2018
ANNUAL REPORT

Office of the Information
and Privacy Commissioner
of Ontario

Privacy and Accountability for a Digital Ontario

Information and Privacy
Commissioner of Ontario

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

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

June 27, 2019

The Honourable Ted Arnott

Speaker of the Legislative Assembly of Ontario

Dear Speaker,

I have the honour to present the 2018 Annual Report for the Information and Privacy Commissioner of Ontario to the Legislative Assembly of Ontario. The enclosed report covers the period from January 1 to December 31, 2018.

A full report, along with statistics and supporting documents can be found online at www.ipc.on.ca/about-us/annual-reports/.

Sincerely yours,

Brian Beamish
Commissioner

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

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

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

CONTENTS

CONTENTS

Commissioner's Message

Commissioner's Message

As 2018 began, my office anticipated a busy year ahead. Alongside our work resolving appeals and complaints, we planned for projects and initiatives to support our mandate of advancing the access to information and personal privacy rights of Ontarians.

Throughout the year, these projects included consultations with institutions and health information custodians on policy and compliance issues, advice to government on new legislation, amendments and new programs, and engagement with public service sectors that, for the first time, will be subject to access and privacy laws.

Our work this year culminated in some noteworthy wins for access and privacy rights in Ontario. I am pleased to share an overview of the significant developments that shaped our efforts, along with specific issues that marked 2018.

Doctors' billings

If you follow the work of my office, you will know about the chronicles of Order PO-3617. This case began in 2014 when the Toronto Star made a request to the Ministry of Health and Long-Term Care for access to information on the top 100 OHIP billers. The ministry denied access to this information. The newspaper appealed to the IPC, resulting in a groundbreaking order where the adjudicator departed from previous rulings about what constitutes personal information of physicians. He ordered the ministry to disclose information relating to physician billings.

The reasoning in the IPC's order centred on the public's right to know how tax dollars are spent. The Ontario Medical Association has twice contested this order — first before the Ontario Divisional Court, then in early 2018, on appeal to the province's Court of Appeal — and both times, the IPC's decision was upheld, affirming the adjudicator's position that a physician's name and OHIP billing is not personal information and should be disclosed.

In 2018, the OMA and two doctors' groups served a joint application for leave to appeal to the Supreme Court of Canada, which the court dismissed in April 2019.

I am proud of the work of adjudicator John Higgins and our legal team for taking on this challenge, resulting in a "win" for openness and transparency.

Algoma Public Health report on allegations of wrongdoing

Also in April, the Ontario Court of Appeal affirmed the IPC's decision in Order MO-3295 that the compelling public interest in allegations of wrongdoing outweighs the personal privacy of senior public officials.

In response to an access request, Algoma Public Health decided to release a report on a potential conflict of interest in the appointment of APH's former interim chief financial officer, and whether any funds were misappropriated or lost. A former senior official appealed APH's decision to my office, claiming the personal privacy exemption and stating that the public interest override did not apply.

After the Divisional Court overturned the IPC's order, the case went to Ontario's Court of Appeal. The appeal was heard at the end of 2018, and in April 2019, the court upheld Order MO-3295.

PHIPA breach reporting

The requirement to report *PHIPA* health privacy breaches to the IPC began in late 2017, ushering

in a new era of accountability and transparency in Ontario's health care sector. As expected, this led to a significant increase in the number of files my office handles in the health sector.

I am happy to report that IPC staff met this new challenge with professionalism and enthusiasm, responding to the hundreds of calls, breach reports, investigations and other issues resulting from this legislative amendment.

This year also marked the first year that health information custodians were required to submit health privacy breach statistics to my office. Ontario's health sector responded with a clear commitment to accountability and protection of patient privacy. As illustrated by our 2018 statistical report, hundreds of custodians across Ontario, including hospitals, pharmacies, doctors' offices, dental clinics and many others, submitted their statistics for 2018, as is now required by law.

I want to take this opportunity to thank my staff — and custodians — for taking on these responsibilities in earnest, and to commend them for their ongoing commitment to upholding the privacy rights of Ontarians.

Data integration

In my 2017 annual report recommendations, I urged the government to enact legislation that provides a strong and consistent framework for data integration. In 2018, we welcomed the opportunity to consult with the Ministry of Government and Consumer Services, the Ministry of Finance and Cabinet Office. Our consultations focused on the need to establish a government-wide solution for data integration. Such a solution would enable data linkages to support effective system planning, analysis, and evaluation while protecting personal privacy.

