Facing Challenges Together

TWO THOUSAND AND SIXTEEN ANNUAL REPORT

Information and Privacy Commissioner of Ontario

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

June 19, 2017

The Honourable Dave Levac
Speaker of the Legislative Assembly of Ontario

Dear Speaker,

I have the honour to present the 2016 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, 2016.

Please note that additional reporting from 2016, 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

Facing Challenges Together

Information and Privacy Commissioner of Ontario • 2016 Annual Report

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE 1

ABOUT US 4

OUR WORK 5

ACCESS TO INFORMATION 8

- PUBLIC INTEREST DISCLOSURES 8
- ENCOURAGING A MORE OPEN GOVERNMENT 9
- THE USE OF INSTANT MESSAGING AND PERSONAL DEVICES FOR BUSINESS 10
- UNDERSTANDING ACCESS AND IMPROVING RECORDS MANAGEMENT 10
- FALSIFIED COMPLIANCE STATISTICS 11
- SOLICITOR-CLIENT PRIVILEGE 12
- OTHER SIGNIFICANT ACCESS DECISIONS 13
- MEDIATED APPEALS 16
- JUDICIAL REVIEWS 18

PROTECTION OF PRIVACY 20

- NEW PRIVACY SAFEGUARDS FOR SUICIDE-RELATED CPIC DISCLOSURE PROCEDURES 20
- ENSURING PRIVACY AND TRANSPARENCY IN THE GOVERNMENT'S STRATEGY FOR A SAFER ONTARIO 20
- PRIVACY COMPLIANT INFORMATION SHARING TO PREVENT HARM 21
- POLICE BODY-WORN CAMERAS (BWCs) 22
- RANSOMWARE ATTACKS 22
- SIGNIFICANT PRIVACY INVESTIGATIONS 22
- IPC PRIVACY MATERIALS PUBLISHED IN 2016 26

CONSULTATIONS 27

PHIPA: A PRESCRIPTION FOR PRIVACY 28

- IMPORTANT AMENDMENTS TO ONTARIO'S HEALTH PRIVACY LAW 28
- NEW HEALTH PRIVACY GUIDANCE: COMMUNICATING PERSONAL HEALTH INFORMATION BY EMAIL 28
- CONSULTATION ON THE VALUATION OF ONTARIO'S DIGITAL HEALTH ASSETS 29
- CONSULTATION ON BILL 41, *PATIENTS FIRST ACT, 2016* 30
- SIGNIFICANT *PHIPA* DECISIONS 30
- *PHIPA* CASES CLOSED THROUGH EARLY RESOLUTION 31

COMMISSIONER'S RECOMMENDATIONS 34

STATISTICS 38

FINANCIAL SUMMARY 45

At the start of my mandate in 2014, I committed to increased engagement and outreach to the citizens of this province. I remain committed to that goal, and in 2016 the IPC further enhanced stakeholder and public understanding of our work within the context of an evolving social landscape.

Brian Beamish
Commissioner

Facing Challenges Together

The right of Ontarians to know how their governments are operating and to be assured of their legitimate right to privacy are the fundamental principles that guide the work of the Office of the Information and Privacy Commissioner. During 2016, my office worked hard to reinforce these principles with government organizations at the provincial and municipal levels and inform the public about their access and privacy rights.

At the start of my mandate in 2014, I committed to increased engagement and outreach to the citizens of this province. I remain committed to that goal, and in 2016 the IPC further enhanced stakeholder and public understanding of our work within the context of an evolving social landscape.

Across privacy, access, and health, the IPC continued to examine emerging issues and develop practical guidance to help institutions and health information custodians ensure they are compliant with access to information and privacy legislation. Our active outreach resulted in more support and guidance to institutions and custodians than ever before. At the same time, we worked to ensure that the public's access to information rights were upheld, and through our advocacy, the concept of open and transparent government was advanced.

TRIBUNAL SERVICES

At the core of my office's mandate is our role in providing independent review of responses to freedom of information requests and investigating privacy complaints under our public sector and health privacy acts. To do this, we have a highly skilled and dedicated Tribunal Services team that is involved in early resolution, mediation, investigation and, if necessary, adjudication. In recent years, the number of cases dealt with by our staff has continued to increase. This past year was no exception, with an increase in incoming cases exceeding 10 per cent. I am pleased that my office successfully managed this increase with no additional resources.

In 2016, Tribunal Services issued orders on a number of complex and high profile issues that underlined the need for government organizations to consider the public interest in deciding whether to disclose records. For example, in June the IPC determined that physician billings are not exempt from disclosure under the *Freedom of Information and Protection of Privacy Act* and issued an order requiring the Ministry of Health and Long-Term Care to release the names of certain doctors, along with their OHIP billings. The adjudicator in this case referred to the concepts of transparency and accountability of government as important considerations supporting disclosure of this information.

In a related vein, I agreed with the decision of Algoma Public Health to release an investigation report into allegations of conflict of interest and financial mismanagement involving former executives. The conclusion in this case was that there was a compelling public interest in the disclosure of the report that outweighed any privacy interests that the former executives might have had.

POLICY

Much of our policy work over the course of the year focused on the benefits and privacy considerations when developing Open Government programs, as well as the benefits and corresponding risks of government's increased use of data analytics. There are definite opportunities presented by the increased availability of complex and rich data sets and the new analytical tools that can be applied to draw lessons from them. Governments and institutions can use the information gained from this process to create better policies, spend money more wisely and more accurately assess the effectiveness of existing programs and services. However, the potential exists for the improper profiling of individuals and groups, drawing incorrect inferences and ultimately using citizens' data in a manner that is discriminatory and invasive. Ensuring that the right privacy and ethical protections are in place prior to engaging in data analytics is crucial.

During the year, I had the opportunity to meet with Court of Appeal Justice Michael Tulloch, who was conducting a provincial review of police oversight bodies. I explained the benefits of releasing more information in the investigation reports of the Special Investigations Unit, including fostering accountability and public confidence in police services, and ensuring transparency in their operations. My position was further articulated in our submission to the Ministry of Community Safety and Correctional Services during its Strategy for a Safer Ontario consultation, in which we recommended that the government amend the *Police Services Act* to require greater transparency with respect to the investigation reports of the Special Investigations Unit.

This issue was also discussed as part of our Privacy Day symposium, held on January 26, 2016. The topic, Privacy and Public Safety, featured a panel discussion among privacy, human rights, and public safety experts, and attracted a significant number of stakeholders and members of the public. A key part of the discussion focused on the need for greater transparency and accountability in the oversight of law enforcement activities.

OUTREACH AND COLLABORATION

In 2016, we continued our popular Reaching Out to Ontario (ROTO) series with visits to Kingston and London where my colleagues and I updated stakeholders on emerging access and privacy issues facing the province's health and public sectors.

These events featured a variety of topics, including the challenges of conducting public business on personal devices; how to protect patient privacy; recent developments in access to information law; and whether cloud computing services are suitable for public sector information management needs.

This year, we also accepted invitations to participate in over 70 conferences and presentations.

Ontario covers more than 1,000,000 square kilometres, and is home to 444 municipalities. As much as we would like to visit each community, the sheer size of this province is an obstacle. To address this issue and to expand our outreach and educational efforts, we launched a new webinar series. Our inaugural event featured an online presentation and live question-and-answer session on information-sharing practices at "situation tables," and how community partners can work together to reduce harm while respecting the privacy of individuals. The turnout was impressive, with 400 individuals and groups logging on. I look forward to continuing the series in 2017.

2016 also saw the launch of our newly redesigned website, featuring a portal through which the public can easily access information and the forms they need to understand and exercise their access and privacy rights.

In 2016 the IPC had the honour of hosting the annual meeting of federal, provincial and territorial information and privacy commissioners. Our meeting included a wide range of important conversations, including discussions on the challenges raised by changes in government, public interest disclosures, open government and big data and surveillance. It also provided me with the opportunity to showcase our beautiful province to my colleagues from across Canada.

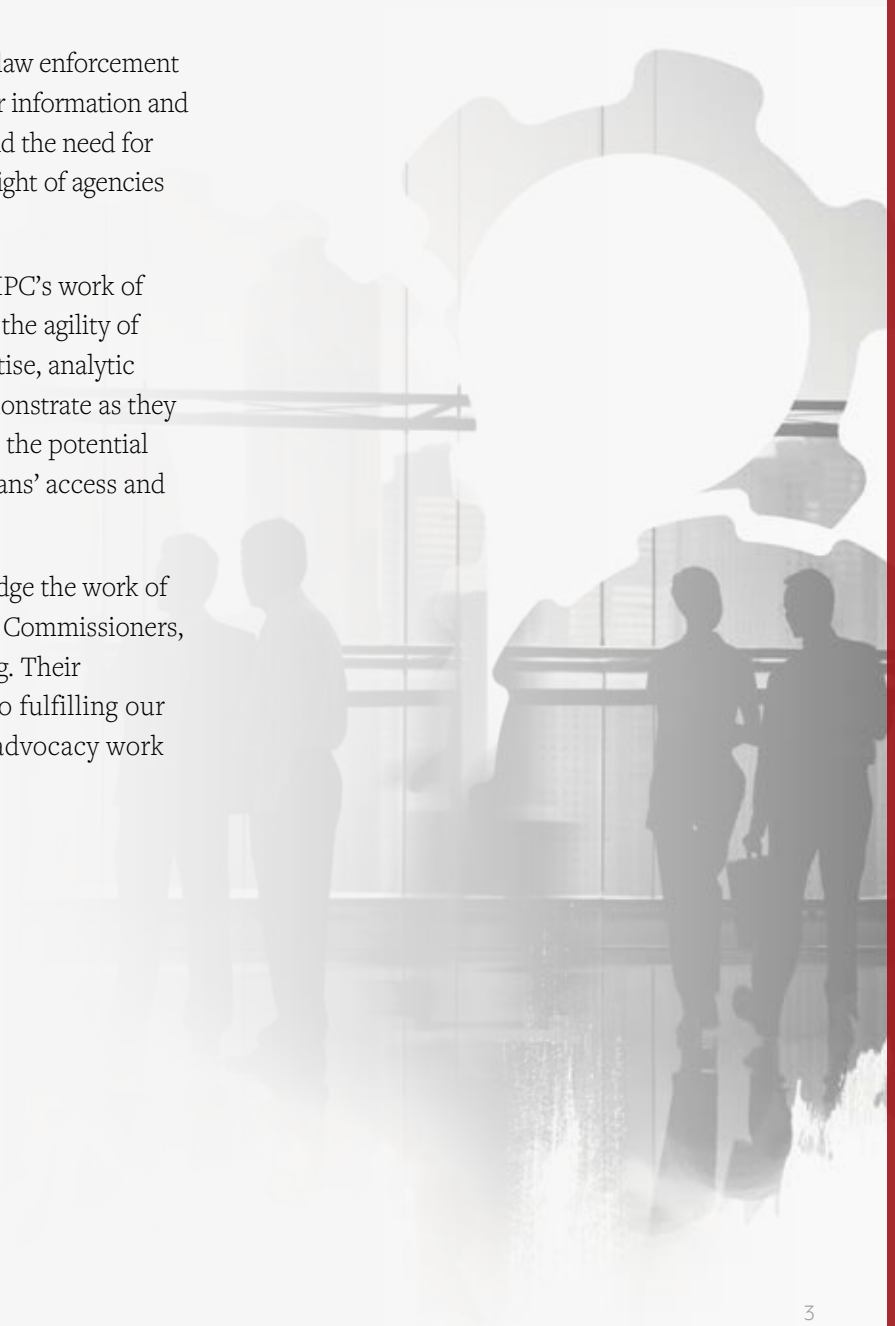
In early December I was pleased to sign my name, along with the federal Privacy Commissioner and my provincial and territorial counterparts, to a submission to the federal government in response to its public consultation on modernizing Canada's national security framework.

The submission raised a number of privacy issues, including the extent of domestic and international information sharing; the collection and retention of communications metadata; proposals to make it easier for law enforcement to access customers' subscriber information and encrypted communications; and the need for greater transparency and oversight of agencies involved in national security.

As I review and reflect on the IPC's work of this past year, I am amazed by the agility of my team. The collective expertise, analytic skill and nimbleness they demonstrate as they are faced with issues that have the potential to disrupt–or enhance–Ontarians' access and privacy rights are astounding.

In closing, I want to acknowledge the work of the IPC staff and my Assistant Commissioners, David Goodis and Sherry Liang. Their commitment and dedication to fulfilling our mandate and furthering our advocacy work continues to inspire me.

Brian Beamish
Commissioner



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.

OUR OFFICE

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.

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 2016, the IPC was mentioned more than 400 times in the media. The Commissioner made over 25 appearances and presentations.

Tribunal

INTAKE

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

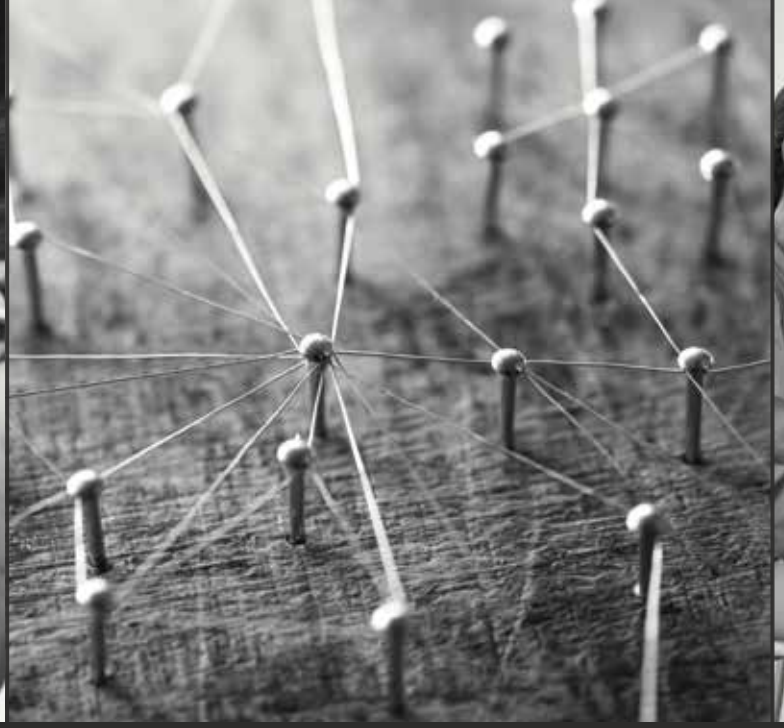
In 2016, our Registrar received:

- 1,548 access appeals, an increase of 10 per cent over 2015
- 537 health complaints, an increase of 17 per cent over 2015
- We received one more privacy complaint than in 2015, when we received 276

We closed more than 250 privacy and 100 health privacy complaints at intake in 2016.

INVESTIGATION AND MEDIATION

Our team of investigators gather information and resolve privacy complaints, including health privacy complaints. Our team of *FIPPA* and *MFIPPA* mediators work to resolve or narrow the issues in access appeals. While our decisions attract the most attention, the majority of access appeals and privacy complaints are resolved through mediation.



In 2016, 77 per cent of access appeals and 83 per cent of privacy complaints (including health privacy complaints) that were referred to mediation were settled.

ADJUDICATION

When a resolution cannot be found through mediation, access appeals and health complaints are forwarded to an adjudicator who will decide whether or not 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.

In 2016, our office issued 246 Access orders and 15 *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 cases regarding access to information and privacy issues.

In 2016, our Legal Services Department made more than 15 presentations and represented the Commissioner in six judicial review hearings.

Policy

Our policy analysts research, analyze and provide advice on current, evolving and emerging access and privacy issues. They are routinely asked to examine and review the access and privacy practices of both public and private organizations. They also examine and provide comments on any proposed legislation that may affect the rights of Ontarians.

