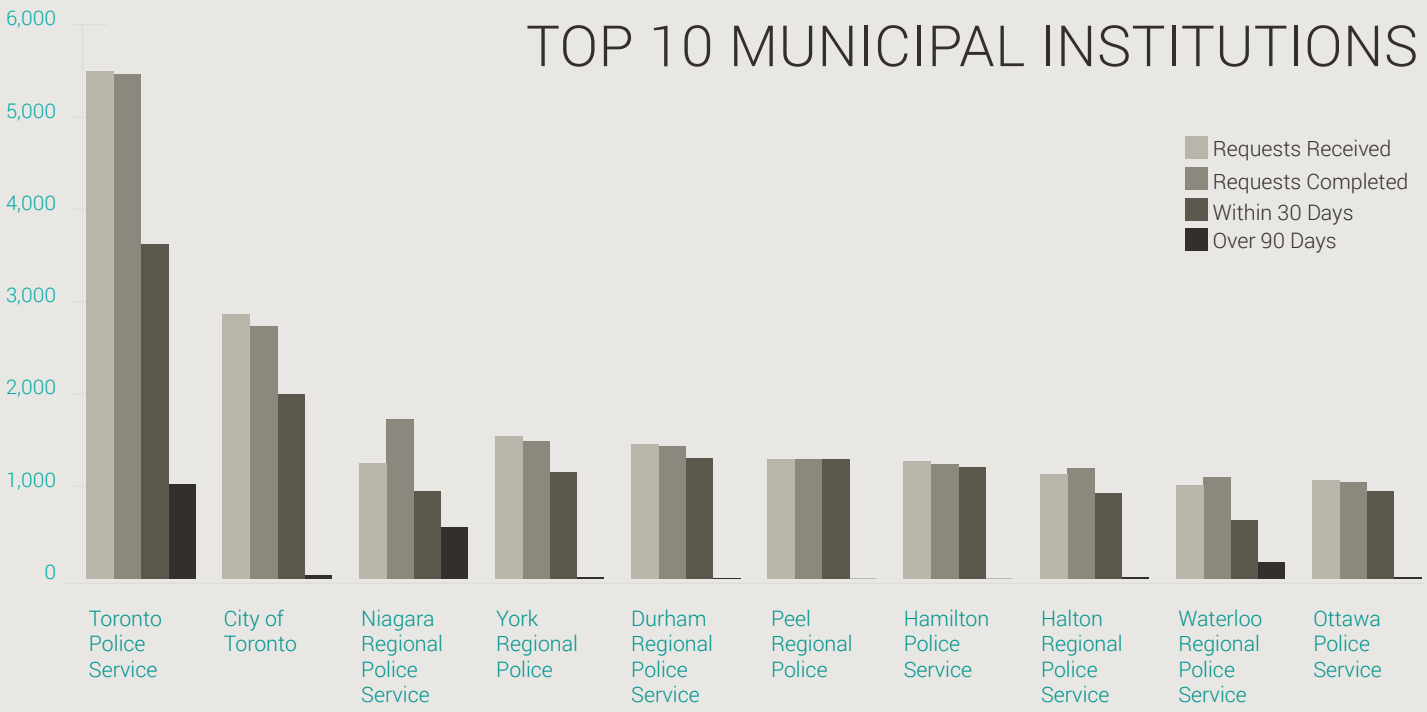
OPENNESS AND TRANSPARENCY ARE ESSENTIAL TO MAINTAINING THE PUBLIC'S TRUST AND CONFIDENCE IN GOVERNMENT INSTITUTIONS. The IPC has long been a champion for increased transparency as a means to support accountability and civic engagement. Over the past year, the IPC has engaged in activities on a number of fronts to support the public's right to know.

Municipal Legislation

Open meetings about government activities are essential to democracy, shining a light on policy development and promoting accountability for public spending. This year the IPC spoke out about changes to Ontario's *Municipal Act* and the *City of Toronto Act*, which expands the criteria a municipality or local board can use to close all or part of a meeting to the public. In its submission to the legislative committee related to Bill 68, the IPC questioned the need to broaden the exceptions to the open meeting requirement and emphasized the impact of closed-door meetings on the public's right to access information. The government made the legislative changes to the closed meeting rules despite the IPC's concerns.

Deletion of Emails

In 2017, the gas plants matter came before the courts and in early 2018 one individual was found guilty of criminal offences related to the deliberate destruction of documents. Our office investigated allegations political staff inappropriately deleted emails about the gas plant cancellations when they originally surfaced back in 2013. At that time, we found that the deletions were in violation of the *Archives and Recordkeeping Act* and recommended amendments to Ontario's access and privacy laws to address the responsibility of institutions to ensure key decisions are documented. In light of the recent conviction and a resolution passed



by all of Canada's information commissioners, the IPC continues to call on the government to create a legislated duty for public entities in Ontario to document matters related to their deliberations, actions, and decisions.

Promoting Understanding of Access Issues

A basic principle of Ontario's access and privacy laws is that the public has a right of access to government-held information, and exemptions from this right of access should be limited and specific. This year, our office hosted a webinar for freedom of information coordinators and other frontline staff to enhance their understanding of this topic. Participants had the opportunity to hear from a panel of IPC experts and ask questions.

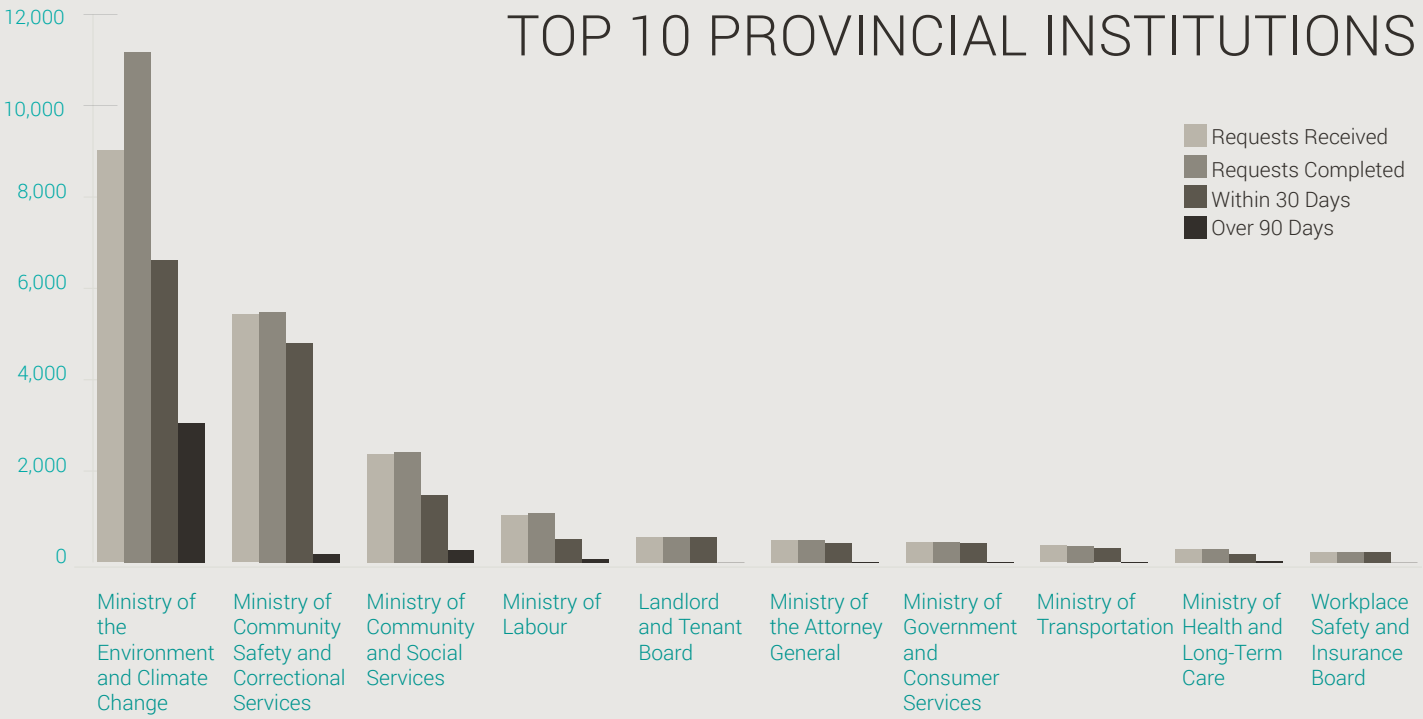
Records and information management (RIM) practices can have far-reaching impacts, helping or hindering an institution's ability to respond to access requests from the public. In 2017, our office released an educational video for institutions, to help them understand the relationship between effective RIM practices and their ability to meet their responsibilities under Ontario's access laws.

Over the past year, our office published a number of guidance materials on access-related topics to increase understanding among institutions and the public. These included fact sheets on *Frivolous and Vexatious Requests*, and *Reasonable Search*, which address the issues of managing excessive requests and how institutions and requesters can ensure adequate searches for records.

Significant Access Decisions

Our Tribunal Services team issued a number of decisions this year, providing guidance on the application of *FIPPA* and *MFIPPA*, including:

MO-3471 – A request was made for access to communications sent or received by staff of a city councillor concerning that councillor's Twitter account. Our office upheld the City of Toronto's decision to



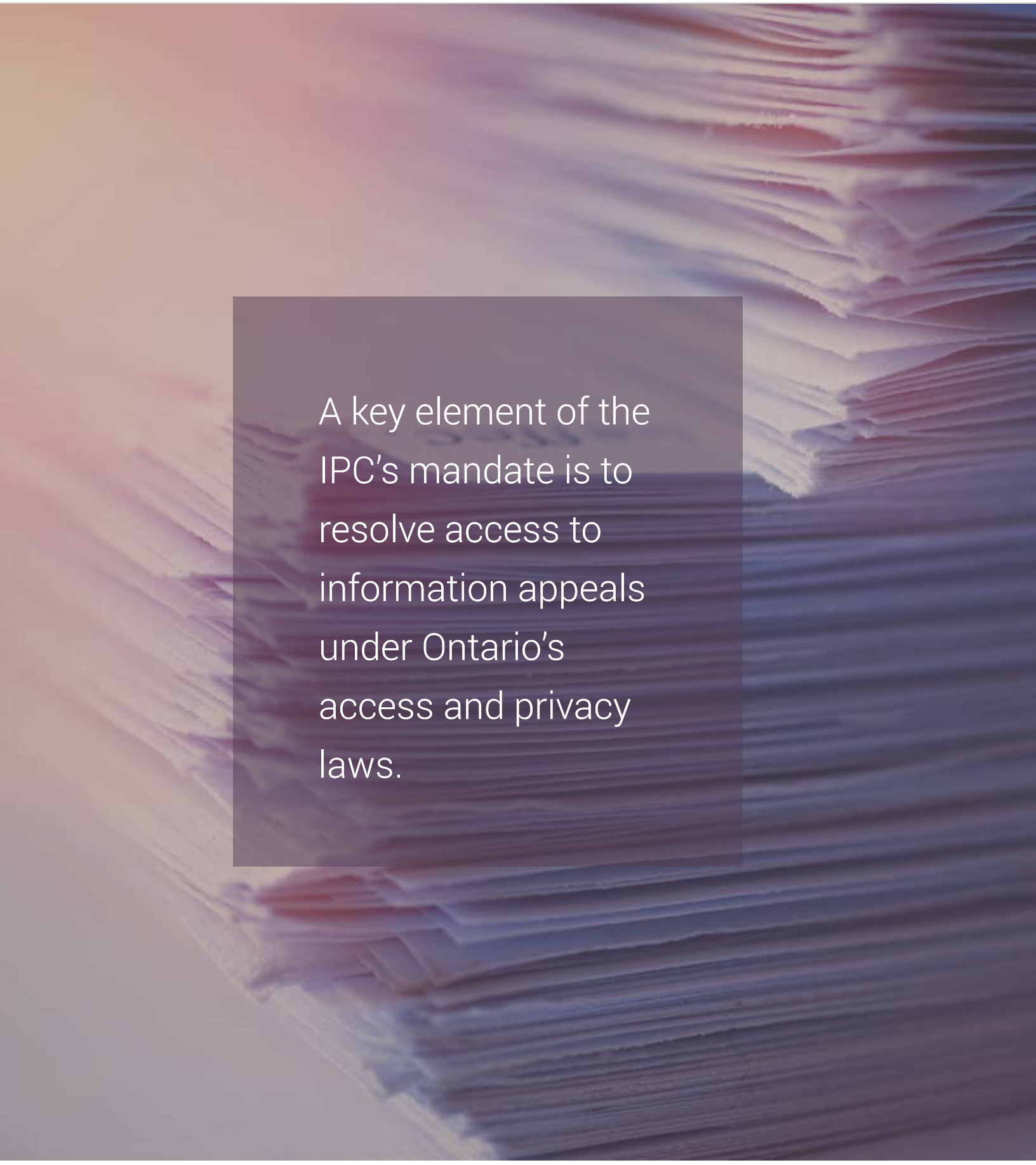
deny access to the records. The adjudicator determined that the records were personal, political records relating to the councillor's activities as an elected representative and were not under the control of the city.

MO-3476 – A requester sought information about police street checks and racial data from the Peel Regional Police. The police denied access to six records, claiming they contained advice and recommendations. The IPC partially upheld their decision, denying access to one record but ordering the release of the others based on a compelling public interest—the accurate reporting of race data as it related to street checks of individuals.

PO-3717 – A request was made to the Ministry of Energy for reports related to the progress of the Darlington Nuclear Generating Station refurbishment. The ministry decided not to release the records on the basis they contained commercial and third-party information and that release would result in harm. Our office found that there was insufficient evidence to establish the harms to the ministry or the third party's economic or other interests, and ordered their release.

MO-3514 – An individual requested access to a motor vehicle collision report related to a car accident they were involved in. The police denied access to the report on the grounds that the information contained in the record was already publicly available. The IPC upheld the decision, finding that a regular system of access was available to allow anyone to obtain the records.

PO-3691 – A requester made numerous requests to the Public Guardian and Trustee (PGT) for records relating to the estates of named deceased individuals (including 40 requests within a nine-week period and 116 total requests). When the PGT limited the number of requests the individual could make at one time, the requester appealed to our office. The IPC found that the number of requests established a pattern of conduct that interfered with the operations of the institution, and that the requests were frivolous and vexatious. Our office limited the number of requests the individual could make to five at any given point in time.