Our work in this area led us to raise concerns about other legislation, such as the proposed *Community Safety and Policing Act* and *Correctional Services and Reintegration Act*, and the new *Child, Youth and Family Services Act*, each with its own data integration framework and inconsistent privacy protections.

We cautioned the government that a fragmented approach to data integration could result in a proliferation of linked databases containing the same or similar information. We also suggested that a unified approach, with consistent privacy protection measures, would lower the risk of breaches.

From this, in 2018 we recommended a coherent, legislative approach to data integration with comprehensive privacy protections, and were pleased to see these legislative amendments introduced at the same time as the 2019 Ontario Budget.

Access and privacy protection for children and families

In April 2018, the *Child, Youth and Family Services Act* became law in Ontario, setting a legislative framework for privacy in the child and family services sector. The IPC's mandate will expand when Part X (ten) of the *CYFSA* comes into force on January 1, 2020. Less than a year from now, children, youth and families will have the right to access and request correction of their personal information held by children's aid societies and other service providers. They will also have the right to file complaints with my office.

To prepare for this milestone, the IPC worked with the Ministry of Children, Community and Social Services (formerly the Ministry of Children and Youth Services) throughout 2018 on public awareness and engagement efforts tailored to those most affected by the new law, including young people and service providers. We will continue this work as we welcome long-awaited access and privacy rights for children, youth and families. Look for Part X updates on our website in the coming months.

A lesson in privacy

In 2018, the IPC intervened in a case before the Supreme Court of Canada. The issue related to whether a teacher's secret video recordings of female

students' chests and cleavage were made in a situation where the students would have a reasonable expectation of privacy.

The IPC argued that there are no "privacy-free zones" even in common areas, where video surveillance cameras are in use.

I was pleased that, consistent with the IPC's submissions, the SCC found that the students' expectation of privacy exists even when they are in areas subject to video surveillance, and subsequently convicted the teacher of voyeurism. I want to congratulate my legal team for their efforts in making Ontario a safer place, particularly for young people who can be vulnerable to predatory and invasive behaviour.

Final thoughts

As we continue to make progress and confront the challenges of the coming year, I want to thank my staff for the commitment and integrity they show every day. Their strong belief in the rights of all Ontarians to privacy and access to information is at the core of our work and drives our success.

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 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 Work

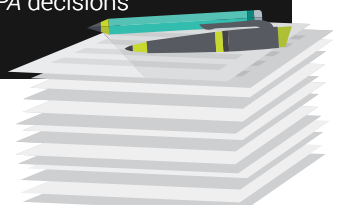
COMMISSIONER

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

In 2018, the IPC was mentioned more than 100 times in the media and made 100 presentations to stakeholders and public audiences.

TRIBUNAL

- 1,442 access appeals received
- 1,431 access appeals closed
- 286 orders issued
- 306 privacy complaints received
- 273 privacy complaints closed
- 870 health complaints received
- 727 health complaints closed
- 15 *PHIPA* decisions issued



INTAKE
383 access appeals resolved
246 privacy complaints closed
667 *PHIPA* complaints closed

INVESTIGATION AND MEDIATION
723 access to information appeals resolved
11 privacy complaints resolved
47 *PHIPA* complaints/breaches resolved

ADJUDICATION
325 access appeals resolved
245 access decisions issued
13 *PHIPA* complaints resolved

LEGAL

- 28 presentations
- represented the commissioner in seven court hearings, including as an intervenor in a case before the Supreme Court of Canada

POLICY

- released 11 guidance documents, fact sheets and reports
- consulted with and provided advice to over 40 organizations
- 17 presentations on privacy and access issues

HEALTH POLICY

- collaborated on five publications
- helped develop amendments to health privacy legislation
- consulted with and presented to over 25 organizations

COMMUNICATIONS

- fielded more than 90 media calls
- produced two webinars
- planned two major events that attracted more than 800 people (in person and via webcast)
- responded to thousands of calls and emails from the public
- Reaching Out to Ontario visits to Hamilton and Barrie
- Right to Know Week

CORPORATE SERVICES AND TECHNOLOGY

Oversees organizational operations such as:

- human resources
- monitoring expenditures
- technical support
- IT support

ABOUT US

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

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

The *Personal Health Information Protection Act* 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.

The *Child, Youth and Family Services Act* came into force on April 30, 2018. Part X of this law will come into force on January 1, 2020, and will mark the first time Ontarians will have the right to access their personal information held by children's aid societies and other service providers and to file privacy complaints.