In 2016, our Policy Department released 15 guidance documents and fact sheets, provided

consultations and advice to a variety of public sector organizations and made more than 20 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 2016, Health Policy issued two 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 with regards to matters of access and privacy. Our website, social media, media relations, and public events are managed by the communications team.

In 2016, Communications fielded more than 150 media calls, hosted a webinar for over 390 registrants, and oversaw three major events that attracted over 550 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.

Access to Information

The past year brought a range of important access to information issues into the spotlight. The issue of police accountability and transparency was the subject of public debate, to which Commissioner Beamish contributed. As well, our office made some important decisions on topics such as the disclosure of OHIP billings and the use of personal email accounts to do government business. Also, for the first time, we reviewed and upheld an institution's decision to rely on *MFIPPA*'s public interest override to release a document.

Public Interest Disclosures

The investigation into the police shooting of Toronto resident Andrew Loku brought Special Investigations Unit (SIU) transparency to the front page. Demands from the public to see the report, which cleared a Toronto police officer of any wrongdoing, dominated the news. The Attorney General subsequently released a redacted version of the report. Another outcome of this public discussion was the appointment of the Honourable Michael H. Tulloch of the Ontario Court of Appeal to lead an independent review of the three agencies that oversee police conduct in the province: the SIU, the Office of the Independent Police Review Director and the Ontario Civilian Police Commission. Commissioner Beamish provided his advice to this review. In his report, released in April of this year, Justice Tulloch made a number of recommendations which, if implemented, would significantly improve the transparency and accountability of police oversight bodies. Separate from the submission to Justice Tulloch, our office offered recommendations related to these agencies in a submission to the Ministry of Community Safety and Correctional Services on its Strategy for a Safer Ontario consultation. Our recommendations included suggested amendments to the *Police Services Act* to ensure transparency and accountability in outcomes of police misconduct complaints and SIU matters.

In June, our office issued a decision which discussed the public interest in disclosure of information relating to OHIP billings (PO-3617). A media requester asked the Ministry of Health and Long-Term Care for the names, specialties, and payments made to OHIP's top 100 billers in each of the past five years. The ministry disclosed all payment amounts and the specialties of some physicians, but withheld the names of the physicians and some of the identified specialties, claiming an invasion of personal privacy. On appeal, Adjudicator John Higgins overruled the ministry's decision and ordered full disclosure of the requested information, deciding that the payment amounts related to the physicians in their professional or business capacity and did not reveal personal information. In his decision, he also discussed the public interest in disclosure of this information, stating that "the concept of transparency, and in particular, the closely related goal of accountability, requires the identification of parties who receive substantial payments from the public purse."

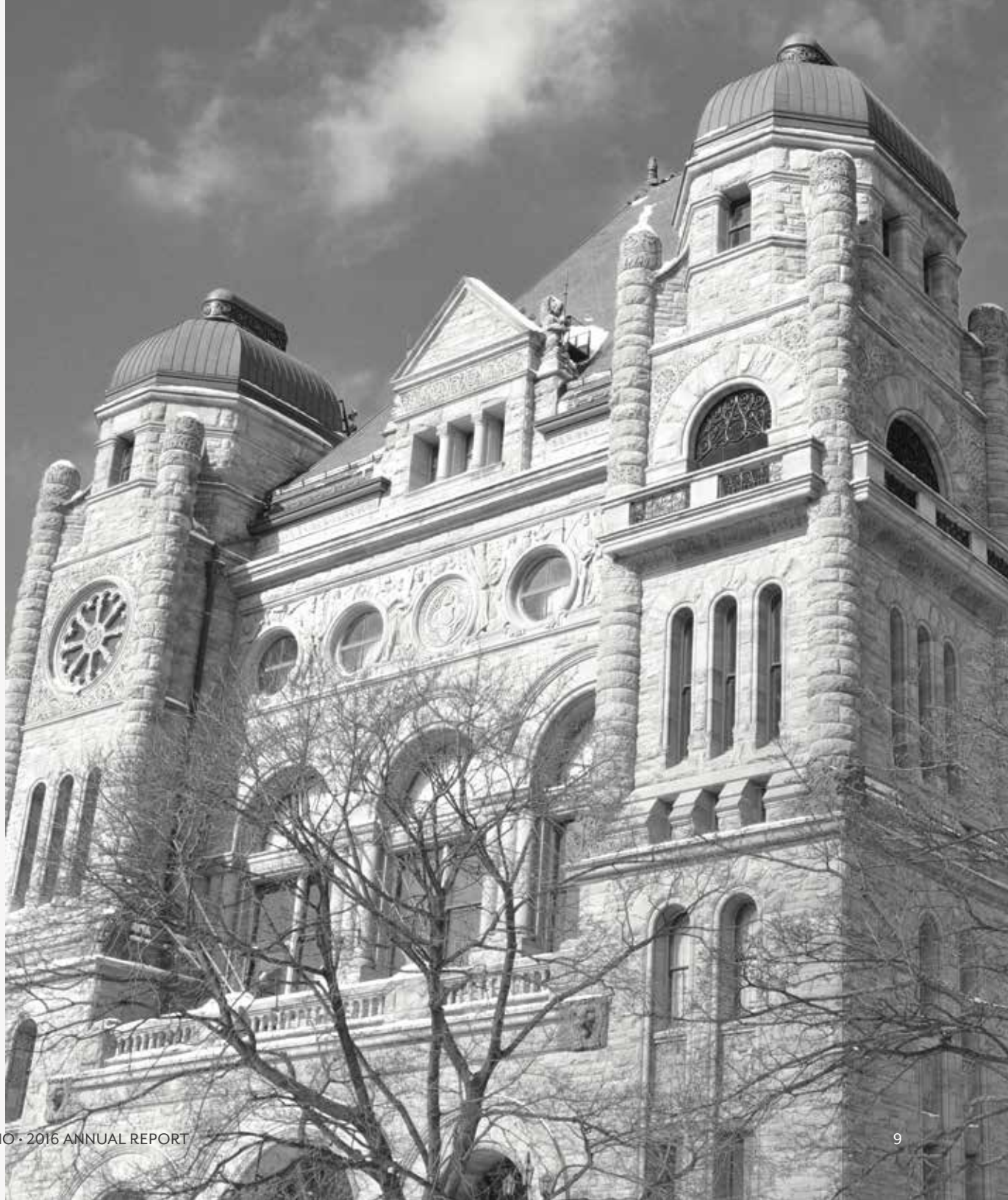
For the first time, our office dealt with an appeal from a decision that granted access to a document using the public interest override. At issue was a report of a forensic review, conducted by KPMG, into allegations of

conflict of interest regarding the appointment of the former interim CFO at Algoma Public Health (APH), and allegations of misappropriation or loss of funds. In response to an access request, APH determined that the report contained personal information, but that the public interest overrode any privacy interests. On appeal (MO-3295), we agreed with this decision. We encourage other institutions to consider whether the public interest override justifies disclosure of records, even where exemptions apply.

Both of these orders are currently under judicial review and we await the court's decision.

Encouraging a More Open Government

We continued to support proactive disclosure of government-held information and stressed the need for open government in a number of papers and presentations. In September, we released two papers, *Open Government: Key Concepts and Benefits* and *Open Government: Key Implementation Considerations*, both of which highlight the benefits of creating more transparent and accountable government. In the future, we will continue to engage with institutions and support their efforts to implement Open Government programs.



The Use of Instant Messaging and Personal Devices for Business

Some of Ontario's public servants, elected officials, and political staff use instant messaging services and personal or political party email accounts, in addition to their institution-issued email accounts, to conduct business.

This year, we ordered (in MO-3281) the city of Oshawa to issue an access decision about an email that a city councillor sent using her personal email account. The email asked an investigator for feedback on the terms of his eventual hiring by the city. The city argued that since the councillor did not use the city's server to send the email, the email was not in the custody of the city and was therefore not covered by Ontario's access to information laws. We found that the matter related to city business and that the email was subject to access legislation. As a result of this decision, we determined that there was a need for more education to help the public sector understand that using personal email accounts does not affect access rights to records otherwise within the custody or control of an institution.

Released in June, *Instant Messaging and Personal Email Accounts: How to Meet Your Access and Privacy Obligations* recommends that leaders of public institutions strictly control the use of instant messaging and personal email accounts for conducting business. If it is necessary to use these tools, institutions should implement appropriate policy and technical measures to ensure that business-related records are saved. It is the responsibility of all institutions subject to *FIPPA* and *MFIPPA* to ensure that the right of access is not undermined through the use of instant messaging or personal email accounts.

Understanding Access and Improving Records Management

We published several documents this past year to help government institutions understand and enhance the public's right to access information. To assist in developing effective records and information management (RIM) practices, we issued *Improving Access and Privacy with Records and Information Management*. Good RIM practices

can improve an institution's ability to respond to access requests in a timely way, to be transparent and accountable to the public, and to ensure the confidentiality and privacy of personal information.

We also created a new series of fact sheets to inform institutions and the public about specific aspects of Ontario's access to information laws. The fact sheets are intended to help parties navigate the access to information process, understand how the IPC applies the exemptions and exclusions in the acts, and learn about key decisions and findings. Fact sheets published in 2016 include: *The Municipal Freedom of Information and Protection of Privacy Act and Councillors' Records*; *You are Affected by a Freedom of Information Request: What You Should Know*; *Your Business is Affected by a Freedom of Information Request: What You Should Know*; and *What is Personal Information?* Additional fact sheets are planned to support institutions' ongoing efforts to become more innovative, effective and responsive to Ontarians' right of access to government information.

Falsified Compliance Statistics

We were alerted this year to a serious issue in one ministry regarding the conduct of its staff in reporting to our office. Ontario's provincial

and municipal access laws place important responsibilities on freedom of information (FOI) staff. These responsibilities include responding to access requests in a timely manner, and accurately reporting statistics about these activities to the IPC. Included in our annual reports are tables showing compliance rates by provincial and municipal institutions with the time requirements of *FIPPA* and *MFIPPA*, known as compliance statistics. The tables set out, for each institution, the number and per cent of FOI requests completed within the 30-day time limit mandated by these statutes, those completed within a permissible extended time, and those that were late. After the release of the 2015 Annual Report, we were informed by the Ministry of the Environment and Climate Change (MOECC) of concerns about the accuracy of the compliance statistics it submitted to the IPC. The ministry's senior management became aware of a practice in the ministry's Corporate and FOI Services Office to change dates recorded in the request tracking system, and consequently misstate the statistics reported to us. In response to this concern, the ministry's deputy minister, Paul Evans, directed the Ontario Internal Audit Division of the Treasury Board Secretariat to audit the practices and procedures of the ministry's FOI office. In December, we received the full audit report, together with a summary of the revised FOI compliance statistics for 2010 to 2015. Auditors concluded that the dates in the ministry's request tracking system were systematically adjusted by staff in order to show completion of requests within the 30-day requirement.

We notified the Speaker of the Ontario Legislature of these events, provided updated compliance rates to the Legislature, and updated our online statistics.

At the Commissioner's request, the Information, Privacy and Archives Division of the Ministry of Government and Consumer Services (IPA) asked Ontario Internal

Audit Division to conduct spot audits in other ministries to assess whether the issues identified at the MOECC were more widespread. The five ministries selected for the audit, the Ministry of the Attorney General (MAG), the Ministry of Community Safety and Correctional Services (MCSCS), the Ministry of Community and Social Services (MCSS), the Ministry of Natural Resources and Forestry (MNRF), and the Ministry of Labour (MOL), along with MOECC, represent 89 per cent of all FOI requests processed by provincial ministries. In addition, the IPA asked all ministries to complete a self-assessment of their FOI operations, approved by each deputy minister or assistant deputy minister with delegated authority to oversee the administration of *FIPPA* within each ministry, which included questions on the verification of statistics reported to the IPC.

The results of the spot audits were shared with the IPC. The report of the auditors revealed some instances in which ministry practices need to be strengthened to ensure full compliance with *FIPPA*. Among other things, the audit found evidence that in three ministries, some dates were modified in tracking systems. The respective ministries confirmed that, unlike at MOECC, the audit revealed no evidence that staff systematically adjusted dates to deliberately manipulate compliance statistics. The ministries also confirmed that any modification of dates was procedural, and due to lack of training and guidance regarding FOI processes. The chief administrative officers of these three ministries have verified that the statistics reported to the IPC for 2016 are accurate, and were compiled with knowledge of and taking into account the findings from the MOECC audit and the audit of their ministries.

The IPA has advised our office that it has begun the process of implementing a number of policies and procedures to strengthen FOI programs across the Ontario Public Service, including the development of comprehensive training and updated guidelines for managers and staff at each ministry's FOI offices, to ensure staff are aware of their responsibilities, and that all offices are consistently processing access to information requests and recording compliance statistics. Follow-up audits and spot checks will be conducted on the ministries in which discrepancies were found.

Solicitor-Client Privilege

In 2016, a Supreme Court of Canada ruling on solicitor-client privilege spurred the IPC to begin talks with the government about clarifying our powers in legislation.

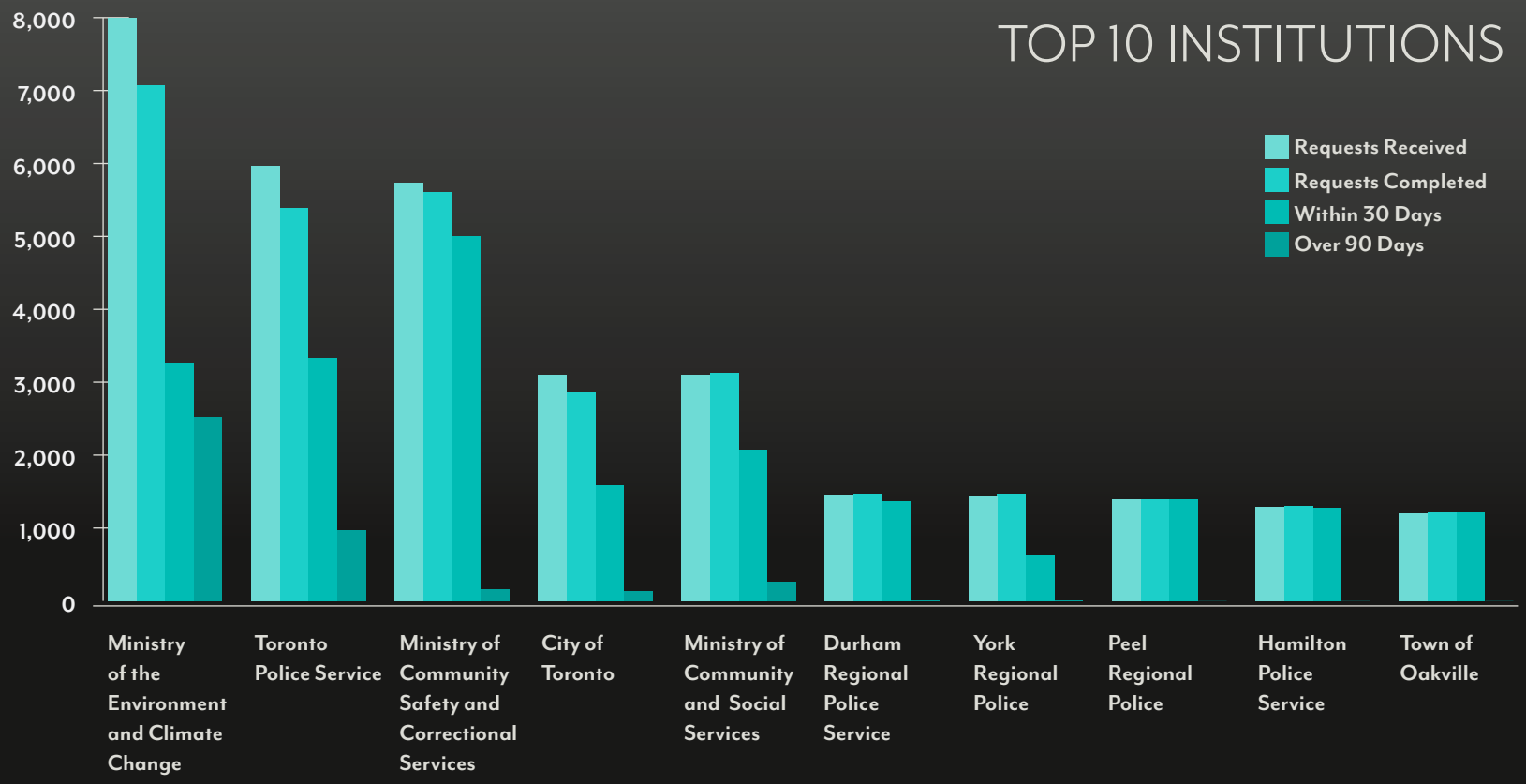
The court found that Alberta's *Freedom of Information and Protection of Privacy Act* was not clear enough to empower the Information and Privacy Commissioner of that province to compel production of records so that she might determine whether solicitor-client privilege was being properly claimed over records sought in an access to information request.