A key element of the IPC's mandate is to resolve access to information appeals under Ontario's access and privacy laws.

Mediated Appeals

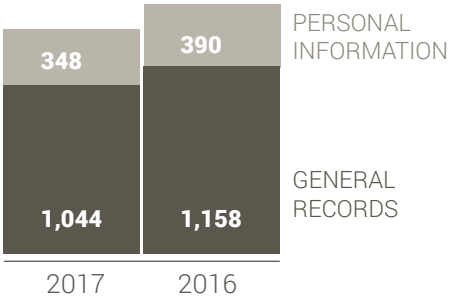
A key element of the IPC's mandate is to resolve access to information appeals under Ontario's access and privacy laws. This is frequently achieved through the mediation process, where parties have an opportunity to explain their respective positions, clarify issues, and discuss potential settlement options.

Our office resolves a large volume of access to information appeals through mediation. Here are some highlights from the past year:

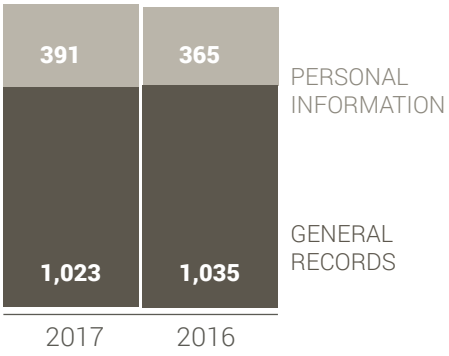
- A police service received a request from an individual for records relating to a security breach involving her credit card. The police denied access to some of the records on the grounds they contained the personal information of another individual. The mediator obtained consent from the other individual to disclose their information, which resulted in the police granting full access to a police report. Following clarification of other issues during mediation, the police also granted access to statistical information previously withheld. These efforts also resulted in the police changing aspects of their policy regarding the disclosure of statistical information. Going forward, they will routinely disclose statistical information that is not subject to mandatory exemptions.

- An individual requested the minutes and audio recording of a town meeting held in closed session. The town denied access to all records, citing the closed meeting exemption. During mediation, the town agreed to transcribe the audio recording of the meeting. The town then exercised its discretion to provide partial access to both the minutes and the transcript, as well as documents considered by the council during the meeting.

APPEALS OPENED IN 2017



APPEALS CLOSED IN 2017



- Police denied a request by an individual for her own report relating to a recent sexual assault on the grounds it was part of a continuing investigation. Through mediation, the individual requesting the report was able to explain her reasons for the request. The documentation was required to alert a foreign embassy of her sexual assault claim against an individual who was currently traveling to his home country. With the assistance of a mediator and additional information about the circumstances related to the request, the police agreed to provide partial access to the report within hours.

- An individual requested statistical records related to faculty members at a university and received a costly fee estimate to locate and prepare the records. During mediation, the university detailed the technical difficulties they were encountering trying to extract the records from an outdated database. During the discussion it was determined that if the request was narrowed slightly, it would significantly speed up the search. The requester amended the request and the university issued a revised fee estimate of about half the original cost. The requester received the records and was satisfied with the result.

Judicial Reviews

OUR LEGAL DEPARTMENT REPRESENTS THE COMMISSIONER IN JUDICIAL REVIEWS AND APPEALS OF THE IPC'S DECISIONS.

Treasury Board Secretariat and Third-Party Records

The Treasury Board Secretariat received a request for access to a copy of a benchmarking report prepared by a third party. After consulting with the third party, the Treasury Board granted partial access to the report, with portions withheld, citing the third-party exemption. The requester appealed the Treasury Board's decision to our office. In Order PO-3663, the adjudicator found that the information at issue was not exempt under the third-party records exemption because disclosure could not reasonably be expected to result in any of the commercial or competitive harms alleged. She ordered disclosure of the information. The affected party sought a judicial review before the Ontario Divisional Court. The Court dismissed the application for judicial review stating that, in its view, the adjudicator's decision was reasonable.

Ministry of Health and Long-Term Care—Access to Physicians' OHIP Billing Information

The record at issue in this appeal, created in response to a request by a journalist, sets out the total dollar amounts paid annually to the top 100 OHIP billers, their names and their medical specialties, for the years 2008 to 2012. The ministry disclosed the dollar amounts and most of the specialties, but withheld the physicians' names and some of the specialties under the personal privacy exemption in *FIPPA*. One of the parties to the appeal also raised the third-party information exemption in *FIPPA*. The appellant claimed that the public interest override applied. In Order PO-3617, the adjudicator found that the record does not contain personal information, and as a consequence, the personal privacy exemption does not apply. The adjudicator also found that the third-party exemption did not apply, and that there was a compelling public interest in the disclosure of the record. The IPC ordered the ministry to disclose the record in its entirety to the journalist.

Ontario's Divisional Court dismissed three applications by doctors' groups to quash the order, ruling that it was reasonable. The Court agreed that the names of the doctors, in conjunction with the amounts they receive in OHIP payments and their medical specialties, is not "personal information." The Ontario Court of Appeal will hear appeals from this decision in June 2018.

Ryerson University and Third-Party Information

The university received a request under *FIPPA* for an agreement between it and a bank relating to the issuance of university-branded credit cards. The university granted partial access to the agreement, withholding some information, citing the third-party information exemption. Both the requester and the bank appealed the university's decision, with the requester arguing that none of the agreement is exempt and the bank arguing that the entire agreement is exempt under that same section of *FIPPA*. In Order PO-3598, the adjudicator found that none of the information in the agreement was "supplied" to the university, therefore the exemption for third-party information did not apply. She ordered the university to disclose the agreement in its entirety to the requester.

The bank, as the affected third party, sought a judicial review of this order in the Divisional Court. The Court dismissed the application stating that the decision of the adjudicator fell within a reasonable range of outcomes given the terms of the legislation and the facts before her.

Ministry of the Attorney General and Office of the Children's Lawyer for Ontario—Application of *FIPPA*

PO-3520—The Ministry of the Attorney General received a request for information related to services provided to the requester's two children by the Office of the Children's Lawyer for Ontario (OCL) in custody and access proceedings. The ministry advised that the OCL took the position that *FIPPA* does not apply to litigation files where it provides services to children. As a result, the ministry claimed that records related to these files were not in its custody or under its control and denied the request.

In Order PO-3520, the adjudicator found that records of the OCL covered by the request were in the custody or control of the ministry and ordered the ministry to issue an access decision to the requester, which could be made by the OCL.

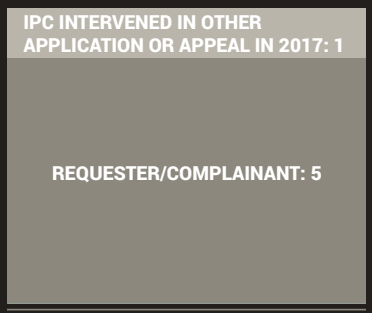
The OCL filed an application for judicial review, which was dismissed by the Ontario Divisional Court. The Ontario Court of Appeal heard the OCL's appeal in late 2017 but has not yet issued its decision.

Algoma Public Health and a Report Relating to Allegations of Wrongdoing

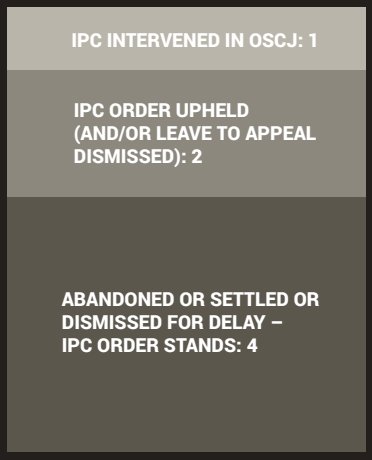
MO-3295—Algoma Public Health (APH) received a request for access to the "final report of [the] 2015 KPMG Forensic Review." The report related to whether a conflict of interest existed regarding the appointment of APH's former interim CFO, and whether any funds were subsequently misappropriated or lost by APH. While APH determined that an exemption for personal privacy under *MFIPPA* applied, it granted access to the report under the public interest override. An affected party appealed APH's decision, claiming disclosure would expose her to civil liability. The affected party also claimed that the public interest override did not apply in the circumstances. The IPC decided that the personal privacy exemption applied to the record, but agreed with APH that there was a compelling public interest in disclosure of the record. Accordingly, the IPC ordered AHP to disclose the record to the requester.

The affected party sought a judicial review of the order and the associated reconsideration order and both orders were quashed by the Divisional Court. The appeal was sent back to the Commissioner for a new hearing.

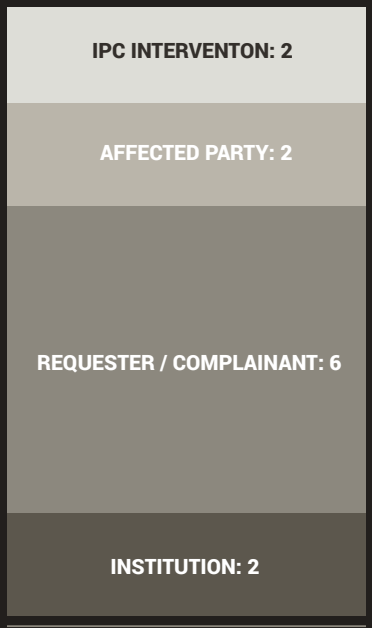
The IPC was granted leave to appeal the Divisional Court's decision to the Ontario Court of Appeal. The appeal is expected to be heard in fall 2018.



New Judicial Review applications & IPC interventions in 2017: 6



Judicial Reviews & IPC interventions Closed and/or Heard in 2017: 7



Ongoing Judicial Reviews & IPC interventions as of December 31, 2017: 12

The IPC remains steadfast in its commitment to protect the privacy of all Ontarians.

PRIVACY

IN 2017, IPC'S WORK SPANNED A RANGE OF TOPICS RELATED TO PRIVACY PROTECTION IN ONTARIO.

Data Privacy Day

The IPC began 2017 by hosting a public event to mark International Privacy Day. Given that big data is changing the landscape of how Ontario institutions develop public policy and design government programs the topic for 2017 was *Government and Big Data*.

Four expert panelists and close to 150 attendees engaged in lively discussions that focused on issues such as the benefits and risks of big data, measures to protect privacy, the potential for biased data sets and identifying solutions to the challenges governments face in a big data world.

Participation in the event extended beyond the venue with more than 700 devices tuned in to watch the live webcast. The event also reached more than 22,000 Twitter accounts and more than 800 LinkedIn accounts.

International Privacy Day offered an appropriate occasion to release our new fact sheet, *Big Data and Your Privacy*, to raise awareness of the public's right to privacy protection in the big data landscape.

There are tremendous opportunities available to government to develop evidence-based programs and policies using big data. To support this, the IPC has called on Ontario to modernize access and privacy laws to ensure that government institutions use data linking and big data analytics in a privacy-protective manner.

The IPC remains steadfast in its commitment to protect the privacy of all Ontarians. We will continue to work closely with government institutions to ensure that their use of big data respects and protects individual privacy rights.

Child, Youth and Families Services Act, 2017

Throughout 2017, we consulted and collaborated extensively with the Ministry of Children and Youth Services to support the development of the new *Child, Youth and Family Services Act, 2017* (*CYFSA*), and its regulations.

Under Part X of the *CYFSA*, and for the first time, Ontarians will have the right to access their personal information held by child, youth, and family service providers, including children's aid societies. They will also be able to file privacy complaints if these service providers do not follow the rules for collection, use and disclosure of personal information contained in the act. Our office has been designated as the oversight body in relation to Part X of the act, bringing child, youth, and family service providers within our jurisdiction.

In March 2017, Commissioner Beamish appeared before the Standing Committee on Justice Policy to provide the IPC's comments and recommendations to help strengthen the privacy protections in the *CYFSA*.

The majority of the *CYFSA* was proclaimed on April 30, 2018, with Part X scheduled to come into effect in January 2020. Our office is working with the Ministry of Children and Youth Services, the Ontario Child Advocate, the child welfare sector and other sectors to prepare for implementation.

This legislation represents a great step forward for Ontario's child and youth sector and will usher in an era of greater public accountability in Ontario.

IPC's De-identification Publication Wins at International Conference

In September, our *De-identification Guidelines for Structured Data* won the inaugural International Conference of Data Protection and Privacy Commissioners' (ICDPPC) award for excellence in research. The ICDPPC awards attracted 90 entries, in a variety of categories, from data protection and privacy authorities around the world and the winning entries were announced at the 39th ICDPPC conference in Hong Kong.

"De-identification" is the general term for the process of removing personal information from a record or data set. De-identification protects the privacy of individuals because once a data set is de-identified, it no longer contains personal information. If a data set does not contain personal information, its use or disclosure cannot violate the privacy of individuals.

Our guidelines are the first of their kind in Canada to use plain language to explain sophisticated de-identification concepts, with the benefit of being useful to a very wide audience.

Privacy in Education

The IPC recognizes that, more than ever, educators and students benefit from privacy education and digital literacy skills.

In May 2017, we worked with the Office of the Privacy Commissioner of Canada to review free online educational tools and services used in Ontario classrooms. The review was part of a larger international "sweep" effort coordinated by the Global Privacy Enforcement Network (GPEN).

In October, we published our *GPEN Sweep Report* summarizing our findings and outlining best practices for ensuring student privacy and compliance with Ontario privacy laws when using online services. We advised educators to consult school officials before choosing an online educational service and recommended that school board officials carefully examine privacy policies and terms of service before approving their use in the classroom. We also recommended that educators provide students with

ongoing guidance on how to configure and use the educational services in privacy-enhancing ways. For example, we learned that students could use pseudonyms instead of their real identities when using some online tools.

In November, the IPC jointly sponsored a workshop with the Ontario Association of School Business Officials at the annual "Bring IT Together" conference on educational technologies. The workshop, Privacy in the Networked Classroom, brought together teachers, school board administrators and IT staff to examine the uses and impacts of technology in schools. Renowned Canadian scholars shared new research on the benefits and risks posed by networked classroom technologies and the use of educational software in classrooms.

The IPC joined our fellow federal, provincial and territorial privacy regulators to encourage the Council of Ministers of Education to take steps to ensure that future generations of Canadians develop strong digital and privacy skills. These skills are the key to ensuring that young people are well equipped to exercise their privacy rights and responsibilities as digital citizens, and to succeed in a networked and data-driven world.