The *Anti-Racism Act* came into force on June 1, 2017. It applies to public sector organizations including ministries, municipalities, school boards, universities and colleges, and correctional institutions, and their use of race-based data.

Top 10 provincial institutions

	REQUESTS RECEIVED	NUMBER OF APPEALS
Ministry of the Environment, Conservation and Parks	8,492	24
Ministry of the Solicitor General	5,496	136
Ministry of Children, Community and Social Services	3,187	21
Ministry of Labour	915	11
Landlord and Tenant Board	680	2
Ministry of Government and Consumer Services	484	9
Ministry of Transportation	420	16
Ministry of the Attorney General	394	28
Ministry of Health and Long-Term Care	267	38
Workplace Safety and Insurance Board	221	18

Access to Information

Openness is essential to democracy. The public has a right to know how the government makes decisions and spends public funds. Access to government-held information is fundamental to ensuring this transparency. During the past year, our office upheld the public's right to know through work aimed at increasing access to information and encouraging institutions to be as transparent as possible about their activities.

In 2018, institutions covered by Ontario's access and privacy laws completed 58,812 access to information requests. More than 75 per cent of the institutions' responses met the 30-day compliance standards set by Ontario's access laws. The number shows a marked improvement over the compliance rates of two decades ago, which were under 50 per cent. Compliance rates started to rise when the IPC began publishing statistics in our annual report.

This year our annual report includes a side-by-side analysis of the number of access appeals to our office for the ten provincial and municipal institutions with the largest volume of requests. In Ontario, only 2.4 per cent of all FOI requests resulted in appeals to the IPC, demonstrating a commendable commitment by institutions to living up to the intent of our access laws.

Access to tribunal records

On the legislative front, the IPC supported the development of new legislation to improve public access to tribunal records. Our office participated in the government's consultation on new access and confidentiality rules for tribunal records consistent with open court principles. The substance of our advice balanced the principles of upholding the public's right to know and protecting individual privacy and other confidentiality interests.

Services to children, youth and families

Changes to services for children and youth were set in motion when the government introduced the new *Child, Youth and Family Services Act*. In April, the CYFSA became law in Ontario.

Top 10 municipal institutions

	REQUESTS RECEIVED	NUMBER OF APPEALS
Toronto Police Service	5,048	95
City of Toronto	2,904	54
York Regional Police	1,589	21
Durham Regional Police Service	1,458	14
Peel Regional Police	1,386	26
Hamilton Police Service	1,358	18
Niagara Regional Police Service	1,295	9
Halton Regional Police Service	1,187	23
Waterloo Regional Police Service	1,138	15
London Police Service	1,006	7

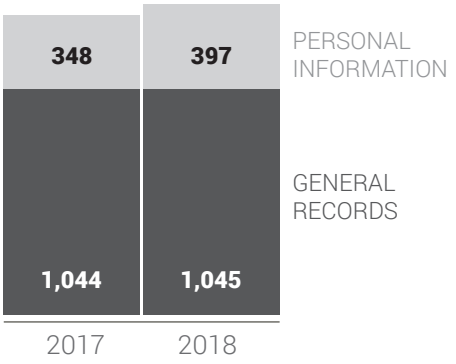
When Part X of the new law, which governs personal information, comes into force on January 1, 2020, children, youth, and their families will have the right to access and request correction of their records of personal information held by children's aid societies, group homes and other service providers. They will also have the right to file complaints with our office and have increased control over how their personal information is shared.

Overseeing this new framework significantly expands the IPC's mandate while creating new obligations and responsibilities for service providers.

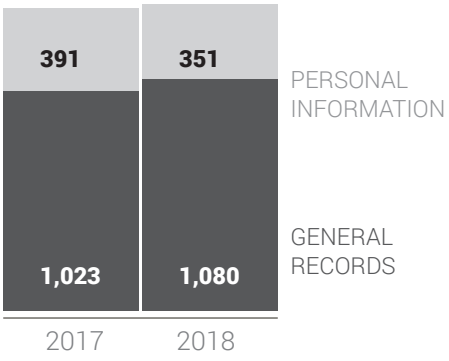
The IPC spent much of 2018 working with the Ministry of Children, Community and Social Services and stakeholder organizations to prepare for this increase in our oversight responsibilities. Our work included consulting on the development of the regulation relating to privacy breach reporting, research requirements, and record handling and retention.

Our work will continue through 2019 as we develop guidance materials and increase public outreach to ensure that service providers and families across the province are aware of these new rights and responsibilities.