Although the wording of Ontario's laws is different from that in Alberta, legislation confirming our powers in this area is needed. In September we wrote to the Chief Privacy

Officer and Archivist of Ontario suggesting potential amendments to Ontario's *FIPPA* and *MFIPPA* which would clarify that the IPC can view records claimed to be privileged or excluded, including when solicitor-client privilege is claimed, and that providing records to the IPC does not constitute a waiver of solicitor-client privilege. This proposed clarification would ensure that our office receives the information we need to discharge our responsibility to decide whether exemptions are being properly applied by government institutions. No decision has yet been made on these recommendations.

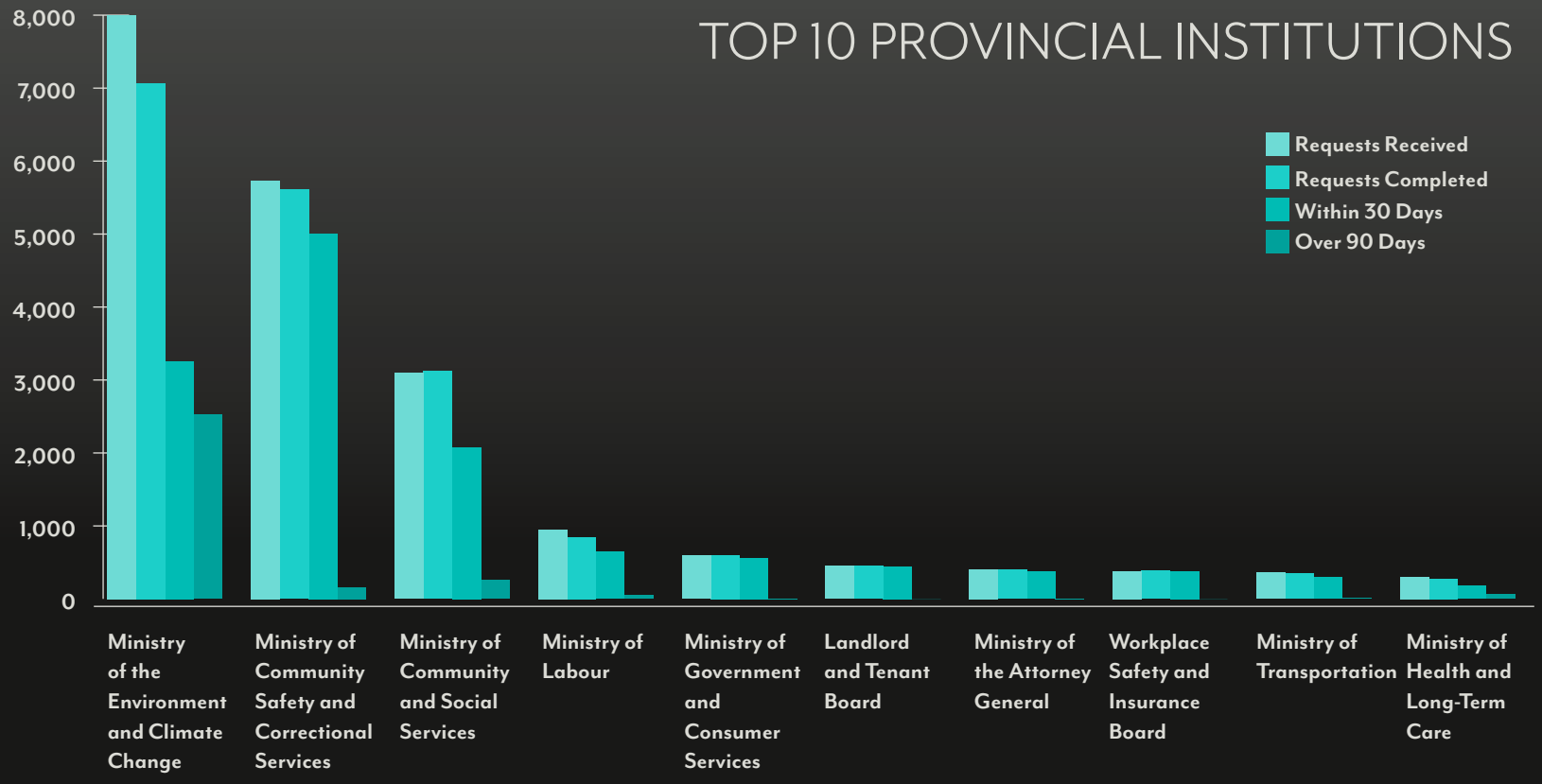
Other Significant Access Decisions

In addition to Orders PO-3617 and MO-3295, described above, our office issued a number of other decisions this year giving direction on how *FIPPA* and *MFIPPA* should be applied, including:



PO-3599 - The requester wished to have access to OPP investigation records about allegations that he had committed a criminal offence involving his daughter. Our office upheld the Ministry of Community Safety and Correctional Services' decision to deny access to the records, finding that the requester is not entitled to exercise access to information rights on behalf of his children in these circumstances.

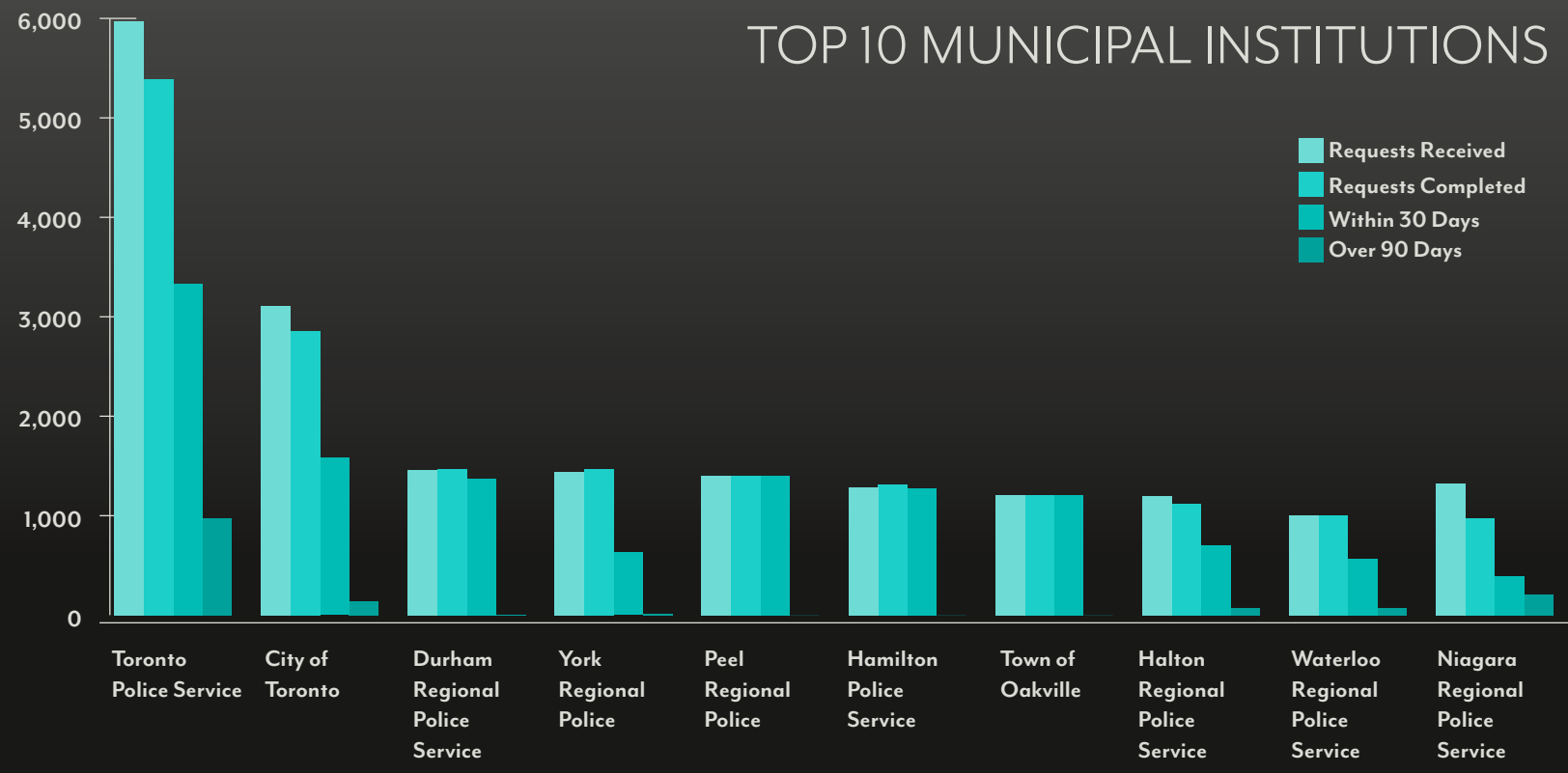
MO-3320 - A newspaper reporter requested a chart showing the number of students who were suspended or expelled at each high school in the Durham District School Board over a three-year period. The board denied access to this record using various exemptions (economic and other interests, information soon to be published and



personal privacy). We found that this record is not exempt under any of those provisions and ordered it to be disclosed.

PO-3643 - A request to the Ministry of Community Safety and Correctional Services for the number of in-patient suicides committed at named Ontario hospitals and psychiatric facilities in certain years was found not to be "personal information." We determined that the disclosure of the numbers alone would not reveal information about identifiable individuals.

MO-3395-I - A request was made to the town of Newmarket for access to records relating to the town's decision to provide a $2.8 million loan to a local soccer club. The town's decision to deny access to the records under the third-party information exemption was not upheld.



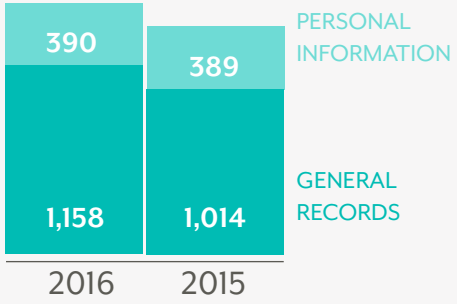
We ordered these files to be disclosed with the exception of one record which qualified under the closed meeting exemption.

Mediated Appeals

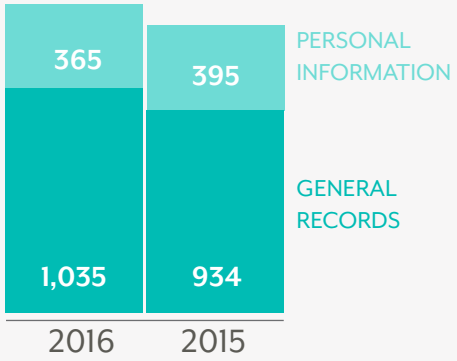
While our office's decisions receive most of the public's attention, a large number of access to information appeals are resolved through mediation. Below are some examples of resolutions we achieved through mediation last year:

- A police service denied a reporter's request for statistical information regarding the staffing of patrol officers. During mediation, the police advised the reporter that it does not collect the type of statistical information she requested. However, following further inquiries, the police located manually-recorded information which could be used to generate this data. The parties discussed the details in a teleconference which resulted in the police preparing a chart with the specific information. Upon receiving the data, the reporter was satisfied with the results.
- An individual requested a list of policies currently in force from a police service, including policies on note-taking, impaired driving, and domestic disputes/violence. The police granted access to its notebook maintenance and retention policy, but denied access to the remainder, citing law enforcement and health and safety concerns. The mediator sought clarification from the requester about the type of information he was specifically seeking, and provided the parties with previous IPC orders pertaining to policy manuals. The police subsequently issued a revised decision to the requester, providing an explanation about the particular internal policies, and also re-exercised its discretion to disclose additional information, which satisfied the individual.
- A city denied access to records relating to a tender for local towing services. Following a review of our orders dealing with similar types of procurement records provided by the mediator, the city notified three affected parties to seek their views on disclosure. The city received submissions from two of the parties resisting disclosure, while a third affected party said it had no concerns with disclosure. The city then issued a revised decision granting full access to the records remaining at issue, subject to third-party appeals filed by the towing companies. Additionally, the city advised us that it is in the process of changing its practice to encompass the proactive disclosure of procurement records.

APPEALS OPENED IN 2016



APPEALS CLOSED IN 2016



We support institutions' ongoing efforts to become more innovative, effective and responsive to Ontarians' right of access to government information.

Judicial Reviews

Metrolinx and Third-Party Records

Metrolinx received a request for records which form part of, or relate to, the PRESTO Master Supply and Services Agreement between the Ministry of Transportation and a third party (Accenture). Metrolinx granted the requester access to the responsive records, in part. Other information was withheld based on the third-party information exemption. Both the requester and Accenture appealed Metrolinx's access decision to the IPC. In PO-3392, the adjudicator largely upheld Metrolinx's decision and also ordered Metrolinx to disclose additional information relating to unit prices. Accenture sought judicial review of our decision. The Divisional Court dismissed the judicial review, finding that the IPC reached a reasonable decision respecting the application of the third-party information exemption. Among other things, the court rejected the notion that the adjudicator was unreasonable in requiring "detailed and convincing" evidence to satisfy the existence of a reasonable expectation of probable harm.

Actuarial Reports Qualify for Exemption

The Ministry of Finance denied access to actuarial reports and other financial records related to three separate pension plans based on the third-party information exemption, among other exemptions. The requester appealed this decision to our office. At adjudication, the request was narrowed to the actuarial reports, for which only the third-party information exemption was claimed. The adjudicator held in PO-3472 that the ministry and the administrators of the pension plan did not provide sufficient evidence to substantiate the "harms" component of the third-party information exemption. Two of the pension plans sought judicial review of our decision. On review, the Divisional Court found that the standards of proof and causation applied by our office were too onerous in the circumstances and that the adjudicator had failed to adequately take into account the labour relations context in which this information was sought. Accordingly, the court quashed our decision.

Common Interest Privilege Does Not Apply

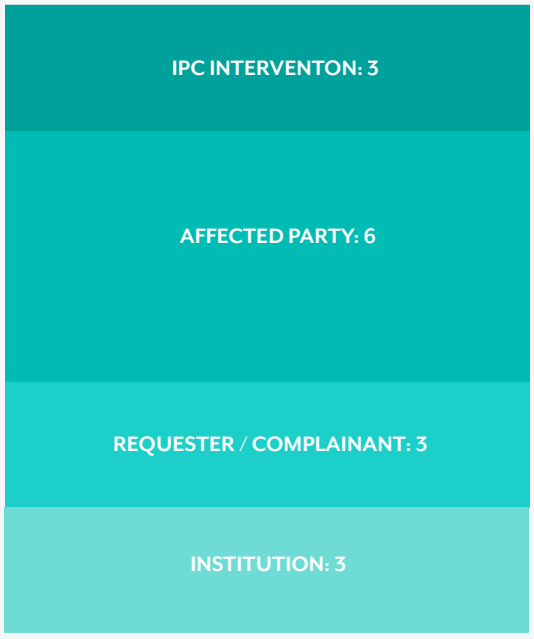
The Ministry of the Attorney General received a request for access to three drafts of a ministry guideline relating to the prosecution of HIV exposure and transmission cases. The ministry denied access based on the solicitor-client privilege exemption. The requester appealed to our office and argued that the drafts are not privileged, but even if they were, privilege was waived when one of the drafts had been shared with a manager of the public health unit at the city of Hamilton. PO-3514 found that the drafts were initially privileged, but the sharing of one of the drafts with the city manager was not a solicitor-client communication. Moreover, the ministry and the manager did not have a common interest in the privileged

communication and therefore the privilege had been waived by the disclosure. Accordingly, the draft guideline that had been shared was ordered disclosed. The ministry sought judicial review of the decision and argued, among other things, that the adjudicator erred in finding that common interest privilege did not apply. The court rejected the ministry's claims and dismissed the judicial review application.