Police Services Act

On November 2, the government introduced Bill 175, the *Safer Ontario Act*, the largest transformation in policing and public safety in Ontario in over 25 years. The bill included a new *Police Services Act*, which gives the Minister of Community Safety and Correctional Services broad powers to collect and share personal information to enhance evidence-based decision-making. Our office worked with the ministry to ensure that measures to support a privacy protective approach to data collection and integration were included in the legislation. Our office also helped to ensure that improved transparency was at the heart of the bill. For example, we helped the ministry develop rules under the new *Policing Oversight Act* that require the publication of SIU investigation reports that conclude police should not face criminal charges in connection with the death or serious injury of a member of the public. The bill received Royal Assent on March 8, 2018.

Anti-Racism Act

In June, Ontario passed the *Anti-Racism Act, 2017* (*ARA*). Under this legislation, the government is responsible for developing and maintaining an anti-racism strategy that aims to eliminate systemic racism and advance racial equality. The government also has the authority to mandate public sector organizations to collect defined race-related information to support the purposes of the act.

The *ARA* requires the development of data standards governing the management of personal information, and that the government consult with the IPC on these standards to ensure robust privacy protections are in place.

The IPC is the oversight body for the privacy requirements under the *ARA*. Under this act, we have the authority to order an organization to change or discontinue its personal information handling practices if the practices contravene the *ARA* or the data standards. This order-making power is key to protecting the privacy of affected individuals. We can also make comments or recommendations on the privacy implications of any matter related to the *ARA*.

Big Data

Government institutions are increasingly relying on the analysis of big data to shape and improve the programs and services they provide to the public. While big data may benefit individuals, it also raises a number of privacy, fairness, and ethical concerns about how institutions use advanced technologies to process personal information. Institutions should understand and

address these concerns to prevent unexpected, invasive, inaccurate, or discriminatory uses of personal information.

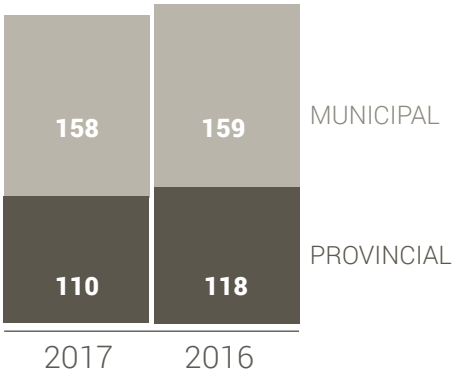
In May, the IPC released its *Big Data Guidelines* to inform institutions of the key issues to consider and best practices to follow when they conduct big data projects. These guidelines offer practical advice to ensure that personal information is appropriately collected, linked, analyzed, and used when making automated decisions about individuals. Institutions with the legal authority to conduct big data projects should follow the best practices developed in these guidelines.

The IPC will continue to work on issues related to big data and plans to release additional guidance documents aimed at specific sectors of government and at providing further information on some of the best practices identified in the *Big Data Guidelines*.

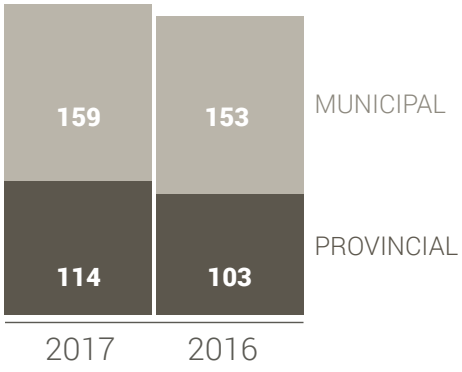
Open Government and Privacy

In our view, proactively addressing privacy risks from the outset is key to carrying out open government initiatives that enhance public services without compromising privacy. To assist institutions in putting open government into practice, this year we published *Open Government and Protecting Privacy*. This guide outlines methods for designing, implementing, and monitoring open government programs to support transparency while addressing potential privacy risks.

PRIVACY COMPLAINTS OPENED IN 2017



PRIVACY COMPLAINTS CLOSED IN 2017



Privacy Investigations

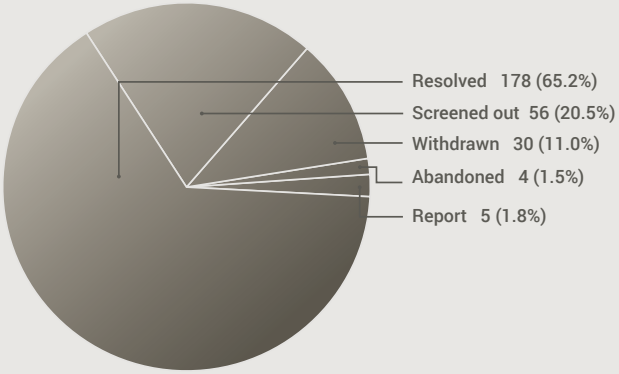
Our privacy investigations look at whether government institutions are protecting the personal information they collect and retain, and may result in recommendations to ensure compliance with Ontario's access and privacy laws.

Privacy Complaint PI16-3

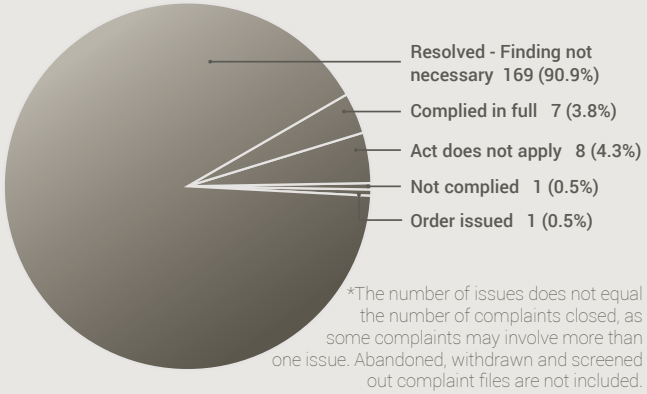
Ministry of Community Safety and Correctional Services

The IPC opened a Commissioner-initiated privacy complaint under *FIPPA*, against the Ministry of Community Safety and Correctional Services. The complaint related to the collection and destruction of personal information captured in a recording made by a police officer on his personal cell phone during a traffic stop. The IPC was unable to make a finding as to whether the record at issue contained personal information because the device that contained the recording had been discarded. We concluded that, in the particular circumstances, collection of the personal information would have been authorized under the act. Our report included the recommendation that the OPP amend its personal device policy to require staff to copy any operational information obtained on a personal device to an authorized OPP system or device within a reasonable time.

PRIVACY COMPLAINTS CLOSED BY TYPE OF RESOLUTION

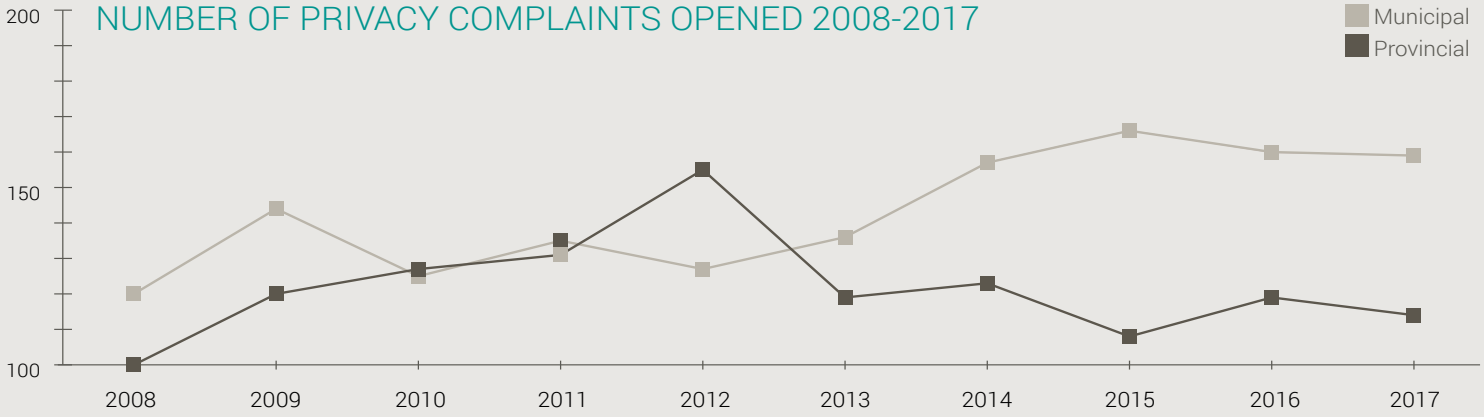


OUTCOME OF ISSUES* IN PRIVACY COMPLAINTS

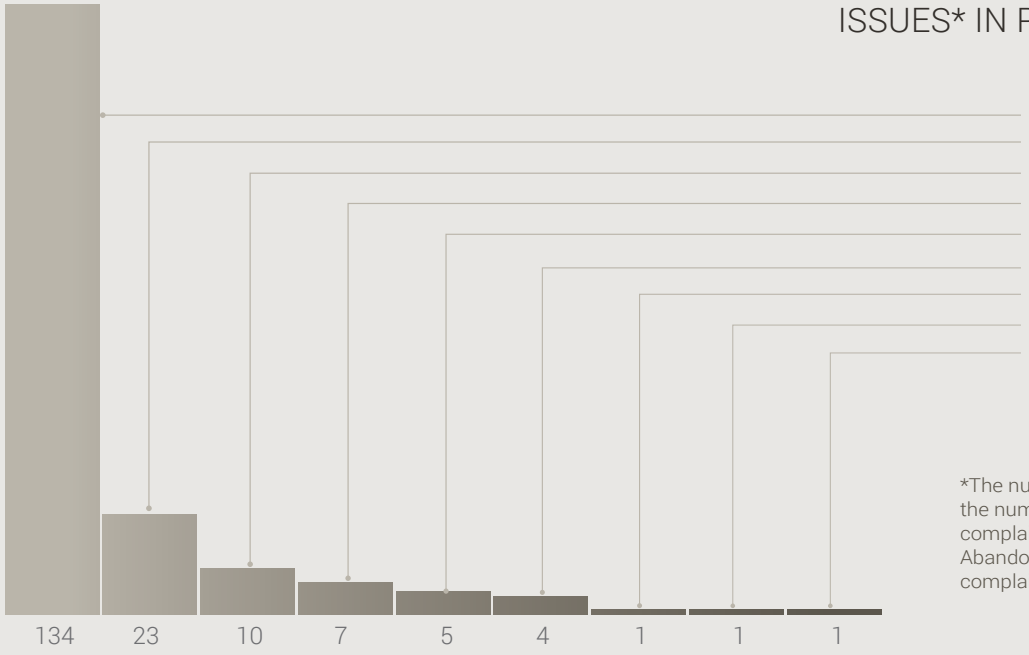


*The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue. Abandoned, withdrawn and screened out complaint files are not included.

NUMBER OF PRIVACY COMPLAINTS OPENED 2008-2017



ISSUES* IN PRIVACY COMPLAINTS



Disclosure (72.0%)
General privacy issue (12.4%)
Security (5.4%)
Collection (3.8%)
Access (2.7%)
Use (2.2%)
Consent (0.5%)
Notice of collection (0.5%)
Retention (0.5%)

*The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue. Abandoned, withdrawn and screened out complaint files are not included

Privacy Complaint MC16-7

Ottawa Police Services

Two Correctional Services Canada (CSC) employees filed complaints alleging that the Ottawa Police Service inappropriately disclosed personal information pertaining to criminal charges against them to their employer. CSC manages correctional institutions and supervises offenders under conditional release in the community. The investigation report concluded that the CSC is not an institution or a law enforcement agency, and the police's disclosure of personal information to CSC was not consistent with the requirements of *MFIPPA*. Our report noted that such requests for personal information should be made in writing to ensure a detailed record of the information requested, as well as noting the legislative authority under which the information is sought.

Privacy Complaint MI17-2

Greater Sudbury Police Services

The IPC opened a Commissioner-initiated privacy complaint against the Greater Sudbury Police Services after a journalist contacted the IPC about the Lion's Eye in the Sky Surveillance Program. The aim of the investigation was to ensure that the expansion of the surveillance program was in keeping with the act and current privacy best practices.

We found the surveillance program complied with the act. There were, however, opportunities to improve the existing privacy practices. The IPC identified concerns and through discussions with the IPC's policy unit related to signage, security, training, auditing, and retention of surveillance data, the police addressed the concerns, adopted our recommendations, and committed to comply with current privacy best practices.

Privacy Complaints Resolved at Intake

The IPC's Intake team, headed by the Registrar, serves as the IPC's front-line response to privacy breaches. The vast majority of privacy complaints we receive are resolved at Intake, and do not require investigation and mediation. These are some public-sector

privacy complaints that were resolved at Intake in 2017:

A Municipality

An individual submitted a complaint alleging that a city inappropriately disclosed information regarding his application to construct a front yard parking pad. As part of the approval process, a number of neighbours within a certain radius of the complainant's home were notified of the application. The city advised that the local municipal code requires public polling. Polling provides an opportunity for individuals who own or live in residences within the polling area to determine whether their properties and neighborhood may be affected. The city submitted that disclosure of the property address was authorized under *MFIPPA*. The IPC reviewed the city's response and the application of *MFIPPA* with the complainant, who was satisfied and agreed to withdraw the complaint.

A School Board

An individual submitted a complaint concerning the disclosure of her personal information by a school board to an individual who made a request for his own information. The complainant believed that even though her name had been redacted from the record disclosed to the requester, other information in the record could identify her. Following discussions with the IPC, the school board acknowledged its error, and issued a letter of apology to the complainant. The school board also expanded its training regarding access and privacy. The IPC was satisfied with the board's response.

A Township

An individual submitted a complaint alleging that a town in central Ontario had posted her Tax Arrears Extension Agreement online as part of the town's council meeting agenda, in contravention of the privacy provisions of the *MFIPPA*. The town acknowledged that it had improperly disclosed the complainant's personal information on its website. The town immediately removed the document from its website and apologized to the complainant. The town also made commitments to developing formal privacy policies and providing privacy training to its staff. The complainant and the IPC were satisfied with the steps taken by the town and the file was resolved.