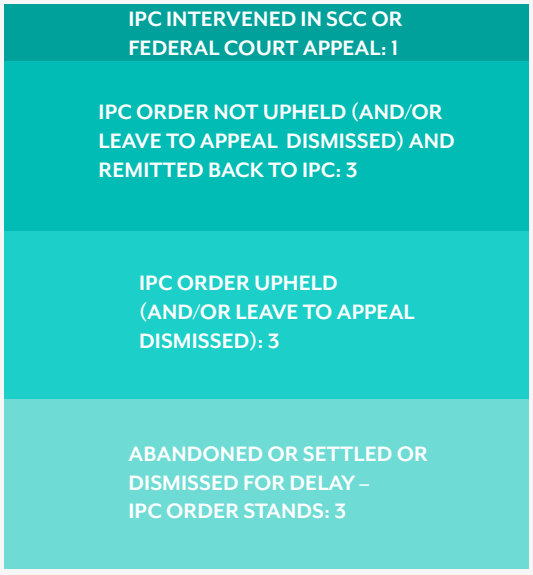
Factual Material Does Not Qualify for Advice or Recommendation Exemption

A request was submitted to the town of Arnprior for information relating to the town's electronic records storage initiative and service contracts with existing suppliers for services, including internet services, maintenance of existing hardware and firewall services. The town denied access to some responsive information based on several exemptions including advice and recommendations, third-party information and danger to safety and health. In MO-3174-I/MO-3175, the adjudicator found only limited portions of records qualified for the advice and recommendations exemption. We ordered the town to re-exercise its discretion for these portions and to disclose the remainder of the records. The Divisional Court upheld this decision on judicial review. Among other things, the Divisional Court rejected the town's argument that factual material, which can be disclosed without revealing any advice or recommendations, is exempt from disclosure simply because it appears in a document which may also contain advice or recommendations.

New Judicial Review applications & IPC interventions in 2016: **13**



Ongoing Judicial Reviews & IPC interventions as of December 31, 2016: **15**



Judicial Reviews & IPC interventions Closed and/or Heard in 2016: **10**

Protection of Privacy

In 2016, the IPC continued its work with provincial and municipal institutions, which included supporting their efforts to comply with Ontario's privacy laws. We also participated in consultations and provided advice on privacy issues relating to topics such as technology and public safety. Here are the highlights of the key privacy issues for 2016.

New Privacy Safeguards for Suicide-Related CPIC Disclosure Procedures

In July the IPC, the Toronto Police Service (TPS) and the Toronto Police Services Board ended legal action after new police procedures, developed in collaboration with the IPC, were put in place to better protect the privacy of Ontarians who have had information related to attempted suicide collected by the Canadian Police Information Centre (CPIC).

The new measures restrict the disclosure of attempted suicide-related information to U.S. Customs and Border Protection, allow for time-limited, public safety disclosures to police in Canada, and provide affected individuals with a right to seek early removal from CPIC.

The new measures came after the IPC went to court to request an order to stop the broad disclosure of suicide-related information to U.S. agencies via the CPIC database. The IPC had previously called for all Ontario police services to restrict CPIC disclosures under the Mental Health Disclosure Test (MHDT), set out in the special investigation report: *Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CPIC*.

In announcing the end of legal action, Commissioner Beamish described the new approach as a privacy compliant model for police across Ontario, "By working collaboratively, the IPC and the TPS have been able to address privacy and public safety. Input from police, privacy, mental health and human rights stakeholders made all the difference. I recommend that other Ontario police services incorporate the new safeguards into their suicide-related CPIC disclosure procedures."

Ensuring Privacy and Transparency in the Government's Strategy for a Safer Ontario

In April, we presented a submission to the Ministry of Community Safety and Correctional Services (MCSCS) in response to its public consultation on the government's Strategy for a Safer Ontario.

Our submission commended MCSCS for openly engaging with the public on this important initiative and made several recommendations associated with MCSCS' goal of ensuring effective, sustainable and community-based policing.

The IPC recommended that collaborative community safety and well-being initiatives such as situation tables (described further below) be supported by clearly defined governance frameworks that meet transparency and privacy best practices, including the data minimization principle.

The IPC recommended that the government enact province-wide standards governing the use of surveillance technologies such as automated licence plate recognition and body-worn cameras. Such rules are needed to ensure transparency and accountability in the use of these technologies.

The IPC also recommended that police services be required to establish data collection and retention systems to record human rights-based data on key interactions with civilians, and to publish detailed de-identified reports. We also recommended amending the *Police Services Act* to ensure that police disciplinary hearing decisions, police chiefs' SIU (Special Investigations Unit)-related disciplinary investigation reports, and SIU investigation reports generally be made available to the public.

Privacy Compliant Information Sharing to Prevent Harm

MCSCS' GUIDANCE ON INFORMATION SHARING IN MULTI-SECTORAL RISK INTERVENTION MODELS

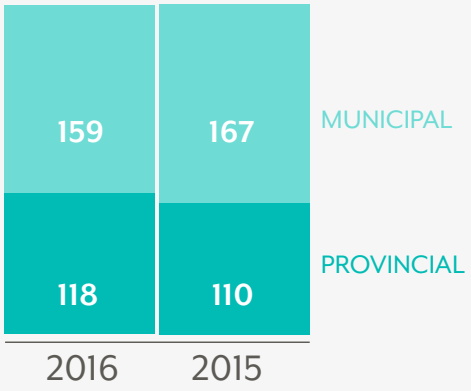
This year, we advised the Ministry of Community Safety and Correctional Services (MCSCS) on the development of its *Guidance on Information Sharing in Multi-Sectoral Risk Intervention Models*. This publication outlines the recommended privacy protective approach to the sharing of personal information between different community agencies (for example police, schools and health care providers) involved in collaborative risk reduction work, such as at a "situation table." A situation table is a group of professionals that meets periodically to identify and address individual cases that raise serious and immediate concerns about community safety or well-being that one agency cannot address alone.

The guidance document, which has the support of the IPC, discusses a common set of principles—including those tied to privacy requirements—that should be followed by the professionals when considering sharing personal information at such tables.

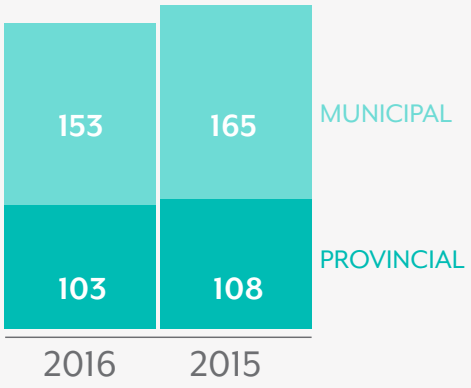
For example, the ideal way to share personal information about an individual is by first obtaining that individual's consent. When it is not possible to obtain consent, disclosure may be permitted under what MCSCS calls the 'Four-Filter' approach. The need to use de-identified information to the greatest extent possible is emphasized in this approach.

In December, situation tables were discussed among a panel of experts as part of the first in a series of webinars focusing on access and privacy issues. The IPC's *Privacy Protective*

PRIVACY COMPLAINTS OPENED IN 2016



PRIVACY COMPLAINTS CLOSED IN 2016



Roadmap for Situation Tables webinar drew close to 400 participants. The presentation continues to be used to help train professionals on privacy issues that may arise during the situation table process.

Police Body-Worn Cameras (BWCs)

The IPC supports the use of BWCs by police to enhance community safety, police accountability and public confidence in policing. The key is to put in place the technological controls, business practices and governance framework that will help ensure that BWCs are implemented and used in a manner that respects Ontarians' rights to privacy and access to information.

In 2016 we continued to work with the Toronto Police Service (TPS) on its BWC pilot project. In response to a proposal to require that BWCs be used to record all informal police-civilian interactions, the IPC advised that "there are significant privacy concerns associated with broadening the scope of the BWC pilot project to include the recording of informal interactions." The TPS agreed that using a BWC to record all informal interactions would not be in line with privacy requirements and police duties.

Ransomware Attacks

In 2016 large Canadian institutions such as universities and hospitals reported having their computer networks or systems attacked by some form of ransomware, which is a type of malicious software (malware) that encrypts files on devices or computers and then demands payment in exchange for the key needed to decrypt the files.

To help Ontario's public institutions and healthcare facilities protect themselves against the threat of ransomware, we published a fact sheet, *Protecting Against Ransomware*, that outlines various strategies for protecting information and how to respond to an attack. We describe a number of administrative and technological approaches organizations may take to help them meet their legislative requirements as outlined in Ontario's freedom of information and privacy laws. These approaches include employee training, limiting user privileges, software protections, and more.

Significant 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.

DISCLOSURES TO CHILDREN'S AID SOCIETY (CAS)

In January 2016 our office released *Yes, You Can. Dispelling Myths About Sharing Information with Children's Aid Societies*, in conjunction with the Provincial Advocate for Children and Youth. This guide assists professionals working with children to understand that privacy laws

are not a barrier to sharing information with a children's aid society (CAS) about a child who may be at risk.

During 2016, our office received two privacy complaints regarding disclosure of personal information to a CAS, which presented specific facts demonstrating the application of the principles discussed in the guide. The first case involved disclosure of personal information to a CAS by school board employees. This case was dismissed at the intake stage of the complaint process on the basis that the disclosure was authorized in accordance with a duty to report under section 72 of the *Child and Family Services Act*.

In the second case the IPC's investigator concluded that disclosure of some personal information of a parent by a police officer to the CAS was also in accordance with the duty to report. However, information relating to a withdrawn fraud charge was not relevant to the safety of the children and should not have been disclosed. The police service apologized to the complainant for this inadvertent disclosure and reminded its officers about the need to limit disclosure of personal information to that relevant to the particular safety concerns at issue.

COLLECTION OF TENANTS' PERSONAL INFORMATION

Our office received a complaint about a city's inappropriate collection of tenants' personal information during the process of licensing landlords. In particular, the city's landlord licensing by-law required landlords to provide their tenants' names, telephone numbers and other personal information. As a result of this complaint, the city agreed to cease collecting tenant information and subsequently amended its by-law. The city also confirmed that the personal information collected to date will be destroyed.

DISCLOSURES BY ADMINISTRATIVE TRIBUNALS

In 2016, the IPC received two complaints against separate administrative tribunals alleging that internet publication of tribunal decisions was a violation of the complainants' privacy. In each case the complainant was party to a proceeding before the tribunal.

In one case, the complainant was the applicant initiating the proceeding. This case was dismissed at the intake stage as the tribunal demonstrated that its hearings and the decisions that arise out of them are part of public proceedings. The IPC concluded that disclosure of the complainant's personal information through publication of decisions on the internet was consistent with *FIPPA*.

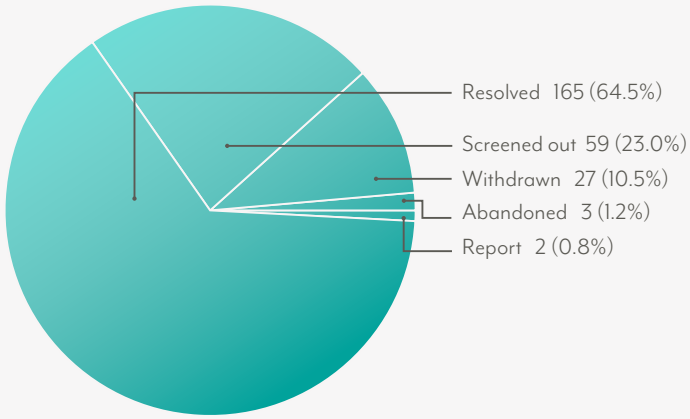
In the other case, the complainant was a member of a profession regulated by the tribunal. As a result of a complaint about his professional activities, the tribunal initiated a proceeding, concluding that the complainant had breached his professional duties, and imposed a lifetime ban on practicing within his profession. This case was dismissed at the intake stage as it was

determined that the tribunal has the authority to investigate and impose sanctions against members of the profession who may have breached the law. The continuing publication of the information about the complainant was consistent with the purpose for which it was collected, and not a breach of *FIPPA*.

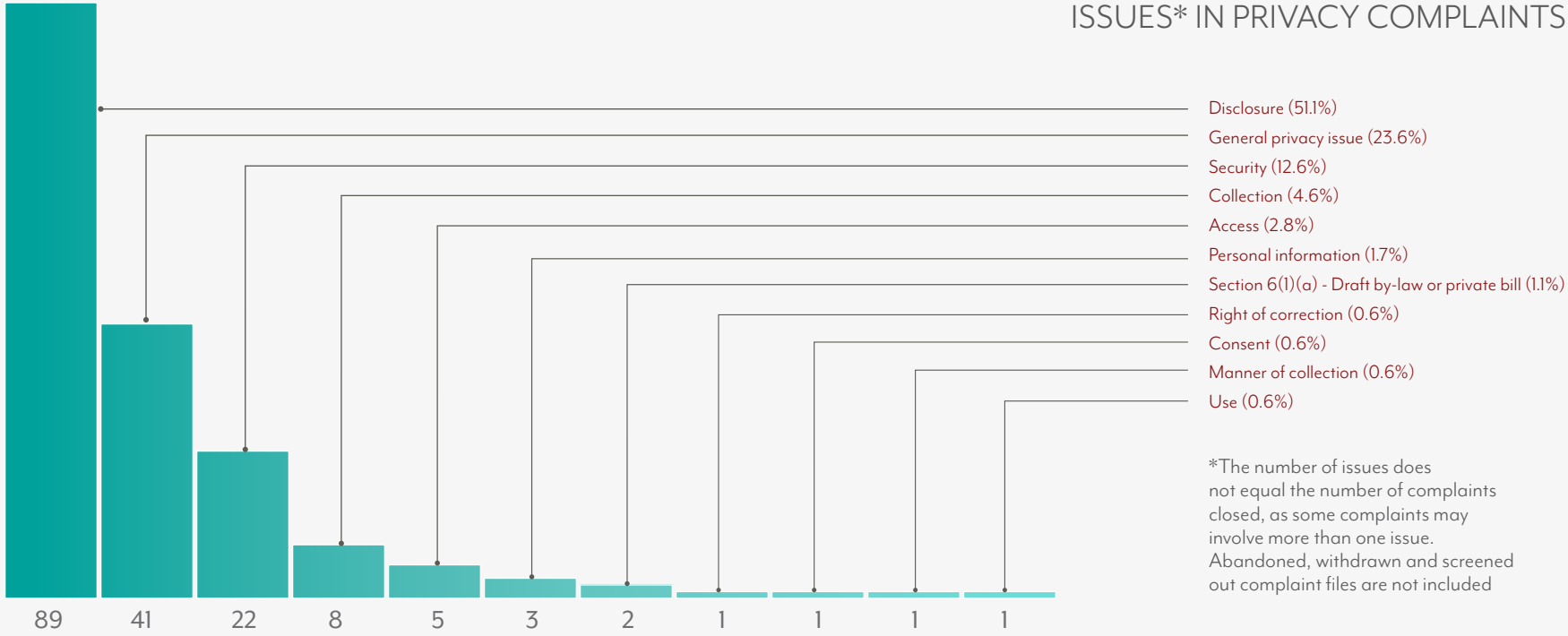
DISCLOSURES BY POLICE

A police association complained on behalf of its members (police officers) about disclosure by the police service to the media of *Police Services Act* (*PSA*) disciplinary decisions. The police service took the position that the IPC does not have jurisdiction to address the complaints made by the police association because the records at issue relate to employment and are therefore excluded from the act under section 52(3). We concluded, after receiving submissions from the parties, that disciplinary hearings relate to the "employment of a person by the institution,"

PRIVACY COMPLAINTS CLOSED BY TYPE OF RESOLUTION

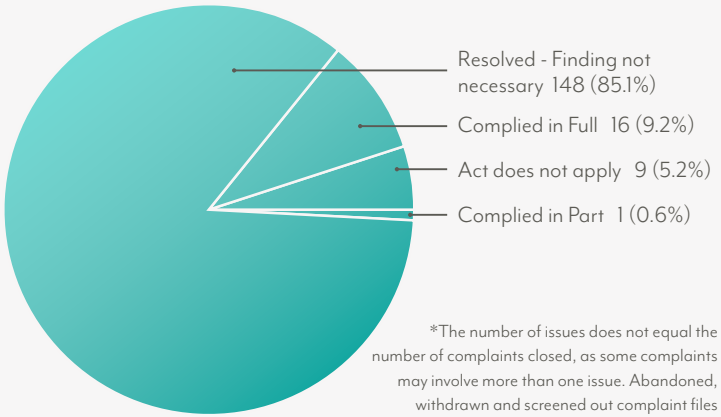


ISSUES* IN PRIVACY COMPLAINTS



*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

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.

and that the records at issue are excluded from the scope of *MFIPPA*.