Anti-Racism Directorate, Cabinet Office

- Bill 114, *Anti-Racism Act, 2017*

City of Brampton

- Access and Privacy Guide for Council

Durham District School Board

- Workforce Census

Durham Regional Police Service

- Body Worn Camera Pilot Project

Global Privacy Enforcement Network (GPEN)

- GPEN "Sweep"—International Study of User Controls (Online Educational Services in Ontario schools)

Independent Electricity System Operator

- Data Strategy Advisory Council Terms of Reference

Kingston Police Service, Ottawa Police Service and the Ottawa Rape Crisis Centre

- Philadelphia model-related privacy guidance for external sexual assault and domestic violence case review committees

Metrolinx

- Disclosure of PRESTO Card information to law enforcement

Ministry of the Attorney General

- Katelynn Sampson Inquest Recommendations
- Bill 175, *Safer Ontario Act, 2018—Policing Oversight Act, 2018*, and *Ontario Policing Discipline Tribunal Act, 2018*

Ministry of Children and Youth Services

- *Child, Youth and Family Services Act, 2017*—Amendments and Regulations
- Child Welfare Identity-Based Data Collection Initiative
- Youth Justice Services Identity-Based Data Collection Initiative

Ministry of Community Safety and Correctional Services

- *Bill 175, Safer Ontario Act, 2018—Police Services Act, 2018*, *Missing Persons Act, 2018*, and amendments to the *Coroners Act*
- Bill 195, *Correctional Services Transformation Act, 2018*

In keeping with the IPC's commitment to outreach, engagement and collaboration, we actively participated in a number of consultations in 2017.

CONSULTATIONS

Ministry of Energy

- Green Button Implementation and Regulatory Proposal

Ministry of the Environment and Climate Change

- Drive Clean Program – Remote Emissions Testing

Ministry of Finance

- Statistics Transformation
- Bill 174, *Ontario Cannabis Retail Corporation Act, 2017*

Ministry of Government and Consumer Services

- Guide for Interaction with the Office of the Information and Privacy Commissioner of Ontario
- Bill 59, *Putting Consumers First Act (Consumer Protection Statute Law Amendment)*, 2017—Door-to-Door Solicitation Restrictions and Compliance Requirements

Ministry of Municipal Affairs

- Bill 68, *Modernizing Ontario's Municipal Legislation Act, 2017*

Ministry of Transportation

- Highway 407 East Project

Municipality of Middlesex Centre

- Video Surveillance Policies and Procedures

Niagara Regional Police Service

- Crime Mapping Tool

Region of Peel

- Video surveillance systems at municipal facilities

Town of Parry Sound

- Water/Wastewater Warranty Protection Plan

University of Toronto and Toronto District School Board

- Data sharing agreement for research project on student achievement

Various School Boards in the Province

- School bus camera surveillance systems

Our office urges the government to complete this work in a timely manner so that the privacy rights of Ontarians are protected and they are given the tools to exercise their legal rights.

Amendments to the *Personal Health Information Protection Act* (*PHIPA*)

HEALTH

THIS YEAR SAW A NUMBER OF AMENDMENTS TO ONTARIO'S HEALTH PRIVACY LAW. These changes allow for increased protection of patient privacy and improved accountability and transparency in our health care system. These amendments also help to ensure that personal health information (PHI) remains secure and confidential.

On October 1, 2017, it became mandatory for health information custodians (HICs) to report certain privacy breaches to our office. This new reporting requirement enhances the IPC's ability to address key concerns and gives health care providers the opportunity to benefit from our advice and assistance in responding to a breach. To help them meet this new requirement, we published the guidance document, *Reporting a Privacy Breach to the Commissioner*. This document explains the reporting criteria and summarizes circumstances under which a custodian should notify our office of a privacy breach.

Since mandatory reporting came into effect, we have seen a dramatic increase in the number of reported breaches. From 2016 to 2017, the number of reported breaches more than doubled in the months October to December, from 58 to 125. The number of cases involving snooping into medical records remained steady at 24 per cent for both years. The number of cases involving general unauthorized collection, use, and disclosure and stolen PHI grew from 15 per cent to 18 per cent. Misdirected or lost PHI, which has always been the majority of reported breaches, also grew from 28 per cent to 37 per cent.

This year we also issued *Annual Reporting of Privacy Breach Statistics to the Commissioner* to help custodians prepare for reporting their privacy breach statistics to our office. HICs began to track their privacy breach statistics as of January 1, 2018, and starting in March 2019, they will be required to provide an annual report on the number of privacy breaches that occurred during the previous calendar year. These statistics will be collected through our statistics submission website, which will launch in early 2019.

In our last annual report, we urged the government to move forward with the proclamation of amendments to *PHIPA* relating to the shared provincial electronic health record (EHR). As Ontario's health sector transitions from paper and stand-alone electronic medical records to a shared provincial EHR, these amendments will provide an effective governance framework to protect the privacy of individuals. Among other things, these amendments would provide individuals with the ability to withhold and withdraw their consent to the collection, use and disclosure of their PHI from the provincial EHR system for health care purposes. The government committed to implementing the regulations necessary to provide individuals with a broad range of options to exercise this right back in 2012. Our office urges the government to complete this work in a timely manner so that the privacy rights of Ontarians are protected and they are given the tools to exercise their legal rights.

New Code of Procedure for Matters under *PHIPA*

A new *Code of Procedure for PHIPA* came into force in March, taking immediate effect on all IPC files under Ontario's health privacy legislation. This new code was borne out of an internal review of our *PHIPA* processes. The revised code now represents a single comprehensive protocol for all matters arising under *PHIPA* where the previous Code of Procedure only applied to access and correction complaints.

We also published five *PHIPA Practice Directions* that provide additional guidance to parties about exercising their rights and complying with their obligations under *PHIPA*.

Three-Year Reviews of Prescribed Health Entities and Persons

Under *PHIPA*, health information custodians can disclose PHI, without consent, to prescribed entities for the purpose of analysis or compiling statistical information needed to plan and manage the health care system. Similarly, they can disclose PHI, without consent,

SUMMARY OF PHIPA COMPLAINTS

-4%	-9%	+38%	+68%
ACCESS/CORRECTION OPENED	INDIVIDUAL OPENED	SELF-REPORTED BREACH OPENED	IPC INITIATED OPENED
2017 155	**2017 105**	**2017 322**	**2017 47**
2016 161	2016 115	2016 233	2016 28
+21%	-9%	+64%	+119%
ACCESS/CORRECTION CLOSED	INDIVIDUAL CLOSED	SELF-REPORTED BREACH CLOSED	IPC INITIATED CLOSED
2017 164	**2017 102**	**2017 305**	**2017 46**
2016 135	2016 112	2016 186	2016 21

to prescribed persons that compile or maintain registries of personal health information for the purposes of enabling or improving the provision of health care.

Every three years we review the information practices and procedures of these prescribed entities and persons.

In 2017, we reviewed:

Prescribed Entities

- Cancer Care Ontario
- Canadian Institute for Health Information
- Institute for Clinical Evaluative Sciences
- Pediatric Oncology Group of Ontario.

Prescribed Persons

- Cardiac Care Network of Ontario in respect of its registry of cardiac and vascular services
- INSCYTE Corporation in respect of CytoBase
- Cancer Care Ontario in respect of the Ontario Cancer Screening Registry
- Children's Hospital of Eastern Ontario in respect of the Better Outcomes Registry and Network
- Ontario Institute for Cancer Research in respect of the Ontario Tumour Bank
- Hamilton Health Sciences Corporation in respect of the Critical Care Information System.

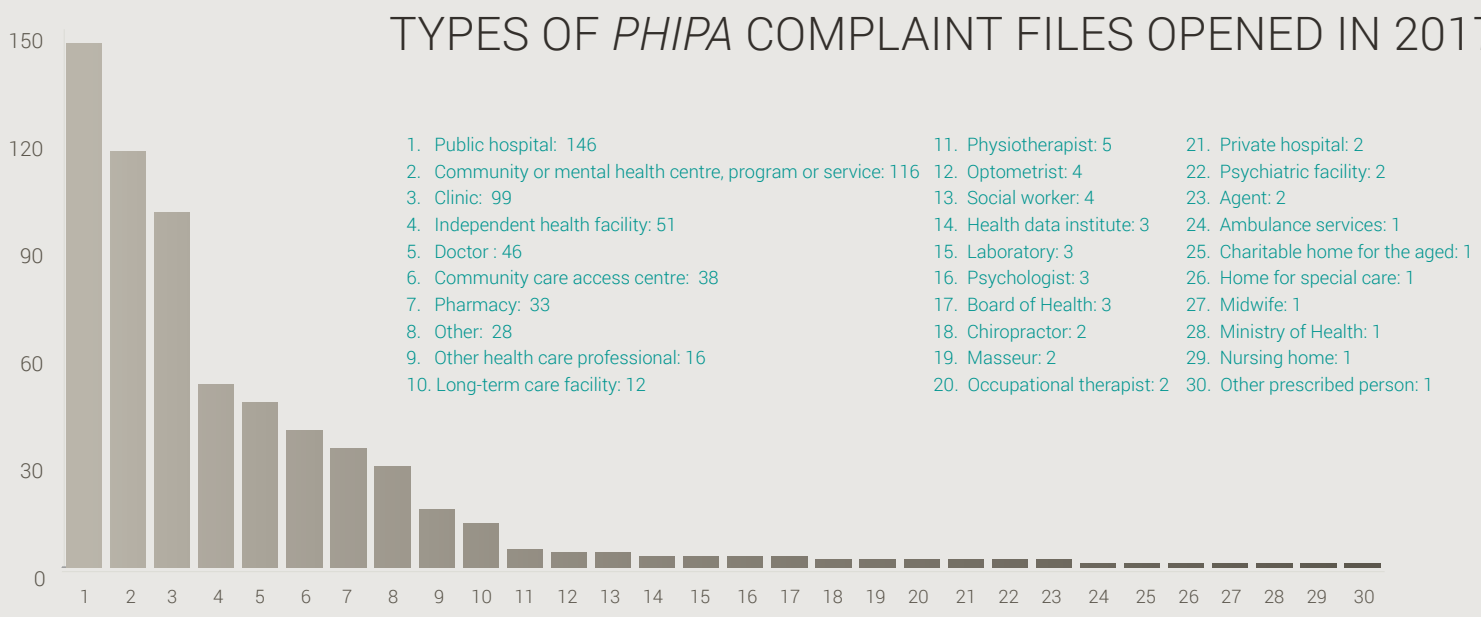
We found that all of the above prescribed entities and persons continue to meet the requirements of *PHIPA*. Reports, affidavits and approval letters for each of these reviews are publicly available.

Significant *PHIPA* Decisions

The following are some noteworthy *PHIPA* decisions published in 2017.

Decision 49

A doctor received an email from an individual containing an image of a computer screen in the doctor's



examination room that showed the personal health information of a number of patients. The doctor and the doctor's lawyer asked the individual to delete the image but he refused. The IPC conducted a review of the incident and found that the individual was in contravention of *PHIPA* by using the PHI of individuals without authorization. Decision 49 ordered the individual to securely dispose of the personal information of other individuals in the image and provide an affidavit confirming compliance to our office. The IPC filed this order with the Superior Court and is bringing a contempt motion to enforce it.

Decision 50

A medical clinic contacted the IPC with concerns about the management of personal health information by the service provider hosting their electronic medical records (EMR). The clinic found that the service provider had transferred hundreds of patient records to a physician who was leaving the clinic. The doctor claimed that those patient records belonged to him. After investigating, our office decided not to conduct a review under *PHIPA* given that both parties consented to a court order providing the physician with access to PHI in the EMR, and for the delivery of original patient records to him. The clinic has since amended its agreement with physicians, clarifying who has responsibility for patient records.

Decision 52

An individual sought access to all the electronic data about himself, in its native, industry-standard electronic format. The hospital did not provide the requested information and noted that some of the raw data was not available to the hospital itself. Our office found that the requester only has a right of access to underlying raw data that the hospital can extract through custom queries and that the hospital is entitled to reasonable cost recovery in providing access. Our office also found that, due to the significant staff time and resources that would be required to extract a certain type of data, it was not reasonably available to the hospital itself, and so was not subject to the right of access.

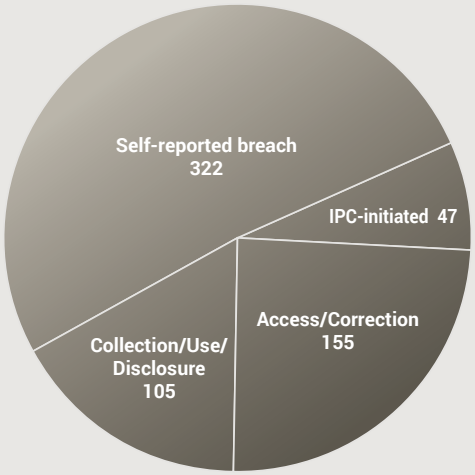
Decision 56

The Ministry of Health and Long-Term Care (MOHLTC) advised our office that OHIP numbers were compromised by criminal activity involving the filing of fraudulent claims with an insurance company. Upon investigation, we discovered that the insurance company was collecting and using OHIP numbers as part of its application process for purchasing supplementary health insurance plans. It was also collecting, using, and disclosing the numbers when emergency medical travel claims were filed. Our office decided that the collection and use of OHIP numbers at the time of application for supplementary health insurance plans contravened *PHIPA*. However, the practice of collecting, using, and disclosing OHIP numbers for the purpose of processing emergency medical travel claims was allowed. The insurance company discontinued its practice of collecting OHIP numbers on both paper and electronic applications and deleted any numbers it had collected from its administrative system.