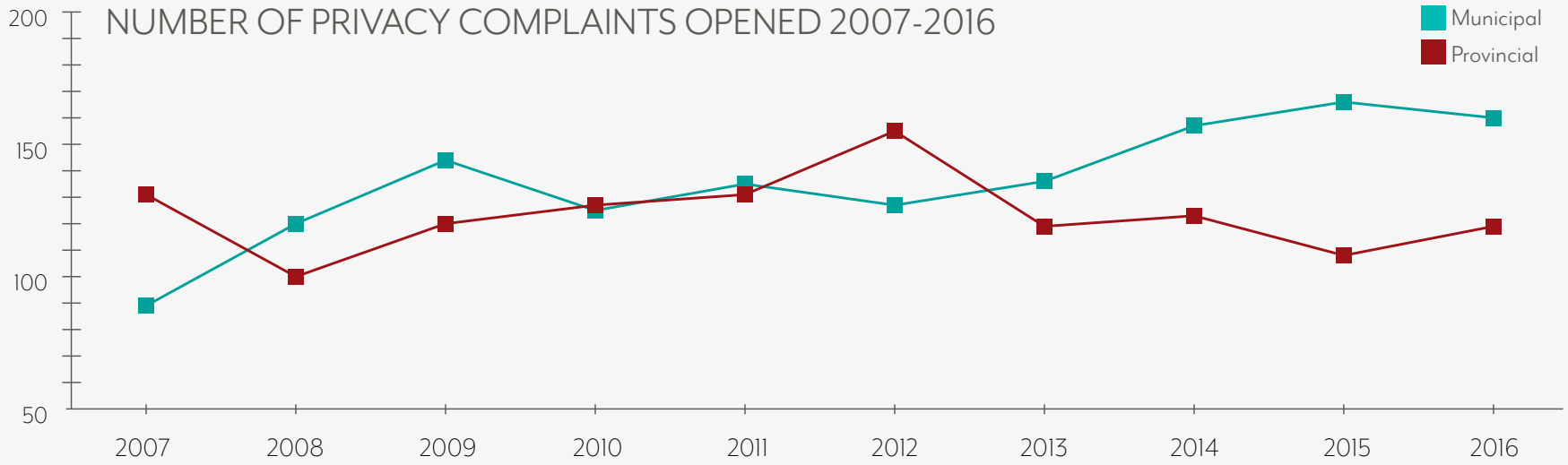
Privacy Complaint MC14-5

Hamilton-Wentworth Catholic District School Board
June 16, 2016

Privacy Complaint MC11-73

York Region District School Board
June 15, 2016

In each of these cases, the IPC received a complaint alleging that a school board contravened *MFIPPA* when it disclosed parts of a student's Ontario School Record to the Human Rights Tribunal of Ontario. In both cases, the parent of a student had brought a complaint to the tribunal against the school board. The disclosures by the boards were made in compliance with the tribunal's rules of procedure requiring parties to disclose to the tribunal any document on which they intend to rely during the hearing of a complaint. The privacy complaint reports conclude that the school boards did not breach *MFIPPA* in disclosing the records to the tribunal.



IPC Privacy Materials Published in 2016

The IPC regularly issues documents about access and privacy laws for government institutions to help them with compliance; the IPC also issues information for the public to inform them of their rights. Here is an overview of some of our privacy publications from 2016.

Privacy Fact Sheets

What is Personal Information? (October) provides the answers to frequently asked questions about the meaning of the term "personal information," as defined in Ontario's access and privacy laws.

Video Surveillance (November) outlines important factors Ontario institutions should consider before implementing a video surveillance system so they comply with Ontario's access and privacy laws.

Technology Fact Sheets

Our first in the series, *Protecting Against Ransomware* (July), provides information on how public institutions and healthcare organizations in Ontario can protect themselves against ransomware.

Guidance Papers

Thinking About Clouds? Privacy, security and compliance considerations for Ontario public sector institutions (February) helps institutions evaluate whether cloud computing services are suitable for their information management needs. It raises awareness of the risks associated with using cloud computing services and outlines some strategies to mitigate those risks.

De-identification Guidelines for Structured Data (June) outlines key issues to consider when de-identifying personal information in the form of structured data and provides a step-by-step process that institutions can follow when removing personal information from data sets.

Instant Messaging and Personal Email Accounts: Meeting Your Access and Privacy Obligations (June) assists institutions in meeting their administrative and legal obligations under Ontario's access and privacy laws with regard to the use of instant messaging and personal email accounts.

Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services (September) assists police services considering implementing this technology to ensure it is used in a privacy-protective manner.

Partnerships

Yes, You Can. Dispelling the Myths About Sharing Information with Children's Aid Societies (January) (with the Provincial Advocate for Children and Youth) is a guide to help professionals working with children understand that privacy laws should not be a barrier to sharing information with a children's aid society about a child who may be at risk.

Online Educational Services: What Educators Need to Know (November) (with the Ontario Association of School Business Officials). Brochure and poster that offers information for educators about the potential privacy risks of online educational services.

Consultations

MINISTRY OF MUNICIPAL AFFAIRS

- Bill 68—*Modernizing Ontario's Municipal Legislation Act, 2016* - Open Meeting Amendments to the *Municipal Act, 2001*, and the *City of Toronto Act, 2006*

INDEPENDENT ELECTRICITY SYSTEM OPERATOR

- Smart Metering Entity License Renewal Order

MINISTRY OF CHILDREN AND YOUTH SERVICES

- Bill 89—*Supporting Children, Youth and Families Act, 2016*

CITY OF TORONTO

- Specialized Program for Interdivisional Enhanced Responsiveness (SPIDER)

MINISTRY OF GOVERNMENT AND CONSUMER SERVICES

- Expert Panel on Gender and Sex Information on Government IDs and Forms
- Proposals to Strengthen Consumer Protection in the Alternative Financial Services Sector, including Amendments to the *Payday Loans Act, 2008*

PROVINCIAL ADVOCATE FOR CHILDREN AND YOUTH

- Information Sharing and the Death and Serious Bodily Harm Reporting System

CITY OF WATERLOO

- Automated Licence Plate Recognition Program for Parking Enforcement

ONTARIO ASSOCIATION OF SCHOOL BUSINESS OFFICIALS (OASBO)

- *Privacy Risks of Using Online Educational Services: What Educators Need to Know*

GLOBAL PRIVACY ENFORCEMENT NETWORK (GPEN)

- GPEN "Sweep"—International Study of "Internet of Things" (Accountability of Health-Related Devices)

MINISTRY OF COMMUNITY SAFETY AND CORRECTIONAL SERVICES

- *Police Record Checks Reform Act, 2015* Regulations
- Public Consultation—Strategy for a Safer Ontario

OTTAWA POLICE SERVICE

- Traffic Stop Race Data Collection Project
- Ottawa Police Service—John Howard Society Gang Exit Strategy Program, Time for Change

PROVINCIAL POLICE-HOSPITAL TRANSITION TASK FORCE

- *Improving Police-Hospital Transitions: A Framework for Ontario and Tools for Developing Police-Hospital Transition Protocols in Ontario*

TORONTO POLICE SERVICE

- Police and Community Engagement Review—PACER—Advisory Committee (Street Checks)
- Open Data Strategy

INTERNATIONAL WORKING GROUP ON DIGITAL EDUCATION

- Development of an International Competency Framework for Privacy Education

MINISTRY OF FINANCE

- Bill 70—*Building Ontario Up for Everyone Act* (Budget Measures), 2016—Amendments to the *Land Transfer Tax Act*

TREASURY BOARD SECRETARIAT

- *Broader Public Sector Executive Compensation Act*

PHIPA: A Prescription for Privacy

Important Amendments to Ontario's Health Privacy Law

In May 2016, the Ontario government passed Bill 119, the *Health Information Protection Act, 2016,* amending Ontario's health privacy law, the *Personal Health Information Protection Act* (*PHIPA*), in a number of ways. These amendments to *PHIPA* were developed in close consultation with our office to better protect patient privacy and improve accountability and transparency across Ontario's health sector.

One amendment doubles the maximum fines to $100,000 for individuals and $500,000 for organizations convicted of health privacy offences. Another amendment removes the six-month time limit for laying charges under *PHIPA*. The removal of this limit will allow more time for investigations into alleged privacy offences.

These amendments also bring in a new mandatory requirement for health information custodians (custodians) to report privacy breaches to the IPC. Previously, custodians were only required to notify patients affected by a privacy breach. Now, if a privacy breach meets a certain threshold (to be set out in *PHIPA*'s regulations), custodians must also notify our office about the breach. Custodians will also be required to notify health regulatory colleges where, among other things, they employed a member of a college who has been subject to disciplinary action due to an unauthorized collection, use, disclosure, retention or disposal of personal health information.

Not all provisions of Bill 119 are in force yet, including those that establish a privacy framework for the provincial electronic health record (EHR). When they come into force, these provisions will set rules for the collection, use and disclosure of personal health information within the provincial EHR. They will also allow individuals to withhold or withdraw their consent to the collection, use and disclosure of their information in the provincial EHR by custodians for health care purposes, subject to any limitations set out in *PHIPA*'s regulations.

The IPC will continue to consult with the Ministry of Health and Long-Term Care (MOHLTC) on the regulations that will give effect to Bill 119.

We strongly support these important amendments to *PHIPA* and believe they will increase accountability and enhance patient privacy for all Ontarians.

New Health Privacy Guidance: Communicating Personal Health Information by Email

In 2016, our office published a fact sheet on *Communicating Personal Health Information by Email*. This fact sheet provides practical guidance on how custodians can minimize the risk to privacy and ensure that they meet their obligations to protect their patients' personal health information. It outlines some of the technical, physical and administrative safeguards that custodians must have in place when they communicate by email with their patients or other custodians.

The IPC expects that email communication of health information among custodians will be encrypted, barring exceptional circumstances. When emailing personal health information between custodians and patients, custodians should use encryption, where feasible. If encryption is not feasible, custodians should determine whether it is reasonable to communicate with their patients through unencrypted email, considering the factors set out in the fact sheet. The fact sheet also describes some of the other obligations of custodians when they communicate personal health information by email, such as the requirement to have a written email policy, notify patients of this policy, and obtain patient consent prior to the use of unencrypted email.

SUMMARY OF PHIPA COMPLAINTS

+66% ACCESS/CORRECTION OPENED **2016 161** 2015 97	-2% INDIVIDUAL OPENED **2016 115** 2015 117	+31% SELF-REPORTED BREACH OPENED **2016 233** 2015 178	-59% IPC INITIATED OPENED **2016 28** 2015 68
+61% ACCESS/CORRECTION CLOSED **2015 135** 2015 84	+6% INDIVIDUAL CLOSED **2016 112** 2015 105	+6% SELF-REPORTED BREACH CLOSED **2016 186** 2015 175	-69% IPC INITIATED CLOSED **2016 21** 2015 68

Consultation on the Valuation of Ontario's Digital Health Assets

On October 7, 2016, the Minister of Health and Long-Term Care wrote an open letter to Ed Clark, Chair of the Advisory Council on Government Assets, to request that he review and assess the value of Ontario's digital health program. The IPC was pleased to consult with Mr. Clark on this initiative to ensure that the protection of personal health information was reflected in his recommendations to the ministry.

In our submission, we emphasized that a comprehensive privacy framework for a provincial EHR already exists in Ontario with the passage of Bill 119. We urged the government to proceed with proclamation of the Bill 119 amendments as soon as possible to ensure the harmonization of privacy standards across the province.

We also urged the government to exercise great caution prior to any consideration of monetizing Ontarians' personal health information in the provincial EHR. The government should consider who has custody and control of this information, and ensure that custodians de-identify it. We further noted that any movement towards monetizing this information, even when it is de-identified, may give rise to unintended consequences, such as individuals' withholding information that is needed to provide safe and effective health care.

Additionally, we stated that, should the government wish to proceed to de-identify Ontarians' personal health information for such purposes, broad public consultation

and a comprehensive legislated framework would be required. The IPC also stressed the need for secure digital technologies that will empower Ontarians to directly access their health information so that they can make important decisions about their health care.

Consultation on Bill 41, *Patients First Act, 2016*

In 2016, our office provided comments to the Ministry of Health and Long-Term Care based on our review of Bill 41 (the *Patients First Act, 2016*). These comments were included in a submission to the Standing Committee on the Legislative Assembly.

Bill 41 eliminates Ontario's Community Care Access Centres and transfers their functions to Ontario's Local Health Integration Networks (LHINs). It also gives LHINs an expanded role to oversee, and plan for, the delivery of health care at the regional level, and gives the ministry a similarly expanded role to oversee the operations of LHINs. To address the privacy implications of Bill 41, the IPC recommended amendments, including limiting the collection, use, and disclosure of Ontarians' personal health information by ministry and LHIN investigators and supervisors. The IPC believed that these amendments were straightforward, yet necessary, to ensure that the health information of Ontarians is properly protected from improper collection, use and disclosure.

We were pleased that our recommendations were adopted and are reflected in the final version of Bill 41.

Significant *PHIPA* Decisions

This year, our office published a number of *PHIPA* decisions that provide guidance to custodians and the public on their rights and obligations under Ontario's health privacy law. Below are summaries of some of these decisions.

PHIPA DECISIONS 19 AND 22

PHIPA permits, but does not require, a custodian to disclose the personal health information of a deceased individual to a surviving relative who reasonably requires this information to make knowledgeable decisions about their health care, or their children's health care.

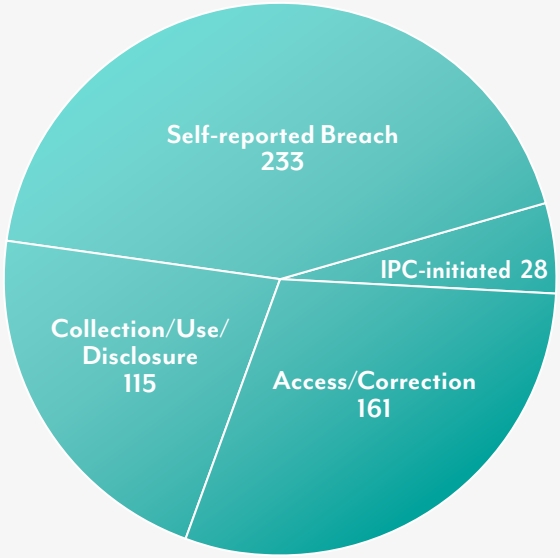
In *PHIPA* Decision 19, the complainant was a surviving relative of a deceased individual. The custodian denied the complainant's request to disclose a list of the names of medical practitioners who submitted OHIP claims related to his deceased family member. The complainant stated that he required this information to contact these practitioners to make decisions about his health care. The adjudicator agreed with the custodian's decision and found that the complainant did not establish that he reasonably required this information to make decisions about his health care.

In another decision on disclosure to a surviving relative, *PHIPA* Decision 22, the IPC concluded that the custodian had not adequately considered whether it should disclose information to a grieving daughter about her deceased mother, and directed the custodian to review her request for disclosure again.

PHIPA DECISION 26

PHIPA permits a custodian to charge fees for access to records of personal health information that do not exceed the amount of reasonable cost recovery. In *PHIPA* Decision 26, the IPC considered whether a fee charged by a custodian for a medical-legal report was a fee for making available a record of personal health information. The adjudicator found that the fee charged for this report was not a fee for making a record of personal health information available, but rather a fee the custodian charged for preparing the report. At the time the complainant made her request, this report did not exist. *PHIPA*'s requirements concerning right of access and

SUMMARY OF *PHIPA* COMPLAINTS OPENED



provisions regarding the fee for access did not apply to the creation of this report.

PHIPA DECISION 34

Generally, custodians are responsible for providing individuals with access to their personal health information, and may only refuse an access request in limited situations. One such situation is where access could reasonably be expected to result in a risk of serious harm to the treatment or recovery of the individual, or serious bodily harm to the individual or another person. In *PHIPA* Decision 34, a custodian denied the complainant's access request on this basis. In its representation to the IPC, the custodian submitted a psychiatrist's statement that supported its decision to deny access. The IPC upheld the custodian's access decision and noted that the custodian did not need to prove that disclosure would in fact result in a risk of serious bodily harm to the individual or others, as long as the evidence supports a reasonable expectation of harm.

PHIPA DECISION 36

Under *PHIPA*, an individual who believes that their record of personal health information is incomplete or inaccurate may ask the custodian who authored the record to correct it. While custodians must correct an incomplete or inaccurate record, they are not required to change professional opinions. In *PHIPA* Decision 36, the IPC upheld a custodian's decision not to make the corrections requested by the complainant. The adjudicator found that the complainant failed to establish that the record of personal health information was incomplete or inaccurate for the purpose for which it was used by the custodian, and that this information qualified as the custodian's professional opinion or observation.

PHIPA Cases Closed Through Early Resolution

In 2016 the IPC was pleased to resolve a number of *PHIPA* cases at the intake stage, or through mediation, without the need for the adjudication process. They included the following cases of note:

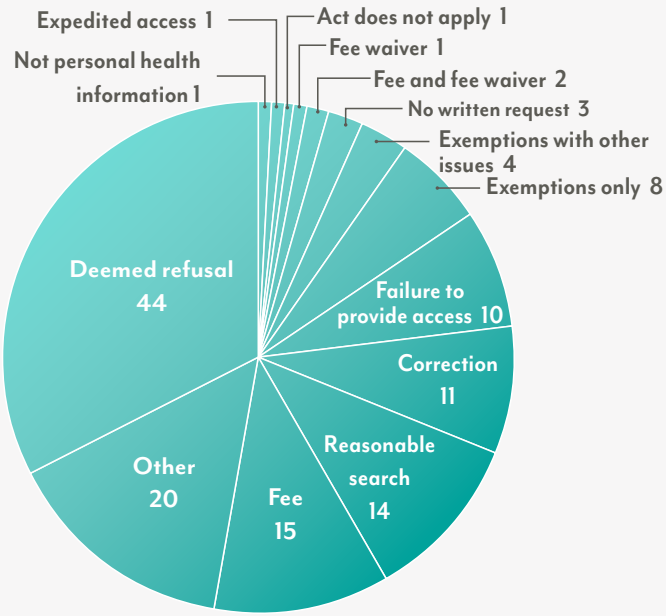
- An individual filed a complaint against a hospital, alleging that a doctor had inappropriately accessed and disclosed his personal health information during a court proceeding without his consent. The doctor was retained as an expert witness by the defence in the complainant's lawsuit, and referred to lab results that came from the complainant's admission to the hospital where the doctor had privileges. The doctor had accessed the complainant's electronic health records in the belief that they were duplicates of records he had received from the law firm that had retained him as an expert witness.

  The hospital's investigation concluded that the accesses were unauthorized. Both the hospital and the doctor participated in the mediation process with the complainant, and agreed to a number of steps, including apologizing to the complainant. The hospital

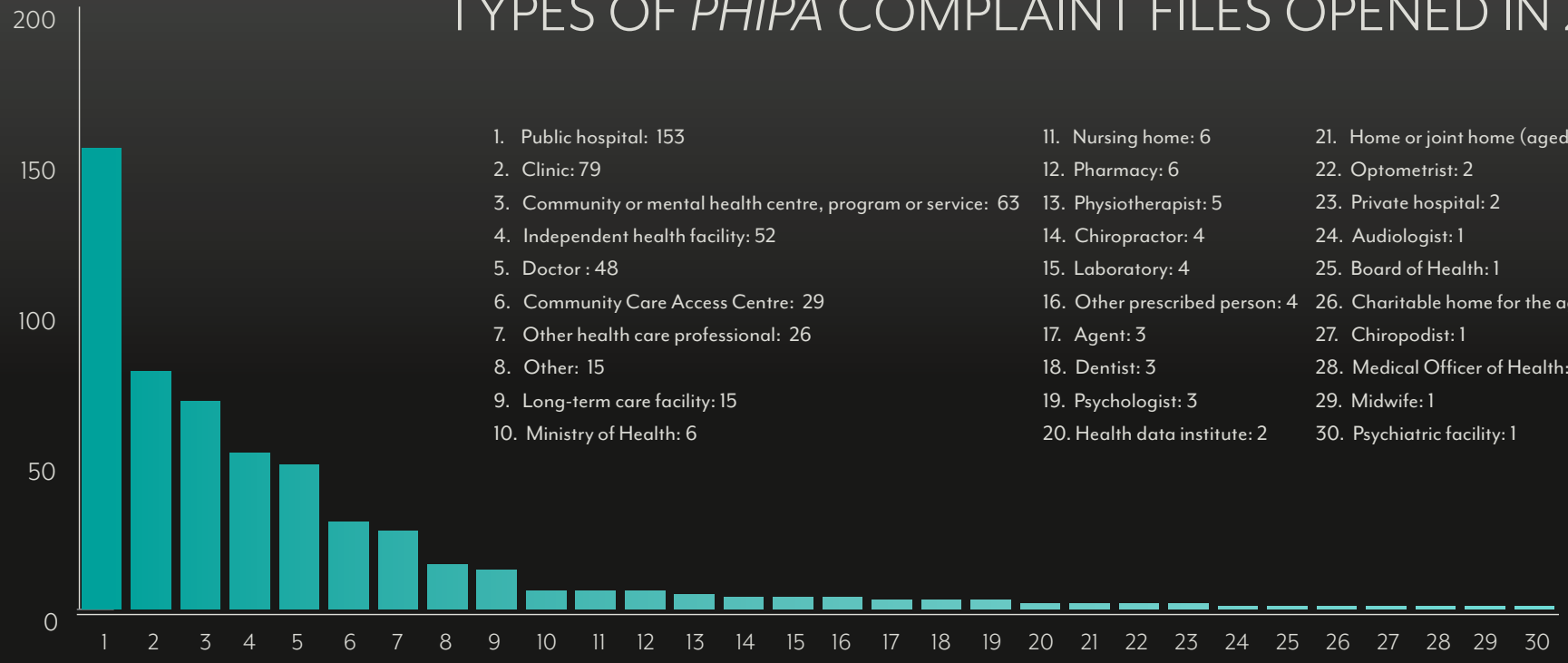
also agreed to issue two communications to physicians and clinicians to remind them of their privacy obligations when acting as an expert witness.

- A hospital denied an individual access to her records of personal health information on the basis that she was suffering from a disorder that would likely cause her to dispute the content of the records authored by her psychiatrist. During mediation, the hospital agreed to reconsider its decision and asked the psychiatrist for evidence to substantiate whether the disclosure of the records could reasonably be expected to result in a risk of serious harm to the treatment or recovery of the individual. In addition, the hospital asked the psychiatrist to consider whether any portions of the records could be severed with a view to provide access. As a result of this further review, the hospital revised its decision and granted the requester full access to her records.
- A treatment centre received an access request from a former patient and provided her with partial access to her health record. However, it denied her access to information that her parents provided to the centre during interviews, at which the requester was not present. The centre argued that it required the informed consent of family members before releasing the portions of the requester's record that contained family information. Following discussions with the mediator, the centre revised its decision and provided the complainant full access to her records.
- A regional hospital reported that some of its staff and agents had inappropriately accessed the personal health information of two patients. The unauthorized accesses were detected during a proactive audit of the hospital's electronic systems for high-profile patients. The hospital confirmed that its privacy practices included proactive audits, annual privacy training, annual re-signing of confidentiality agreements and privacy warning flags on its electronic systems. The IPC was satisfied with the steps taken by the hospital to contain the breach, notify the affected patients and prevent a future occurrence. This case was closed at the intake stage.
- A patient of a family physician complained that her personal health information had been inappropriately disclosed to a company hired by the physician to administer chronic disease education and management for her patients. The physician explained that the company was provided with limited patient information for the sole purpose of assisting with the provision of health care. The physician submitted that the use of the complainant's personal health information by the company was permitted under *PHIPA*. The IPC was satisfied that the company had been hired as an agent of the physician to provide chronic disease education and

ACCESS/CORRECTION COMPLAINTS CLOSED BY ISSUE



TYPES OF *PHIPA* COMPLAINT FILES OPENED IN 2016



1. Public hospital: 153
2. Clinic: 79
3. Community or mental health centre, program or service: 63
4. Independent health facility: 52
5. Doctor : 48
6. Community Care Access Centre: 29
7. Other health care professional: 26
8. Other: 15
9. Long-term care facility: 15
10. Ministry of Health: 6
11. Nursing home: 6
12. Pharmacy: 6
13. Physiotherapist: 5
14. Chiropractor: 4
15. Laboratory: 4
16. Other prescribed person: 4
17. Agent: 3
18. Dentist: 3
19. Psychologist: 3
20. Health data institute: 2
21. Home or joint home (aged or rest): 2
22. Optometrist: 2
23. Private hospital: 2
24. Audiologist: 1
25. Board of Health: 1
26. Charitable home for the aged: 1
27. Chiropodist: 1
28. Medical Officer of Health: 1
29. Midwife: 1
30. Psychiatric facility: 1

management, and was permitted to use the complainant's personal health information for that purpose.

- Another case closed at the intake stage involved an individual who complained that a hospital provided details of her pregnancy to her children's aid society (CAS) caseworker. The caseworker had requested that the hospital notify them should the complainant present at the hospital for delivery or postnatal care. The hospital relied on a duty to report child protection concerns to the CAS under the *Child and Family Services Act*. The IPC found in the circumstances of this complaint that *PHIPA* permitted the hospital to disclose the complainant's personal health information to the CAS without the consent of the complainant.

Commissioner's Recommendations

The growing use of technology presents complex challenges for Ontario's public institutions. Similarly, the IPC is put to the test as we strive to regulate its use within a 30-year old legislative framework. Our access and privacy laws have become outdated and inadequate in the face of newer and more sophisticated data regimes. Once again, I am calling on the Ontario government to undertake an open, public consultation to review *FIPPA* and *MFIPPA*. We must update the acts and ensure that the access and privacy rights of Ontarians continue to be protected as government processes evolve.

Provide a Legislated Framework for Data Integration

Ontario's access and privacy laws were drafted decades ago—long before the proliferation of and advancements in information technology we now take for granted had come to pass. At that time, the needs and expectations surrounding government processing of personal information were different: technology was less prevalent, the types of data were less complex and uses were discrete and determinate. The result was a model of data protection where government institutions were treated as "silos." Now, with the growing amount of information available to government, and the sophisticated analytic tools available to policy makers, Ontario's public sector institutions are increasingly looking at data integration to enable better policy and program development, system planning, resource allocation and performance monitoring.

While we support the goals of evidence-based decision making and efficient public services, personal privacy must continue to be safeguarded. The IPC is calling on government to enact legislation that expressly authorizes information sharing for policy and research purposes and provides a strong, government-wide framework for data integration projects. This would include measures to manage the privacy risks of information sharing, data linking and the use of data for analytical studies, including a robust de-identification process. Further, any legislative changes that support greater data integration and information sharing among institutions should be accompanied by effective governance and oversight. Measures that could be incorporated into existing legislation include:

- additional investigation, order-making and audit powers for the IPC
- mandatory breach notification and reporting
- requirements for privacy impact assessments
- requirements for de-identification
- review and approval by an ethics review body
- public notification of data integration projects
- rights of individuals affected by automated decision making

Confirm Commissioner's Power to Compel the Production of Records

For more than 25 years, Ontario's public institutions and the IPC have operated under the understanding that the IPC has the power to compel production of records in order to verify claims of exemption under solicitor-client privilege. A recent decision of the Supreme Court of Canada that considered the Alberta

Information and Privacy Commissioner's statutory power to compel production has led some public institutions to question the IPC's ability to compel the production of records for which privilege is claimed. Currently, under *FIPPA*, the IPC may examine records despite "any...Act or privilege." We recommend amendments to Ontario's access laws that affirm the power of the IPC to access documents for which institutions claim the solicitor-client privilege exemption and clarify that providing records to the IPC does not constitute a waiver of solicitor-client privilege. This will ensure that the ability of my office to adjudicate the solicitor-client privilege exemption is not undermined.

Proclaim Further Amendments to Bill 119

In September 2015, the Minister of Health and Long-Term Care introduced Bill 119, the *Health Information Protection Act*. Among other things, this bill amended *PHIPA* to include a requirement for custodians to report certain privacy breaches to our office and a requirement to notify regulatory colleges in specific circumstances. This bill also doubled the fines that could be imposed for unauthorized access to patient records. The bulk of the bill related to creating a legislated governance framework for the shared provincial electronic health record (EHR).

Bill 119 was passed in May 2016 with many of its provisions proclaimed in June 2016. However, those provisions of the bill relating to the shared provincial EHR have yet to be proclaimed, and are essential for ensuring that an effective governance framework is in place. As the health sector transitions from paper-based records and stand-alone electronic medical records to a shared provincial EHR, a legislated governance framework is necessary to ensure patient privacy and the protection of personal health information.

I urge the government to promptly move forward with proclamation of these provisions.

Increased Transparency of Ontario's Medical System

Bill 84, the *Medical Assistance in Dying Statute Law Amendment Act* proposed to exclude certain information from *FIPPA* and *MFIPPA*, including information that could identify facilities that provide services relating to medical assistance in dying. We believe that excluding information that could identify facilities providing such services is inconsistent with Ontario's access and privacy laws and would hinder the transparency and accountability of Ontario's health system.

Despite our recommendation, the government did not amend Bill 84 to make this information accessible under freedom of information legislation. I therefore strongly urge Ontario's health institutions to disclose whether or not they provide these services. Ontarians should have the right to know what facilities are providing publicly funded services, including those relating to medical assistance in dying.