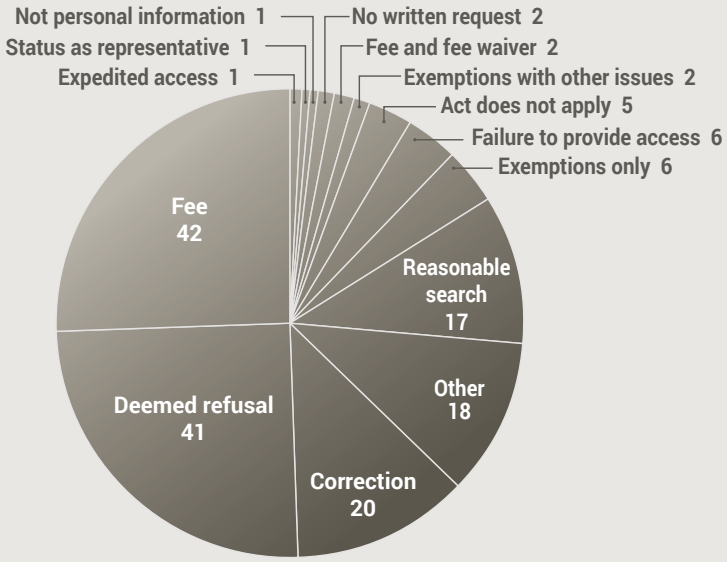
Decision 62

Two complaints alleged that a physician accessed records of PHI of two related individuals at a community health centre without authorization. In response, the centre implemented a number of measures to safeguard the privacy and security of information in its custody or control. The centre also entered into an agreement with a corporation, in which the physician is a shareholder, clarifying responsibility for PHI in the electronic medical records used by physicians practicing at the centre. While the centre did not comply with its obligations under *PHIPA* at the time of these events, the IPC did not issue an order because the centre had already made these changes. Further, while the physician's access to the individuals' PHI was unauthorized, there was no evi-

SUMMARY OF *PHIPA* COMPLAINTS OPENED



ACCESS/CORRECTION COMPLAINTS CLOSED BY ISSUE



dence to suggest that the physician disclosed the PHI in contravention of *PHIPA*.

PHIPA Cases Closed Through Early Resolution

Our office strives to resolve *PHIPA* cases at the intake stage, or through mediation, without the need for adjudication. Below are some of the cases closed through early resolution in 2017.

- A long-term care home, owned and operated by a municipality, reported that six of its employees used their personal cellphones to take and/or receive pictures of a number of residents and then circulate them to other employees via Snapchat. The city took a number of steps to contain the breach, notify the affected individuals and/or their substitute decision makers and prevent a future occurrence, including circulation of an all-staff memo and introduction of an e-learning module on *PHIPA* obligations. Five of the employees no longer work at the home and the home reported two staff members to their regulatory college. Our office was satisfied with the city's response to the breach.
- An individual alleged that a financial institution was requiring individuals to provide a copy of their OHIP card in order to obtain a credit card. This is contrary to *PHIPA*, which states, "*No person shall require the production of another person's health card, but a person who provides a provincially funded health resource to a person who has a health card may require the production of the health card.*" The financial institution acknowledged it is not permitted to require OHIP cards as a form of identification, and deleted information it collected from these cards.
- We received a complaint against a hospital stating that its lobby did not provide a private area for triage, allowing other patients to overhear discussions about their personal health information. In response to the complaint, the hospital introduced partitioned stations to allow for private conversations between patients and hospital staff.

Hospital staff also underwent additional privacy awareness training focused on protecting privacy and confidentiality when conversing with patients.

- A hospital reported that records of PHI were found scattered near a recycling bin on its premises. It was determined that five patients' records were disposed of in an unsecure manner by a staff trainee. The hospital successfully notified the affected patients, retrained the trainee regarding its privacy policy, used the incident as an example to remind residents and staff of proper disposal methods for PHI, and ensured that the records found near the recycling container were properly destroyed.
- We received a report from a hospital that six employees took photos using personal cell phones of a patient's x-ray image. Some of these employees either showed or transmitted the image to other staff members and persons outside of the hospital. Additionally, unknown persons accessed the image, using a physician's login credentials, after the physician failed to log out of the electronic system. The hospital took steps to identify the employees and external persons who were, or may have been, involved and obtained sworn declarations that the image was deleted from their phones. The hospital also took disciplinary action ranging from verbal reprimands up to one-month unpaid suspensions. Following a review of its policies, the hospital committed to additional training programs and implementing a privacy warning for all its computer systems.

Prosecutions under *PHIPA*

- A Master of Social Work student was ordered to pay a $20,000 fine and a $5,000 victim surcharge for willfully accessing the PHI of five individuals. She was the fourth person ever convicted of an offence under *PHIPA*. As part of her guilty plea, she admitted to accessing the PHI of 139 individuals without authorization. This is the highest fine to date for a health privacy breach in Canada. In delivering her sentence, the Justice of the Peace stated, *"Overall, the victim impact statements reveal a lack of trust and a sense of reluctance to share information with future health care providers. I believe this is a truly significant factor, given that we all must believe that when we go to the doctor for our physical illnesses and our mental health illnesses, that we will be able to trust our own health care practitioners and their team and that what we tell them will be respected and held in confidence so we receive the treatment and care we deserve."*
- An administrative support clerk in the emergency department of a GTA hospital

accessed the health records of 44 individuals without authorization, printing out the PHI of 28 of these individuals. The Justice of the Peace noted that this was a serious breach of public trust in the health care system. The clerk pled guilty and was ordered to pay an $8,000 fine and a $2,000 victim surcharge.

Bill 84, *Medical Assistance in Dying Statute Law Amendment Act*

This year, our office voiced objections to amendments to *FIPPA* and *MFIPPA* contained in Bill 84, the *Medical Assistance in Dying Statute Law Amendment Act*. These amendments exclude information related to medical assistance in dying from access laws, if the information relates to identifiable individuals and facilities. This means that individuals do not have a right to information that identifies hospitals, pharmacies, long-term care homes or hospices that provide this service. Our office objected to the exclusion as it applies to facilities, because there is no evidence of harm in other jurisdictions where medical assistance in dying is legal and provider information is available. In our view, if a specific request for information posed a risk of harm, existing exemptions under *FIPPA* and *MFIPPA* would prevent the release of information that created such a risk. In addition, excluding this information may limit access to medical assistance in dying, and potentially prevent the release of statistical information important to public debate and analysis. The bill ultimately became law in June 2017 despite the IPC's concerns. In response, our office called on health institutions in Ontario to set their own standards of transparency, and voluntarily disclose whether they provide these services to patients.

Bill 160, *Strengthening Quality and Accountability for Patients Act*

In his submission on this bill, the Commissioner expressed concern that the proposed changes governing health care services do not include provisions that the IPC considers necessary to protect the privacy of Ontarians. Of particular concern was the exclusion of the Patient Ombudsman's investigative records from *FIPPA*, which will have significant consequences.

Because of this exclusion, patients will not be able to access their own records of personal information held by the Patient Ombudsman in an investigation. Moreover, existing privacy protections will no longer apply to Ombudsman investigations and individuals will not be able to access information used by the Ombudsman to form important recommendations.

In addition to recommending removal of this exclusion, the Commissioner made 11 other recommendations, including restrictions on the collection, use, and disclosure of PHI, confidentiality requirements, and protection of PHI in documents relating to the prosecution of offences.

30 YEARS OF ACCESS AND PRIVACY SERVICE

The *Freedom of Information and Protection of Privacy Act* (*FIPPA*) passes third reading on June 25, 1987, and receives royal assent a few days later on June 29, 1987.

The first Information and Privacy Commissioner of Ontario is Justice Sidney B. Linden.

1988

The *Freedom of Information and Protection of Privacy Act* (*FIPPA*) comes into force.

1991

The *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) comes into force.

Tom Wright succeeds Justice Sidney B. Linden as Information and Privacy Commissioner of Ontario.

1994

The IPC calls on the government to extend *FIPPA* and *MFIPPA* to a wider set of public organizations such as hospitals, universities, and social services agencies to make them more accountable to the public.

1995

Publication of *Privacy-Enhancing Technologies: The Path to Anonymity*. This groundbreaking paper looks at how technology can be used to protect privacy.

1996

The IPC website is launched.

Order P-1190 — Assistant Commissioner Tom Mitchinson finds there is a compelling public interest in the disclosure of records concerning nuclear safety.

1997

Dr. Ann Cavoukian succeeds Tom Wright as Information and Privacy Commissioner.

Order P-1398 – The IPC determines that there is a compelling public interest in disclosure of Ministry of Finance records relating to the impact of Quebec independence on Ontario-Quebec relations.

1998

The IPC is successful in having access and privacy added to the Ontario Civics curriculum and placed in the "Specific Expectations" of what students will learn by the end of the course.

1999

The Reaching Out to Ontario (ROTO) event series is launched, and a small IPC team visits London, St. Thomas and Chatham to meet with stakeholders to discuss access and privacy issues.

The IPC develops teachers' guides on access and privacy for grades five and ten and launches its "Ask an Expert" program, in which IPC speakers visit Grade 5 classes.

2000

The Commissioner tables a special report: *Province of Ontario Savings Office—A Special Report to the Legislative Assembly of Ontario* on the Disclosure of Personal Information, based on an IPC investigation into a privacy breach involving account holders of the Province of Ontario Savings Office.

2004

The *Personal Health Information Protection Act* (*PHIPA*) comes into force.

2005

The first *PHIPA* Order is issued on October 31, 2005: HO-001

MO-1947 – The Commissioner orders disclosure of information about lawsuits filed against the City of Toronto, including the number of claims and the total amounts paid to settle claims.

2006

Ontario universities become subject to the *Freedom of Information and Protection of Privacy Act* (*FIPPA*).

The Divisional Court affirms that the Commissioner has the authority to investigate and report on privacy complaints made by the public about government institutions.

The IPC celebrates the first "Right to Know Week," featuring a public panel discussion on access issues.

2007

For the first time in its 20-year history, the IPC invokes the power to order an institution to cease the collection of personal information.

In MO-2225, the IPC directs the City of Ottawa and the Ottawa Police to stop collecting extensive personal information from individuals selling used goods to second-hand stores and to destroy personal information already collected.

2008

The IPC releases *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report*, which finds that the Toronto Transit Commission's use of video surveillance complies with Ontario privacy law. The IPC makes a number of specific recommendations on how the TTC can enhance privacy.

2009

Following an extensive investigation, the Commissioner orders Crown attorneys to cease collecting any personal information of potential jurors beyond what is necessary under the *Juries Act* and *Criminal Code* and proposes a fundamental shift in the way prospective jurors are screened. Order PO-2826

2010 | The IPC launches the *Stop.Think. Protect.* campaign, calling on leaders in Ontario's health sector to help combat the increase of avoidable breaches of personal health information.

2011

The IPC publishes guidance for hospitals to prepare them for becoming institutions under *FIPPA:*

Applying PHIPA and FIPPA to Personal Health Information: Guidance for Hospitals

Freedom of Information at Ontario Hospitals: Frequently Asked Questions

2012

As of January 1, hospitals are subject to the *Freedom of Information and Protection of Privacy Act*. Ontario is the last province to bring hospitals under access legislation.

The IPC publishes *A Policy is Not Enough: It Must be Reflected in Concrete Practices*, demonstrating how to develop an appropriate privacy policy and embed it in the practices of an organization.

2013

The IPC releases a Special Report: *Deleting Accountability: Records Management Practices of Political Staff*, which details the findings of

30 YEARS OF ACCESS AND PRIVACY SERVICE

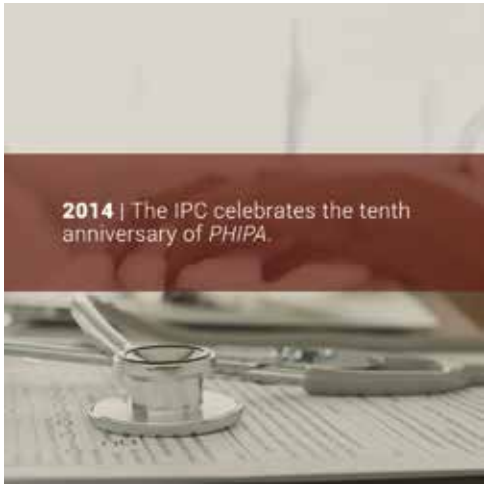
the IPC's investigation into the improper deletion of emails concerning the cancellation of gas plants by the Chief of Staff to the former Minister of Energy.

2014

Brian Beamish is appointed acting Information and Privacy Commissioner of Ontario.

The Supreme Court of Canada upholds IPC Order PO-2811, in which the IPC orders disclosure of statistical information relating to the sex offender registry to a media requester.

Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CPIC is released. The report calls on police to restrict the disclosure of suicide-related information to U.S. agencies via the Canadian Police Information Centre (CPIC) database.



In Order HO-013, Acting Commissioner Beamish finds that Rouge Valley Health System violated *PHIPA* when two employees accessed and sold new mothers' personal health information for financial gain. The Commissioner orders the hospital to implement changes to its electronic information systems, revise its privacy and audit policies and deliver privacy training to all staff.

2015

Appointment of Brian Beamish to five-year term as Information and Privacy Commissioner of Ontario.

Introduction of Bill 119 to amend the *Personal Health Information Protection Act* (*PHIPA*).

The IPC celebrates International Data Privacy Day with an event to commemorate the tenth anniversary of *PHIPA*.

The IPC launches the *Is It Worth It?* campaign, warning health information custodians of the dangers and risks of unauthorized access to information, or 'snooping'.

As part of its Reaching Out to Ontario (ROTO) program, the Commissioner and his team visit St. Catharines, Ottawa and Sault Ste. Marie to discuss current and emerging access to information and privacy issues.

After extensive consultation with the IPC, Ontario's Minister of Community Safety and Correctional Services (MCSCS) introduces the *Police Record Checks Reform Act* in the Legislature, establishing a new provincial standard that clarifies, limits and controls the scope of police record check disclosures to employers, volunteer agencies, and other third parties.

2016

To promote awareness of the importance of sharing information with a children's aid society when there are reasons to believe a child may be at risk, the IPC publishes the guide *Yes, You Can* together with the Office of the Provincial Advocate for Children and Youth.

Order MO-3281 finds that an email sent by a City of Oshawa councillor from the councillor's personal email account is in the custody and control of the city, because it was created in the course of city business. As a result, the IPC orders the city to issue an access decision.

The IPC publishes *Instant Messaging and Personal Email Accounts: Meeting Your Access and Privacy Obligations*, to make public servants aware that records relating to the conduct of government

business are subject to provincial access legislation, even if they are created, sent, or received through instant messaging tools or personal email accounts.

Bill 119, the *Health Information Protection Act*, 2016, amends the *Personal Health Information Protection Act* (*PHIPA*) to better protect patient privacy and improve accountability and transparency across Ontario's health sector.