Public Disclosure of Health Privacy Breach Prosecutions

Recent changes to Ontario's health privacy laws have doubled the fines that may be imposed on

individuals and organizations for unauthorized access to personal health information. The province has successfully prosecuted several individuals for offences under *PHIPA*, resulting in significant fines. However, the province does not proactively publish the details of prosecutions under *PHIPA*. For these prosecutions to achieve the desired effect of deterring unauthorized access, they need to be made public. I recommend that the government adopt the practice of making the details of these prosecutions public to send a strong message that unauthorized access to personal health information will not be tolerated.

Abandoned Records

Since the *Personal Health Information Protection Act* (*PHIPA*) came into effect, our office has investigated numerous instances of abandoned health records. This typically happens when a health information custodian relocates, retires, becomes incapacitated or otherwise ceases to practice.

Despite duties set out in current legislation, guidance provided by regulatory health colleges, and our office issuing both orders and educational materials, abandoned health records remain an issue in this province. Abandoned records pose a significant risk to the privacy of patients and their ability to access their records. In addition, if health records are unavailable to heath care providers, it may affect the delivery of effective care.

Over the past year, our office has researched the issue of abandoned records and how it is addressed across Canada. Some regulatory health colleges have included in their codes of conduct the requirement for members to notify the college before they leave or move their practice and to name a successor. These codes also cite abandoning records as an act of professional misconduct. Some jurisdictions have supplemented the initiatives of regulatory health colleges with amendments to legislation. These jurisdictions have provided either the

minister of health or the regulatory health colleges with the authority to appoint a person to act in the place of a former custodian who has abandoned health records, and have made it an offence to abandon records.

In our 2009 Annual Report, we urged the ministry to engage in consultations with relevant stakeholders with a view to providing a comprehensive legislative framework to ensure that health records are properly secured when a custodian ceases to practice and that those records are available to patients on request. I repeat that call today. Several jurisdictions in

Canada have, since I last addressed this issue, taken action which includes legislation that assigns responsibility for abandoned health records. I strongly encourage the ministry to engage in consultation with stakeholders, specifically the regulatory health colleges, to determine the appropriate combination of actions that will best address the issue of abandoned records in Ontario. I recommend a multi-prong approach involving changes to the codes of conduct and policies of regulatory health colleges, increased education and guidance for custodians, and amendments to legislation to ensure there is authority for either the Minister of Health and Long-Term Care or regulatory health colleges to appoint a custodian to take possession of abandoned records and that it is an offence to abandon records of personal health information.

Submission of False Compliance Statistics

After the release of the 2015 IPC annual report, I was alerted by the Ministry of the Environment and Climate Change to concerns with the accuracy of the compliance statistics the ministry had submitted to my office.

In December 2016 I received a full freedom of information audit report, together with a summary of the revised FOI compliance statistics for 2010 to 2015. Government auditors concluded that the dates in the ministry's request tracking system had been systematically adjusted by staff in the FOI office in order to show completion of requests within the 30-day requirement.

The public's right to access government-held information forms an important part of a democracy and reflects an open and transparent government. As such, Ontario's provincial and municipal access laws place important responsibilities on freedom of information staff. Ontarians expect—and deserve—to know that these duties are being carried out in an open and ethical manner. The falsifying of statistics is a serious issue, and can erode the trust and confidence of Ontarians who should be able to rely on the accuracy of these statistics.

I am pleased that appropriate corrective action was taken at MOECC, and that the government agreed, at my request, to conduct audits on five other ministries to assess whether the issues that arose at MOECC were widespread. However, since the results of the audit revealed areas of non-compliance with *FIPPA* at three other ministries, I am concerned that compliance with Ontario's access laws, and the accuracy of statistics submitted to my office, remains an issue that must be addressed as part of an ongoing assessment and auditing process. I strongly recommend that all Ontario institutions—municipal and provincial—routinely conduct spot audits of their FOI offices, review their practices, and establish regular training programs to help staff understand their responsibility to apply consistent and correct practices to managing access requests.

I also expect the government to implement the recommendations of the Ontario Internal Audit Division in its spot audit report.

In the past, my office has relied on the integrity of the statistics submitted by each government ministry's FOI office. Based on this experience, I would like to see a higher level of accountability for the veracity of these numbers. In future, it is my expectation that 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.

My office continues to work with members of the broader Ontario Public Service to provide guidance and support as they ensure their compliance with Ontario's access laws.

I look forward to seeing these recommendations implemented. My office is ready to assist in any way we can. By listening to each other and working together, we can make sure our access and privacy rights remain relevant and effective well into the future.

YEAR AT A GLANCE

PROVINCIAL

PERSONAL INFORMATION	GENERAL RECORDS	TOTAL
+13% REQUESTS **2016 8,294** 2015 7,367	-2% REQUESTS **2016 15,319** 2015 15,584	+3% TOTAL REQUESTS **2016 23,613** 2015 22,951
+1% APPEALS OPENED **2016 181** 2015 179	+4% APPEALS OPENED **2016 555** 2015 536	+3% TOTAL APPEALS OPENED **2016 736** 2015 715
-8% APPEALS CLOSED **2016 172** 2015 186	0% APPEALS CLOSED **2016 505** 2015 506	-2% TOTAL APPEALS CLOSED **2016 677** 2015 692
+4% AVERAGE COST **2016 $13.86** 2015 $13.37	-0.1% AVERAGE COST **2016 $38.60** 2015 $38.67	

MUNICIPAL

PERSONAL INFORMATION	GENERAL RECORDS	TOTAL
+1% REQUESTS **2016 18,743** 2015 18,492	+5% REQUESTS **2016 19,231** 2015 18,367	+3% TOTAL REQUESTS **2016 37,974** 2015 36,859
0% APPEALS OPENED **2016 209** 2015 210	+26% APPEALS OPENED **2016 603** 2015 478	+18% TOTAL APPEALS OPENED **2016 812** 2015 688
-8% APPEALS CLOSED **2016 193** 2015 209	+24% APPEALS CLOSED **2016 530** 2015 428	+14% TOTAL APPEALS CLOSED **2016 723** 2015 637
+13% AVERAGE COST **2016 $10.75** 2015 $9.49	-4% AVERAGE COST **2016 $24.66** 2015 $25.69	

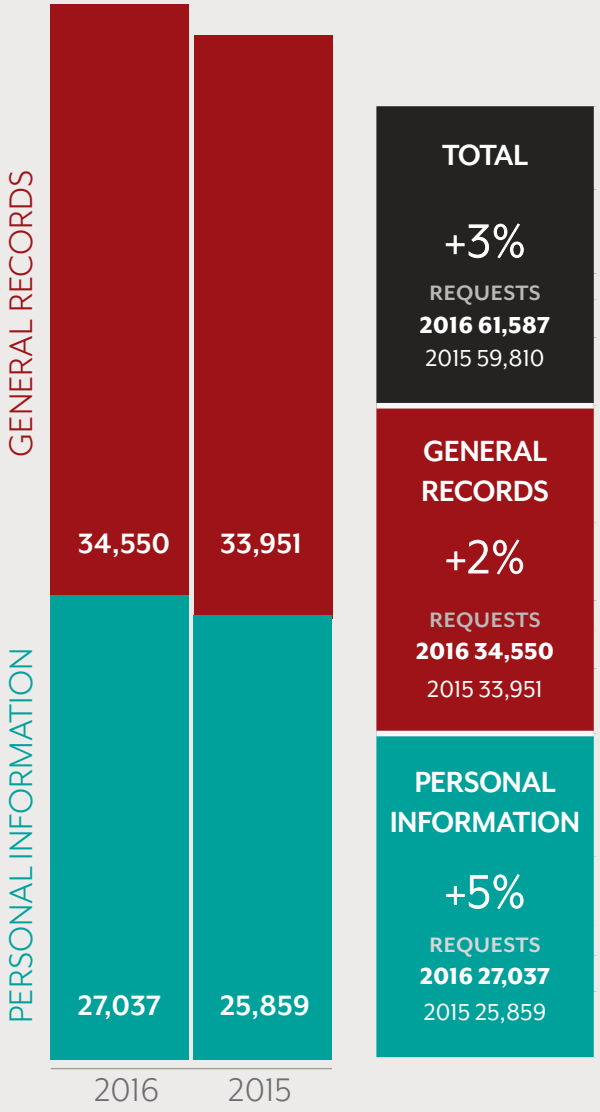
PRIVACY COMPLAINTS

PROVINCIAL	MUNICIPAL
+8% OPENED **2016 118** 2015 109	-5% OPENED **2016 159** 2015 167
-5% CLOSED **2016 103** 2015 108	-6% CLOSED **2016 153** 2015 163

SUMMARY OF *PHIPA* COMPLAINTS

+66% ACCESS/CORRECTION OPENED **2016 161** 2015 97	+61% ACCESS/CORRECTION CLOSED **2016 135** 2015 84	-2% INDIVIDUAL OPENED **2016 115** 2015 117	+6% INDIVIDUAL CLOSED **2016 112** 2015 105	+31% SELF-REPORTED BREACH OPENED **2016 233** 2015 178	+6% SELF-REPORTED BREACH CLOSED **2016 186** 2015 175	-59% IPC INITIATED OPENED **2016 28** 2015 68	-69% IPC INITIATED CLOSED **2016 21** 2015 68

OVERALL REQUESTS



TOTAL

+3%

REQUESTS
2016 61,587
2015 59,810

GENERAL RECORDS

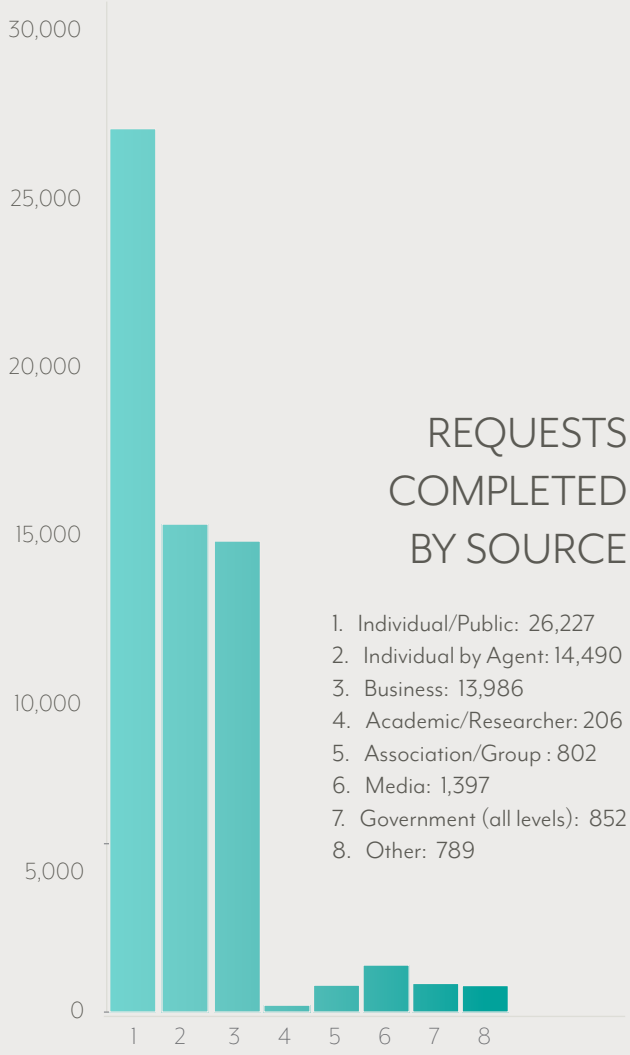
+2%

REQUESTS
2016 34,550
2015 33,951

PERSONAL INFORMATION

+5%

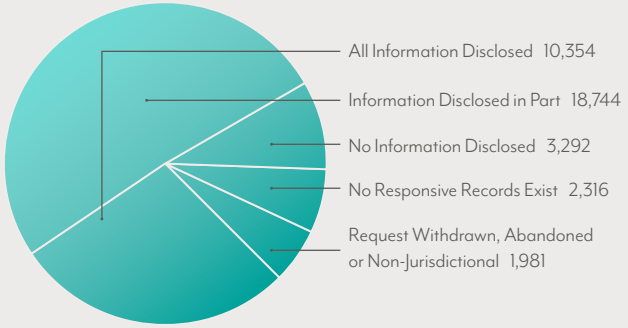
REQUESTS
2016 27,037
2015 25,859



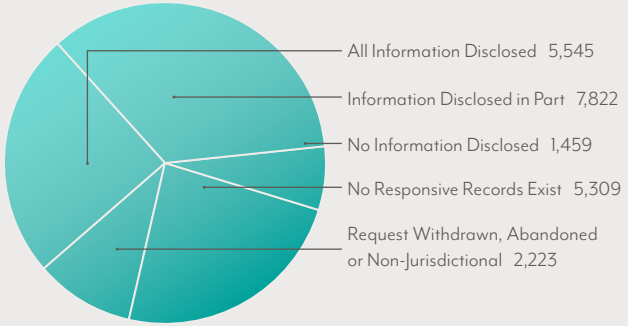
REQUESTS COMPLETED BY SOURCE

1. Individual/Public: 26,227
2. Individual by Agent: 14,490
3. Business: 13,986
4. Academic/Researcher: 206
5. Association/Group : 802
6. Media: 1,397
7. Government (all levels): 852
8. Other: 789

OUTCOME OF REQUESTS: MUNICIPAL



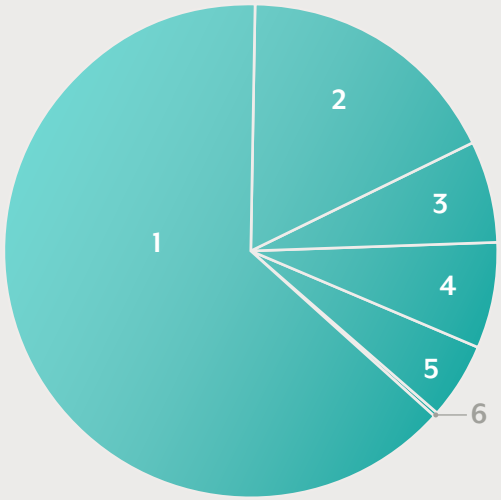
OUTCOME OF REQUESTS: PROVINCIAL



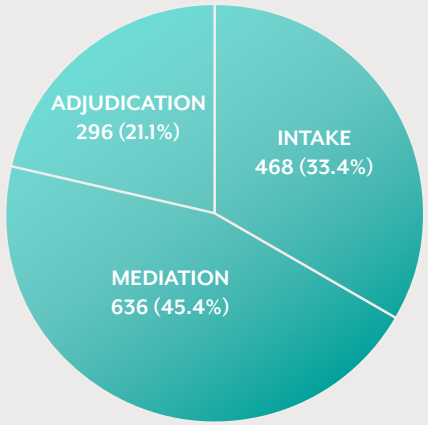
NUMBER OF MUNICIPAL APPEALS OPENED 2007-2016

NUMBER OF PROVINCIAL APPEALS OPENED 2007-2016

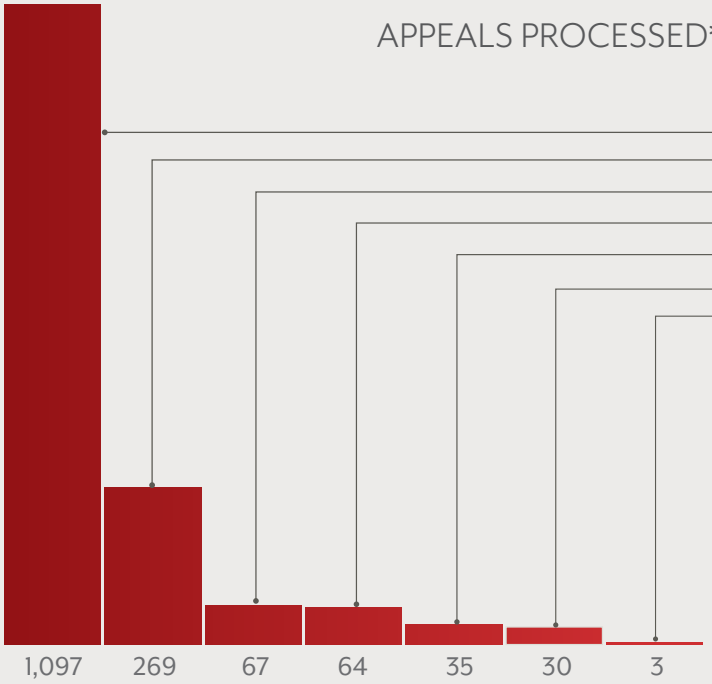
OUTCOME OF APPEALS BY STAGE CLOSED



1. **Mediated in full: 893 (63.8%)**
2. **Order issued: 246 (17.6%)**
3. **Withdrawn: 91 (6.5%)**
4. **Screened out: 97 (6.9%)**
5. **Abandoned: 71 (5.1%)**
6. **Dismissed without Inquiry/ Review/Order: 2 (0.1%)**

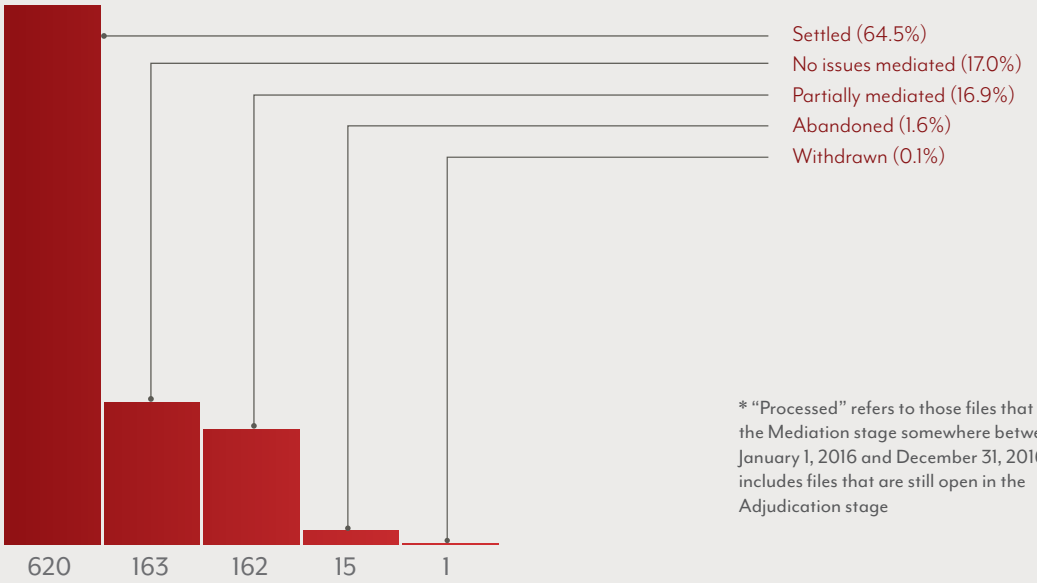


APPEALS PROCESSED* IN INTAKE BY DISPOSITION



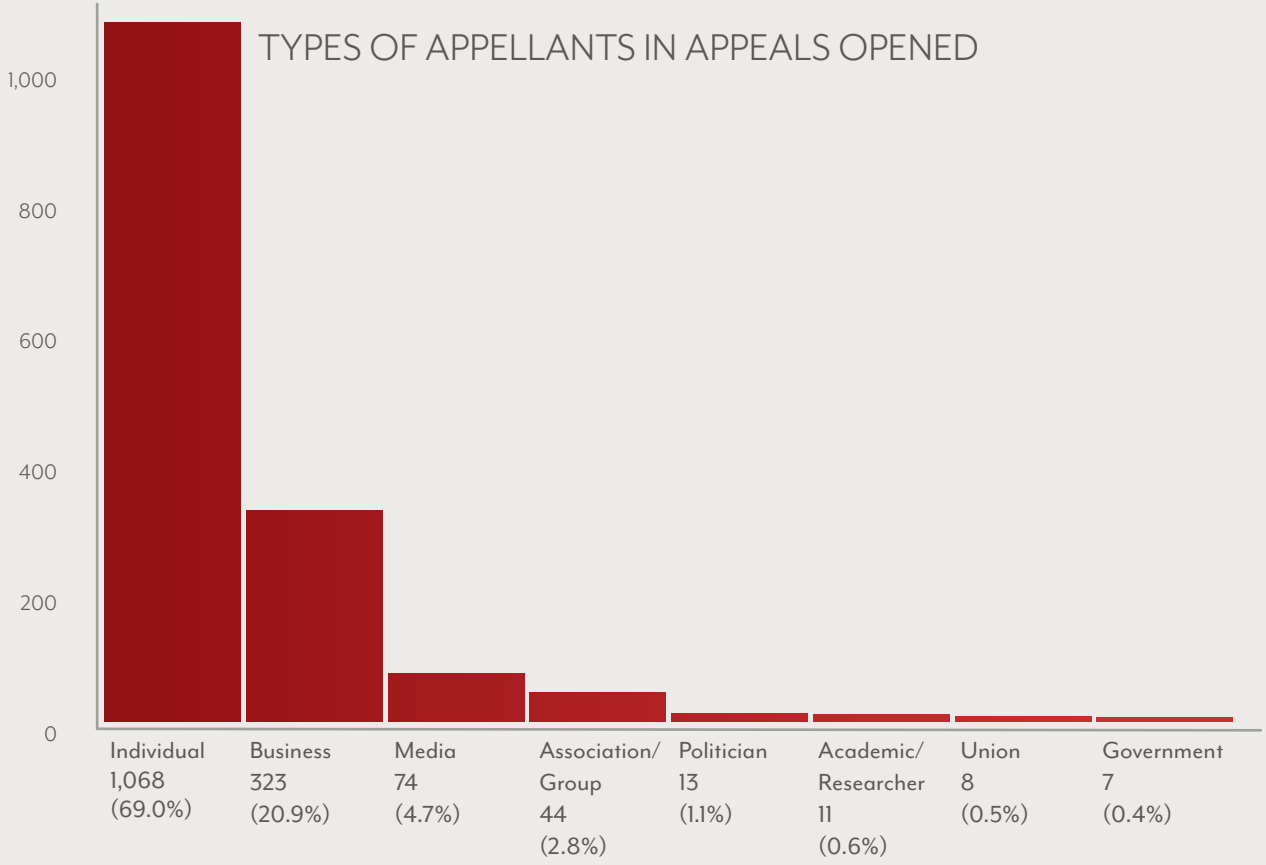
*"Processed" refers to those files that completed the Intake stage somewhere between January 1, 2016 and December 31, 2016 and includes files that are still open in the Mediation and Adjudication stages

APPEALS PROCESSED* IN MEDIATION BY DISPOSITION

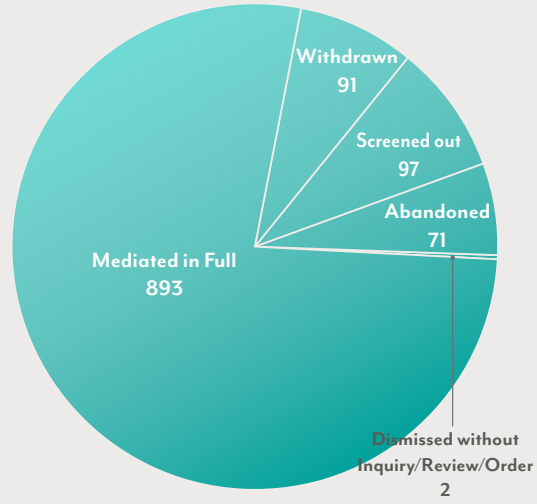


* "Processed" refers to those files that completed the Mediation stage somewhere between January 1, 2016 and December 31, 2016 and includes files that are still open in the Adjudication stage

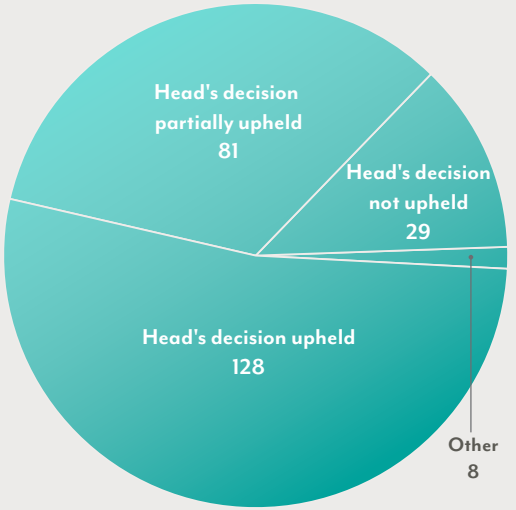
TYPES OF APPELLANTS IN APPEALS OPENED



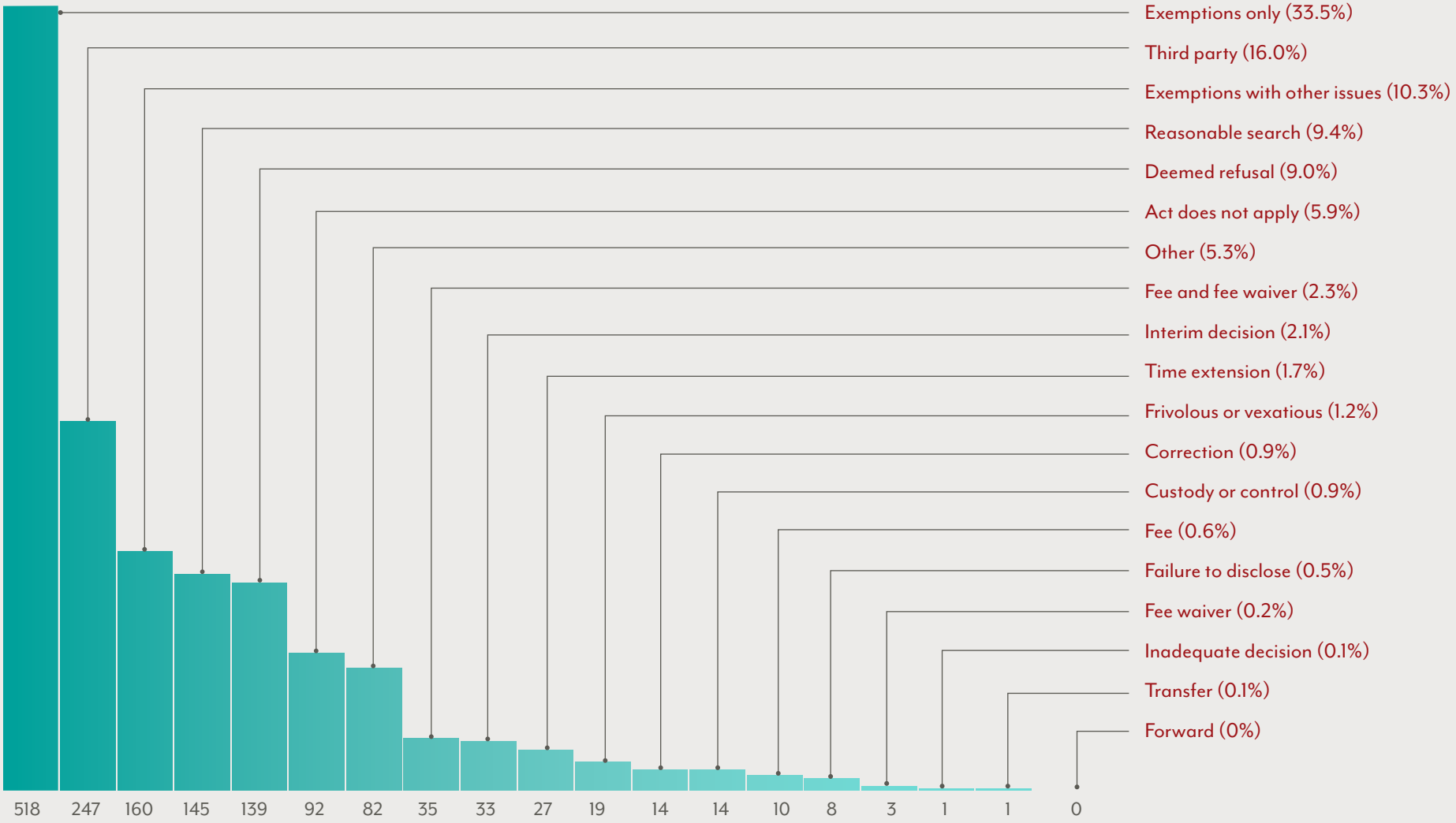
NUMBER OF APPEALS CLOSED OTHER THAN BY ORDER, BY OUTCOME



NUMBER OF APPEALS CLOSED BY ORDER, BY ORDER OUTCOME

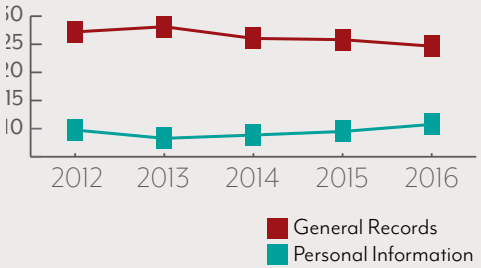


ISSUES IN APPEALS OPENED



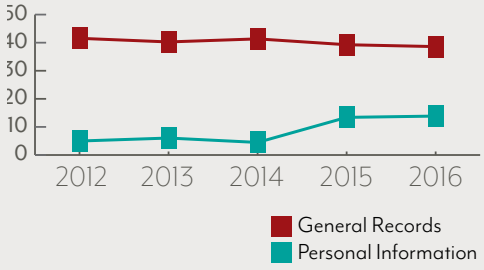
AVG COST OF MUNICIPAL REQUESTS

PERSONAL INFORMATION	GENERAL RECORDS
$10.75	$24.66
2016	2016



AVG COST OF PROVINCIAL REQUESTS

PERSONAL INFORMATION	GENERAL RECORDS
$13.86	$38.60
2016	2016



TOTAL FEES COLLECTED AND WAIVED

MUNICIPAL	PROVINCIAL	TOTAL
$178,876.45 TOTAL APPLICATION FEES COLLECTED 2016	$117,952.05 TOTAL APPLICATION FEES COLLECTED 2016	$296,828.50 TOTAL APPLICATION FEES COLLECTED 2016
$474,483.58 TOTAL ADDITIONAL FEES COLLECTED 2016	$541,622.88 TOTAL ADDITIONAL FEES COLLECTED 2016	$1,016,106.46 TOTAL ADDITIONAL FEES COLLECTED 2016
$653,360.03 TOTAL 2016	$659,574.93 TOTAL 2016	$1,312,934.96 TOTAL 2016
$40,002.43 TOTAL FEES WAIVED 2016	$17,454.30 TOTAL FEES WAIVED 2016	$57,456.73 TOTAL FEES WAIVED 2016

FINANCIAL STATEMENT

	2016-2017 BUDGET $	2015-2016 BUDGET $	2015-2016 ACTUAL $
SALARIES AND WAGES	10,444,100	10,444,100	9,394,705
EMPLOYEE BENEFITS	2,401,900	2,401,900	1,904,065
TRANSPORTATION AND COMMUNICATIONS	337,500	337,500	184,908
SERVICES	1,960,300	1,960,300	2,050,757
SUPPLIES AND EQUIPMENT	336,000	336,000	474,346
TOTAL	**15,479,800**	**15,479,800**	**14,008,781**

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.

2016 Appeals Fees Deposit

(Calendar year)

GENERAL INFO.	PERSONAL INFO.	TOTAL
$18,149	**$3,320**	**$21,469**

HOW TO REACH US

Information and Privacy Commissioner of Ontario
2, Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Toronto area: 416-326-3333
Long distance: 1-800-387-0073 within Ontario
TDD/TTY: 416-325-7539

www.ipc.on.ca
info@ipc.on.ca