In PO-3617 (June 2016), the IPC orders the Ministry of Health and Long-Term Care to release the names of OHIP's top billers to the Toronto Star. The ministry had previously disclosed payment amounts and the specialties of some physicians in response to the Star's request, but withheld the names of the physicians as an invasion of their personal privacy. The IPC decides that the information is of a business or professional nature, and not personal, and orders the ministry to disclose the information. In June 2017, Ontario's Divisional Court dismissed an application to quash the order, ruling that it was reasonable. The court agreed that the names of the doctors, in conjunction with the amounts they receive in OHIP payments and their medical specialties, is not "personal information." The Ontario Court of Appeal will hear an appeal from this decision in June 2018.

The IPC publishes *Open Government: Key Concepts and Benefits* and *Open Government: Key Implementation Considerations* for institutions considering Open Government programs. The papers highlight the importance of enhancing access to government-held information, and provides advice on implementation.

The IPC launches a series of webinars on access and privacy, with the first devoted to the topic of situation tables.

2017

In January, the IPC holds its annual Privacy Day event. The theme is Government and Big Data and features privacy and big data experts offering solutions to privacy risks that governments face in an increasingly big data world.

The IPC makes presentations to legislative committees on three bills:

Bill 68, Modernizing Ontario's Municipal Legislation Act, 2017

Bill 84, the Medical Assistance in Dying Statute Law Amendment Act, 2017

Bill 89, the Supporting Children, Youth and Families Act

De-identification Guidelines for Structured Data wins the inaugural International Conference of Data Protection and Privacy Commissioners' award for excellence in research.

Amendments to *PHIPA* came into force, requiring health information custodians under *PHIPA* to report certain health privacy breaches to the IPC.

January

Big Data and Your Privacy Rights

The information presented in this fact sheet helps members of the public understand the meaning of "big data," and how it can have an impact on an individual's privacy.

March

Open Government and Protecting Privacy

The purpose of this paper is to help institutions understand that privacy is not a barrier to Open Government, and that proactively addressing privacy risks is critical to its success.

April

Reasonable Search

This fact sheet explains the meaning of "reasonable search," how institutions can comply with their search obligations, how requesters can support institutions' efforts to find responsive records, and the role of the IPC in an appeal.

May

Big Data Guidelines

These guidelines inform government institutions of the key issues to consider and best practices to follow when conducting big data projects involving personal information.

July

Guidance on the Use of Automated Licence Plate Recognition Systems (ALPR) by Police Services

This document outlines the key obligations of police services under *MFIPPA* and *FIPPA* in their use of ALPR systems and provides guidance, including best practices, on using these systems in a privacy-protective manner.

August

Frivolous and Vexatious Requests

This fact sheet explains the meaning of a "frivolous or vexatious request." It describes what institutions should do when they receive this type of request, what a requester can do if an institution claims their request is frivolous or vexatious and the IPC's role in an appeal.

Reporting a Privacy Breach to the Commissioner: Guidelines for the Health Sector

These guidelines summarize the seven categories described in the *PHIPA* regulation where custodians are required to report breaches to the Commissioner.

IPC 2017 GPEN Sweep Report: Online Educational Services

This year's GPEN (Global Privacy Enforcement Network) Sweep theme was "user control over personal information." The IPC worked with the Office of the Privacy Commissioner of Canada to design and carry out a review of online educational services. This sweep report summarizes the findings of our review.

GUIDANCE AND FACT SHEETS

November

Joint Federal Provincial Territorial Letter to Council of Ministers of Education on the Importance of Privacy Education

The goal of the joint letter to the Council of Ministers of Education was to encourage them to make privacy education a greater priority by including it as a clear and concrete component in digital literacy curricula across the country.

Annual Reporting of Privacy Breach Statistics to the Commissioner—Requirements for the Health Sector

This document outlines the information the IPC will require from health information custodians in their annual reporting of breach statistics as of March 2019.

Updated Publications

Code of Procedure for Matters under the Personal Health Information Protection Act, 2004

This code applies to complaints, IPC-initiated files, and custodian-reported files under the *Personal Health Information Protection Act*.

PHIPA Practice Direction #1: Clarifying Access Requests

PHIPA Practice Direction #2: Responding to a Request for Access to Personal Health Information

PHIPA Practice Direction #3: Publicly Released Decisions under the Personal Health Information Protection Act, 2004

PHIPA Practice Direction #4: Access/Correction Complaint Form

PHIPA Practice Direction #5: Collection, Use, and Disclosure Complaint Form

2017 IPC Submissions and Comments on Legislation

March

Submission to the Standing Committee on Bill 84, Medical Assistance in Dying Statute Law Amendment Act, 2017

Submission to the Standing Committee on Bill 89, Supporting Children, Youth and Families Act, 2017

April

Comments of the Information and Privacy Commissioner of Ontario on the Proposed Open Meeting Amendments in Bill 68, Modernizing Ontario's Municipal Legislation Act, 2017

November

Comments of the Information and Privacy Commissioner of Ontario on Bill 160, Strengthening Quality and Accountability for Patients Act, 2017

Updating our access and privacy laws is long overdue and necessary if they are to remain relevant and in line with the information age.

COMMISSIONER'S RECOMMENDATIONS

Expand Commissioner's Oversight to Political Parties

POLITICAL PARTIES HOLD A LOT OF POWER IN OUR SYSTEM OF GOVERNMENT; THEY ALSO HOLD A LOT OF SENSITIVE PERSONAL INFORMATION ABOUT INDIVIDUALS. And yet, our political parties are not covered by privacy laws at either the provincial or federal level.

Recent events have illuminated the sensitive and granular nature of the personal information available to political parties for their own purposes. We know that digital tools are now available to amass large amounts of personal information from diverse sources, analyze it in ways previously unforeseen and use insights gained to target individuals in specific and unique ways.

These increasingly sophisticated big data practises, frequently undertaken without voters' knowledge or consent, raise new privacy and ethical concerns. Especially given that such practices aim to influence the outcome of democratic elections, the need for greater transparency is clear.

Personal information held by political parties can also be vulnerable to privacy breaches. This includes unintentional breaches—for example, human error can lead to personal information being disclosed inappropriately. It also includes cybersecurity threats, which may increase with the growing use of big data practises by political parties. Because political parties operate outside of privacy laws, there is little recourse for those impacted by a privacy breach.

To address the privacy, ethical and security risks associated with how political parties are collecting and using our personal information, I recommend that Ontario's political parties be subject to privacy regulation and oversight.

Enact Legislation that Provides a Strong, Government-Wide Big Data Framework

I have long argued that advancements in technology and the ever-expanding use of personal information are outpacing Ontario's public-sector access and privacy laws. These laws were drafted 30 years ago and are poised for a legislative fix to bring them in line with modern technology and information-sharing practices. My call to review and renew the acts stands—we must modernize them if we are to continue to protect and promote the access and privacy rights of the people we serve.

Public institutions increasingly use big data to shape and improve government policies, programs and services, and gain new insights about issues affecting the public they serve. However, the current legislative regime effectively requires institutions to act as "silos" of personal information.

In light of these legislative shortcomings, Ontario needs a new or modified framework, one that supports sophisticated big data projects, streamlines and allows for greater data integration while protecting personal privacy. To this end, I once again call on the Ontario government to update our access and privacy laws to include a consistent, privacy-protective framework for big data and data integration. Such a framework should support a centralized, rather than decentralized, model of data integration. This will help to avoid the replication of multiple government databases that contain sensitive, linked personal information. A government-wide big data framework must contain additional controls to protect privacy, including requirements for de-identification, mandatory breach notification and reporting, and effective and independent oversight, with strong investigative, audit, and review powers for the IPC.

Any future government framework that enables big data projects must adopt this modern approach to privacy protection.

Ensure Smart City Initiatives are Privacy Protective

Across Ontario, there is growing interest in "smart city" initiatives, as evidenced by large-scale announcements such as Toronto's Quayside Project involving Alphabet's Sidewalk Labs and Waterfront Toronto, and the Canada-wide Smart Cities Challenge.

Many of these initiatives rely on the use of data and connected technologies to identify and address the needs of communities. While I acknowledge that smart cities have the potential to improve many aspects of our lives, communities must recognize the corresponding privacy concerns. Smart city projects can involve the collection and linking of large amounts of data that can generate highly personal information, and enable privacy invasive profiling or surveillance. These and other risks must be addressed head on and project leaders must understand their legal obligations under Ontario's privacy laws.

I recommend that communities carry out thorough privacy impact assessments (PIA) to identify and address the privacy risks before they launch smart city programs. Transparency and community engagement will also be critical to help community members understand how the proposed technology might affect them. Conducting a PIA and engaging the community early on will build public accountability and trust. My office will remain engaged in this area and is ready to provide guidance and support to ensure that smart city initiatives comply with Ontario's privacy laws.

Amend Ontario's Access Laws to Affirm IPC's Power to Compel the Production of Records

My office's ability to determine whether an institution has prop-

erly claimed exemptions in the context of an access to information appeal is often dependent on our ability to examine the records at issue, including records over which solicitor-client privilege has been claimed.

In 2016, the Supreme Court of Canada considered whether the wording of the *Alberta Freedom of Information and Protection of Privacy Act* was clear enough to empower the Alberta Information and Privacy Commissioner to compel production of records claimed to be subject to solicitor-client privilege. The court found that the wording of Alberta's legislation was not sufficiently clear. In light of this decision, some institutions have questioned the IPC's authority to compel the production of records over which solicitor-client privilege is claimed.

The federal government has introduced amendments to the *Access to Information Act* and the *Privacy Act* that would clarify the powers of the federal Information Commissioner and the federal privacy commissioner to examine records subject to a claim of solicitor-client privilege.

Once again, I am calling on the Ontario government to follow the federal government's lead and amend *FIPPA* and *MFIPPA* to clarify and affirm the IPC's power to compel records, including those subject to a claim of solicitor-client privilege, and that providing records to the IPC does not constitute a waiver of this privilege.

An Ontario-Based Philadelphia Model

Early in 2017 media reports indicated that, on average, Canadian police services dismissed one out of every five sex-assault allegations on the basis that they were "unfounded" (i.e. that no crime occurred or was attempted). "Unfounded" rates varied widely, including in Ontario. These reports prompted renewed calls for more effective and accountable sexual assault and domestic violence investigations. Advocates in Ontario working to end violence against women pointed to a US model—the Philadelphia Model—as a key part of the solution. Under that model, police and agencies with expertise in combatting violence against women regularly review closed sexual assault files to identify investigative shortcomings associated with, for example, misinformation about complainants. After the City of Philadelphia adopted the model in 2000, the "unfounded" rate dropped to 4 per cent compared to the US national average of 7 per cent.

In 2017, my office engaged with the Kingston and Ottawa police, the Ottawa Rape Crisis Centre, and other policing and violence against women stakeholders on how to implement the US-based Philadelphia Model. Under this model, police and women's advocates regularly review closed sexual assault files to identify any investigative shortcomings that may be the result of biases or stereotypes. The result of our work was the development of a model Memorandum of Understanding (MOU) and confidentiality agreement, designed to set the terms for the review of sexual assault cases by police and external reviewers. I strongly encourage police services across the province who adopt the use of the Philadelphia Model to ensure a privacy-protective framework is in place by using the MOU and confidentiality agreement developed through these consultations.

My office will continue to advocate for the adoption of these recommendations on an active and ongoing basis. Updating our access and privacy laws is long overdue and necessary if they are to remain relevant and in line with the information age. The IPC is ready to work with institutions and assist wherever we can—together, we can help to ensure that Ontarians' access and privacy rights are strongly protected well into the future.

STATISTICS

YEAR AT A GLANCE

PROVINCIAL

PERSONAL INFORMATION	GENERAL RECORDS	TOTAL
-12% REQUESTS **2017 7,220** 2016 8,294	+8% REQUESTS **2017 16,605** 2016 15,319	+1% TOTAL REQUESTS **2017 23,825** 2016 23,613
-15% APPEALS OPENED **2017 154** 2016 181	-19% APPEALS OPENED **2017 450** 2016 555	-18% TOTAL APPEALS OPENED **2017 604** 2016 736
+14% APPEALS CLOSED **2017 196** 2016 172	-3% APPEALS CLOSED **2017 489** 2016 505	+1% TOTAL APPEALS CLOSED **2017 685** 2016 677
-71% AVERAGE COST **2017 $ 4.02** 2016 $13.86	-34% AVERAGE COST **2017 $25.53** 2016 $38.60	

MUNICIPAL

PERSONAL INFORMATION	GENERAL RECORDS	TOTAL
-2% REQUESTS **2017 18,301** 2016 18,743	-8% REQUESTS **2017 17,681** 2016 19,231	-5% TOTAL REQUESTS **2017 35,982** 2016 37,974
-7% APPEALS OPENED **2017 194** 2016 209	-1% APPEALS OPENED **2017 594** 2016 603	-3% TOTAL APPEALS OPENED **2017 788** 2016 812
-1% APPEALS CLOSED **2017 195** 2016 193	+1% APPEALS CLOSED **2017 534** 2016 530	+1% TOTAL APPEALS CLOSED **2017 729** 2016 723
-8% AVERAGE COST **2017 $ 9.92** 2016 $10.75	-1% AVERAGE COST **2017 $24.50** 2016 $24.66	

SUMMARY OF *PHIPA* COMPLAINTS

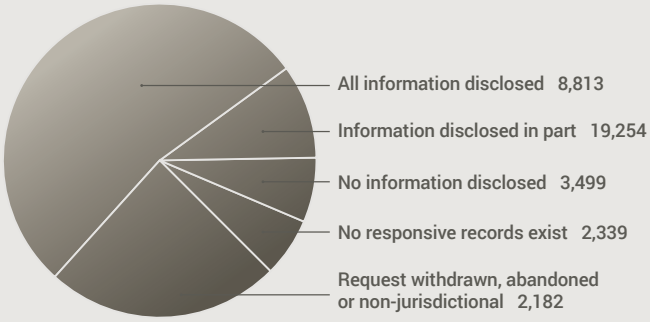
-4% ACCESS/CORRECTION OPENED **2017 155** 2016 161	-9% INDIVIDUAL OPENED **2017 105** 2016 115	+38% SELF-REPORTED BREACH OPENED **2017 322** 2016 233	+68% IPC INITIATED OPENED **2017 47** 2016 28
+21% ACCESS/CORRECTION CLOSED **2017 164** 2016 135	-9% INDIVIDUAL CLOSED **2017 102** 2016 112	+64% SELF-REPORTED BREACH CLOSED **2017 305** 2016 186	+119% IPC INITIATED CLOSED **2017 46** 2016 21

PRIVACY COMPLAINTS

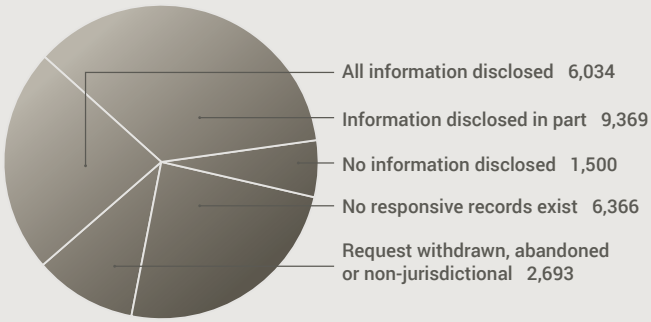
PROVINCIAL	MUNICIPAL
-7% OPENED **2017 110** 2016 118	-1% OPENED **2017 158** 2016 159
+10% CLOSED **2017 114** 2016 103	+4% CLOSED **2017 159** 2016 153

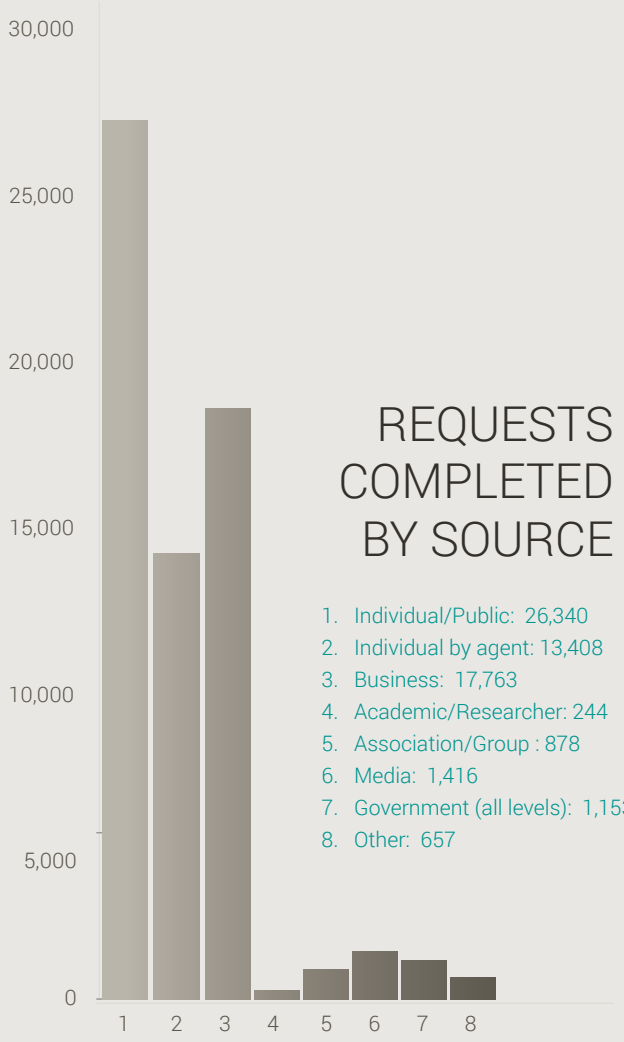
OVERALL REQUESTS

OUTCOME OF REQUESTS: MUNICIPAL



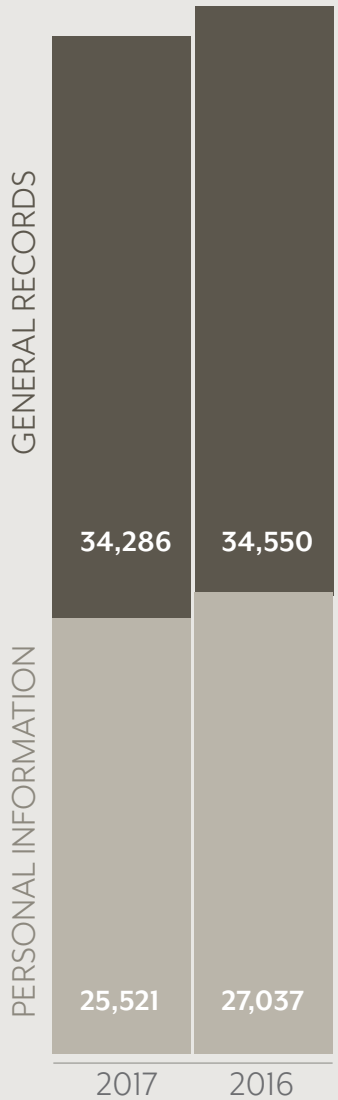
OUTCOME OF REQUESTS: PROVINCIAL





REQUESTS COMPLETED BY SOURCE

1. Individual/Public: 26,340
2. Individual by agent: 13,408
3. Business: 17,763
4. Academic/Researcher: 244
5. Association/Group : 878
6. Media: 1,416
7. Government (all levels): 1,153
8. Other: 657



TOTAL

-2.8%

REQUESTS
2017 59,807
2016 61,587

GENERAL RECORDS

-0.7%

REQUESTS
2017 34,286
2016 34,550

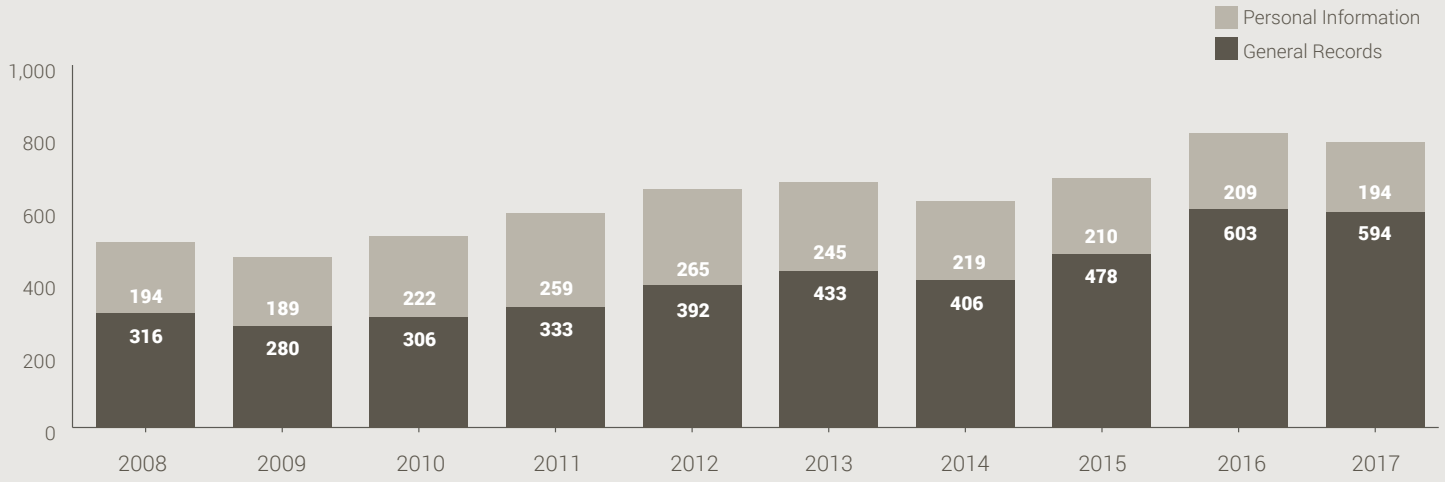
PERSONAL INFORMATION

-5%

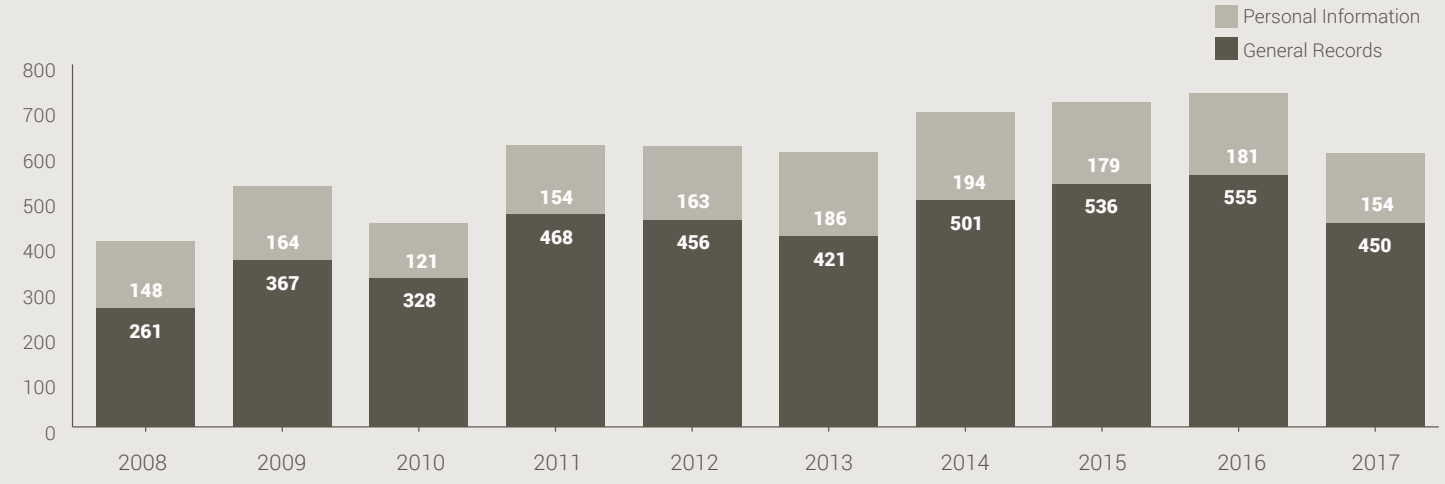
REQUESTS
2017 25,521
2016 27,037

STATISTICS

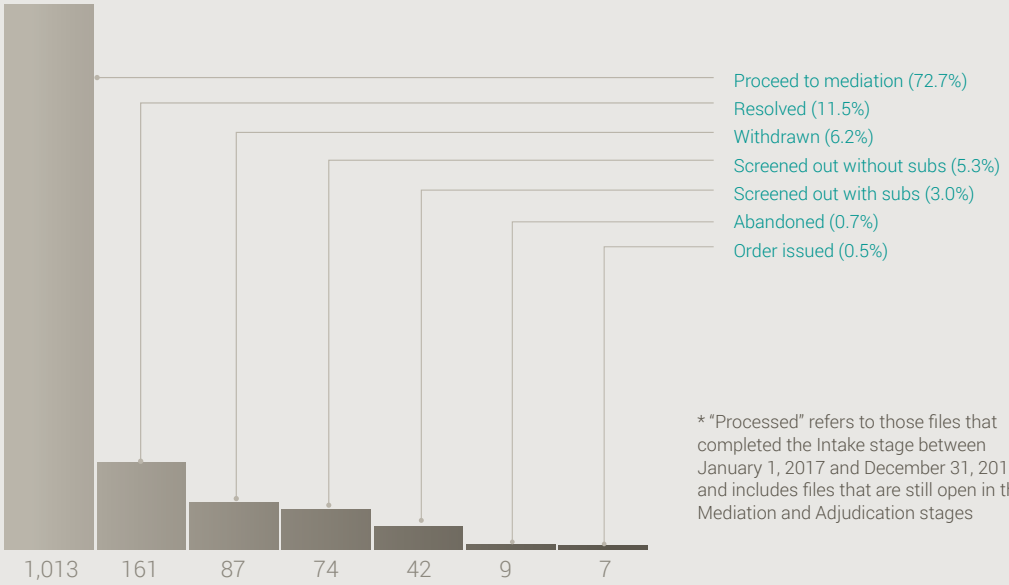
NUMBER OF MUNICIPAL APPEALS OPENED 2008-2017



NUMBER OF PROVINCIAL APPEALS OPENED 2008-2017

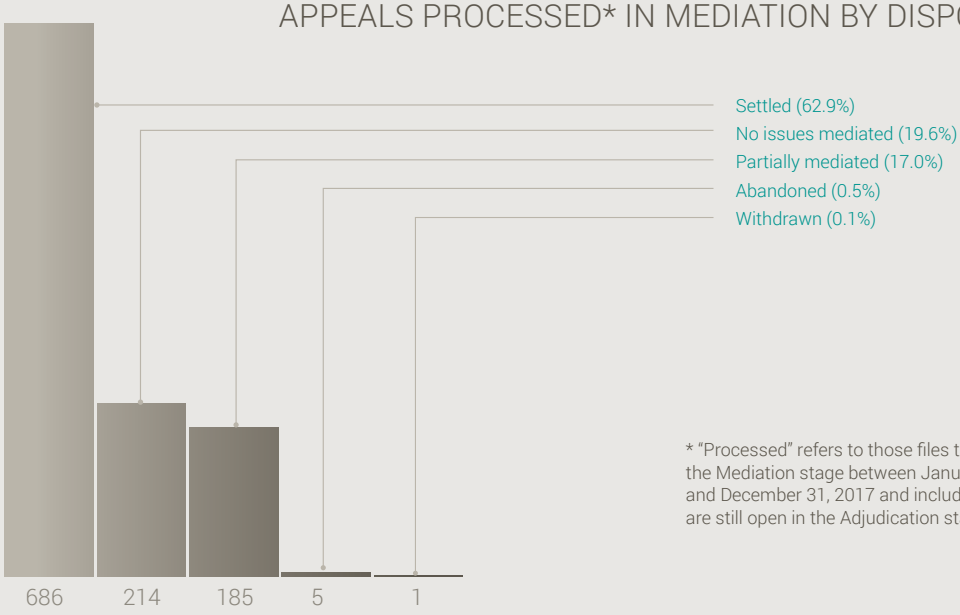


APPEALS PROCESSED* IN INTAKE BY DISPOSITION



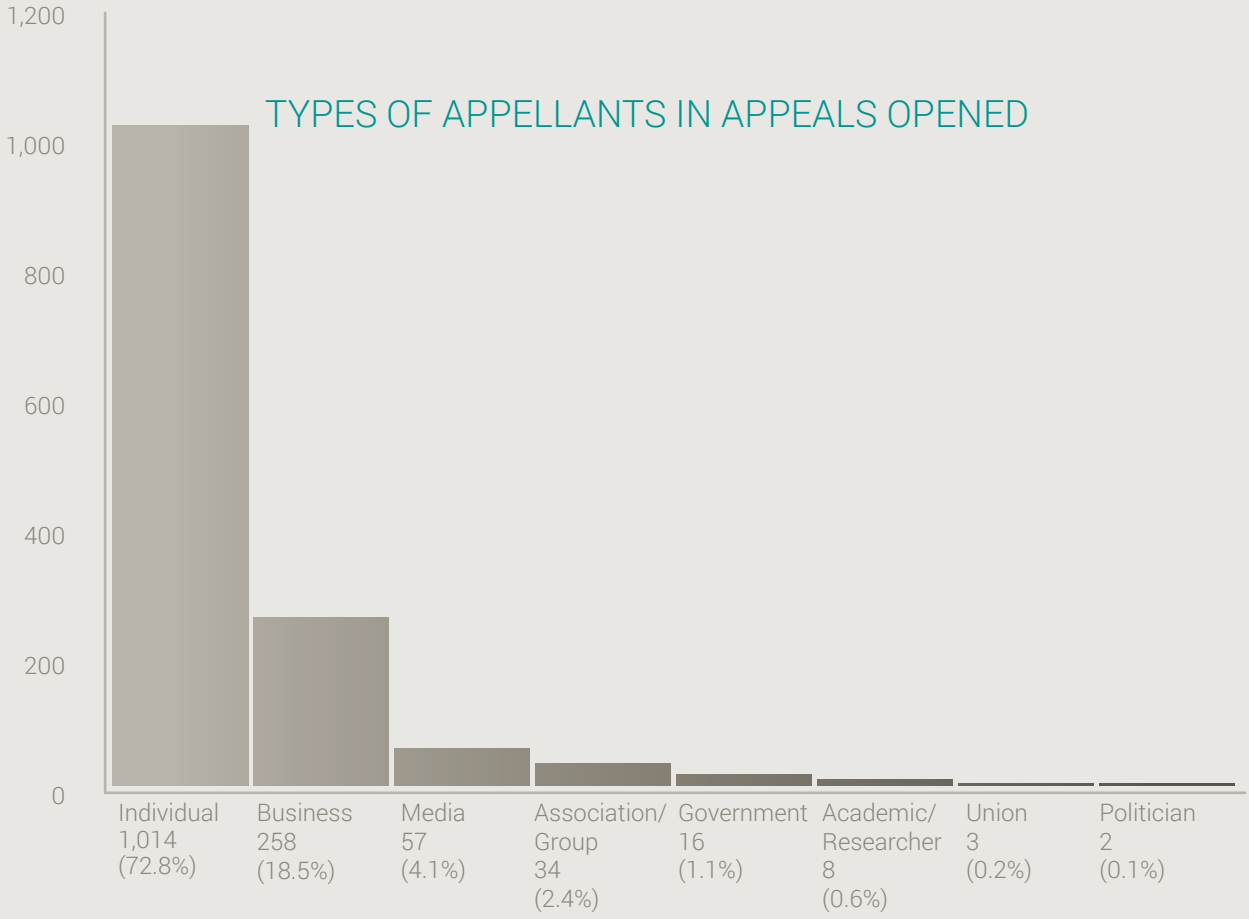
* "Processed" refers to those files that completed the Intake stage between January 1, 2017 and December 31, 2017 and includes files that are still open in the Mediation and Adjudication stages

APPEALS PROCESSED* IN MEDIATION BY DISPOSITION

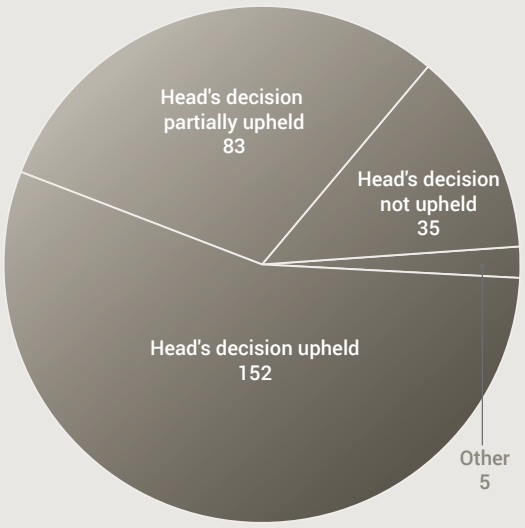


* "Processed" refers to those files that completed the Mediation stage between January 1, 2017 and December 31, 2017 and includes files that are still open in the Adjudication stage

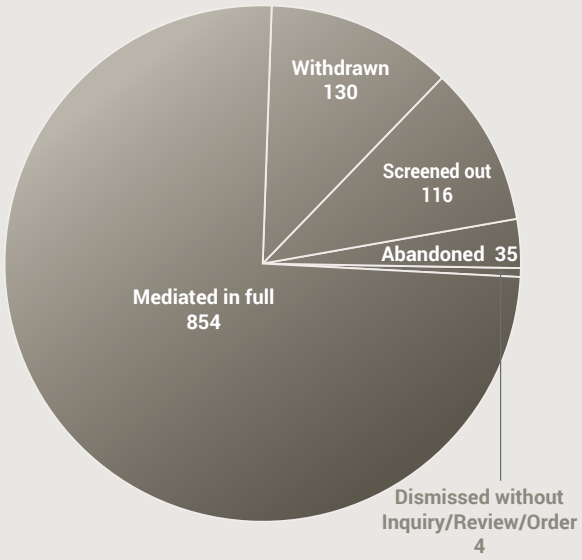
STATISTICS



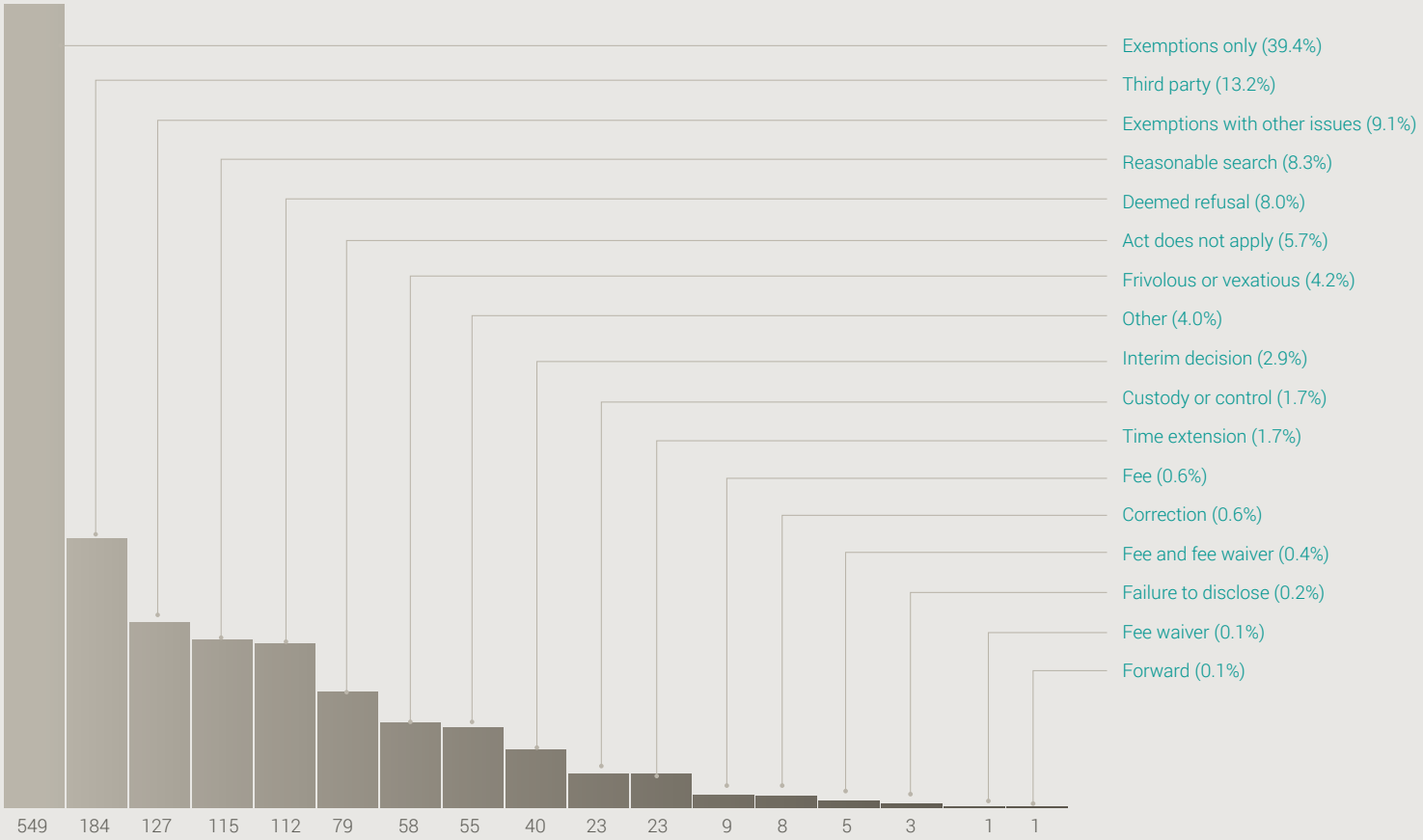
NUMBER OF APPEALS CLOSED BY ORDER, BY ORDER OUTCOME



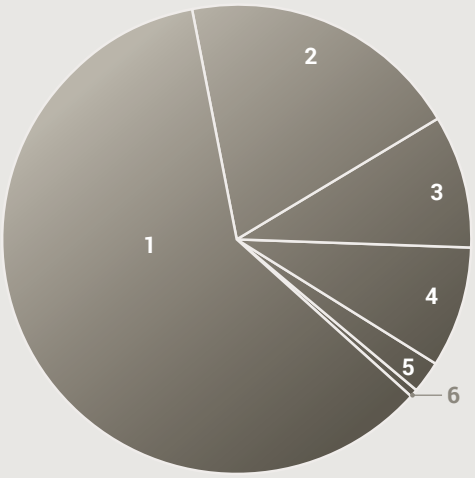
NUMBER OF APPEALS CLOSED OTHER THAN BY ORDER, BY OUTCOME

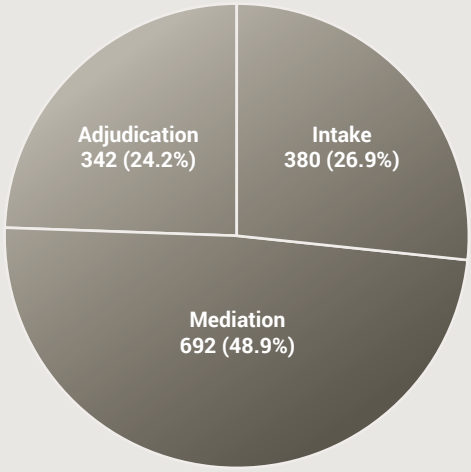


ISSUES IN APPEALS OPENED



OUTCOME OF APPEALS BY STAGE CLOSED



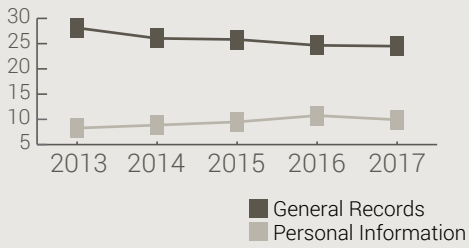


1. **Mediated in full: 854 (60.4%)**
2. **Order issued: 275 (19.4%)**
3. **Withdrawn: 130 (9.2%)**
4. **Screened out: 116 (8.2%)**
5. **Abandoned: 35 (2.5%)**
6. **Dismissed without Inquiry/ Review/Order: 4 (0.3%)**

STATISTICS

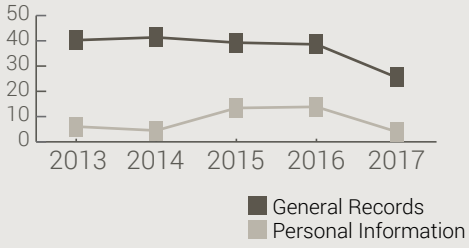
AVG COST OF MUNICIPAL REQUESTS

PERSONAL INFORMATION	GENERAL RECORDS
$9.92	$24.50



AVG COST OF PROVINCIAL REQUESTS

PERSONAL INFORMATION	GENERAL RECORDS
$4.02	$25.53



TOTAL FEES COLLECTED AND WAIVED

MUNICIPAL	PROVINCIAL	TOTAL
$173,078.59 TOTAL APPLICATION FEES COLLECTED	$103,862.45 TOTAL APPLICATION FEES COLLECTED	$276,941.04 TOTAL APPLICATION FEES COLLECTED
$436,405.71 TOTAL ADDITIONAL FEES COLLECTED	$400,480.33 TOTAL ADDITIONAL FEES COLLECTED	$836,886.04 TOTAL ADDITIONAL FEES COLLECTED
$609,484.30 TOTAL	**$504,342.78** TOTAL	**$1,113,827.08** TOTAL
$47,570.83 TOTAL FEES WAIVED	$13,850.59 TOTAL FEES WAIVED	$61,421.42 TOTAL FEES WAIVED

FINANCIAL STATEMENT

	2017-2018 Estimates $	2016-2017 Estimates $	2016-2017 Actual $
SALARIES AND WAGES	13,404,400	10,444,100	10,447,365
EMPLOYEE BENEFITS	3,083,600	2,401,900	2,078,290
TRANSPORTATION AND COMMUNICATIONS	286,700	337,500	165,348
SERVICES	3,123,900	1,960,300	2,353,714
SUPPLIES AND EQUIPMENT	489,000	336,000	247,038
TOTAL	20,387,600	15,479,800	15,291,755

Note: The IPC's fiscal year begins April 1 and ends March 31.
The financial statement of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario.

2017 APPEALS FEES DEPOSIT

(Calendar year)

GENERAL INFO.	PERSONAL INFO.	TOTAL
$18,660	$2,972	$21,632

See further financial information, including IPC Public Sector Salary Disclosure, at www.ipc.on.ca.

2017
ANNUAL REPORT

Office of the Information and Privacy Commissioner of Ontario

2 Bloor Street East,
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

www.ipc.on.ca