APPEALS OPENED IN 2018



APPEALS CLOSED IN 2018



FOI hits and misses

In 1998, two students at Stanford University founded Google. Movie lovers drove to the local Blockbuster to rent films, the first BlackBerry (a pager) was released, and Mike Harris was the Premier of Ontario. The final episode of *Seinfeld* aired, and the IPC opened what would become the longest active file in its history.

The file that resulted in Order PO-1779, issued on May 5, 2000, spanned nearly 20 years, two judicial review applications, two court appeals — including an appeal to the Supreme Court of Canada — five IPC orders and seven IPC adjudicators and lawyers.

This complex, frustrating, and often-confusing file eventually came to serve as an important example for institutions: the public's right to information is not abstract ideology. Public organizations have the ability and the duty to exercise appropriate discretion when making access decisions to ensure the public's right to know is not ignored.

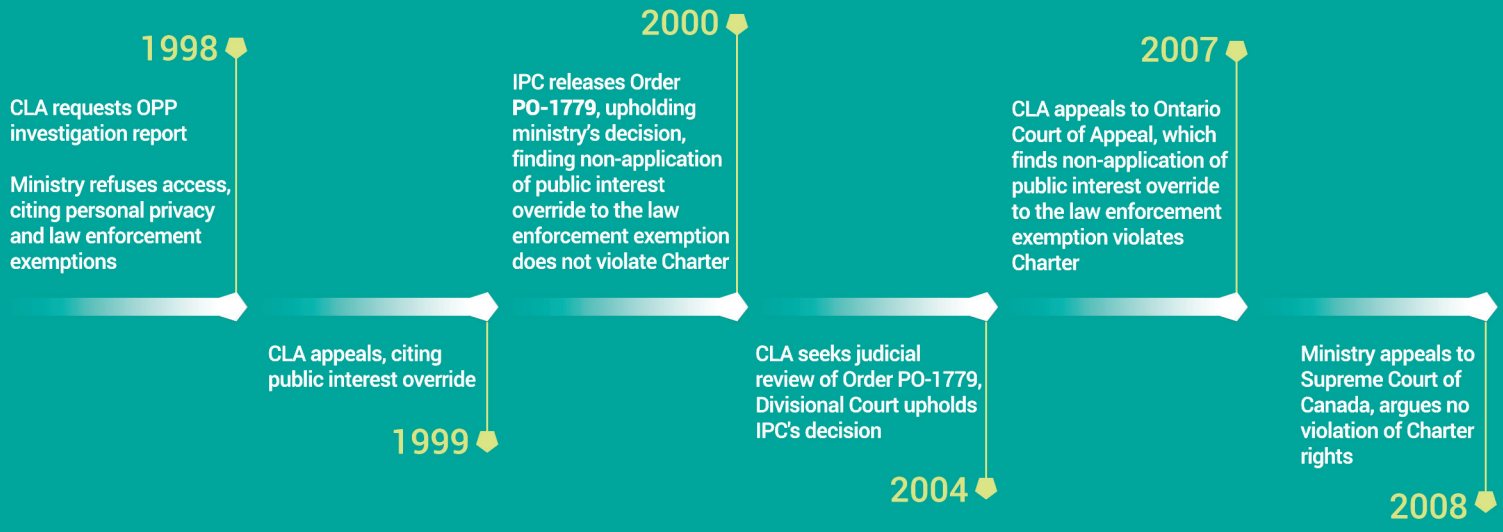
This case resulted in a lengthy, unnecessarily litigious and staggered release of information, partly due to the reluctance of a government ministry to take the exercise of its discretion seriously.

***

Mobster Domenic Racco was murdered in 1983 and in 1992 two men were convicted for his death. In 1997, after both men had spent five years in prison, Justice Stephen Glithero announced he was staying the murder charges because of police and Crown prosecutor misconduct. "The loss of so many audiotapes, videotapes, notes and reports can only be categorized as involving an unacceptable degree of negligent conduct …," said Justice Glithero.

After investigating the judge's allegations, the Ontario Provincial Police announced it found no evidence of misconduct but did not reveal the reasons for its conclusions. As a result, the Criminal Lawyers' Association made a request to the Ministry of Community Safety and Correctional Services for their records, including the investigation report.

Ontario's access laws provide a right to information, except where the information falls within certain exemptions. Here, the ministry denied access to the information,



TIMELINE OF PO-1779

citing personal privacy and law enforcement exemptions. Exemptions can sometimes be set aside where there is a compelling public interest in disclosure of the information. However, Ontario's access laws do not allow the public interest to override the law enforcement exemption.

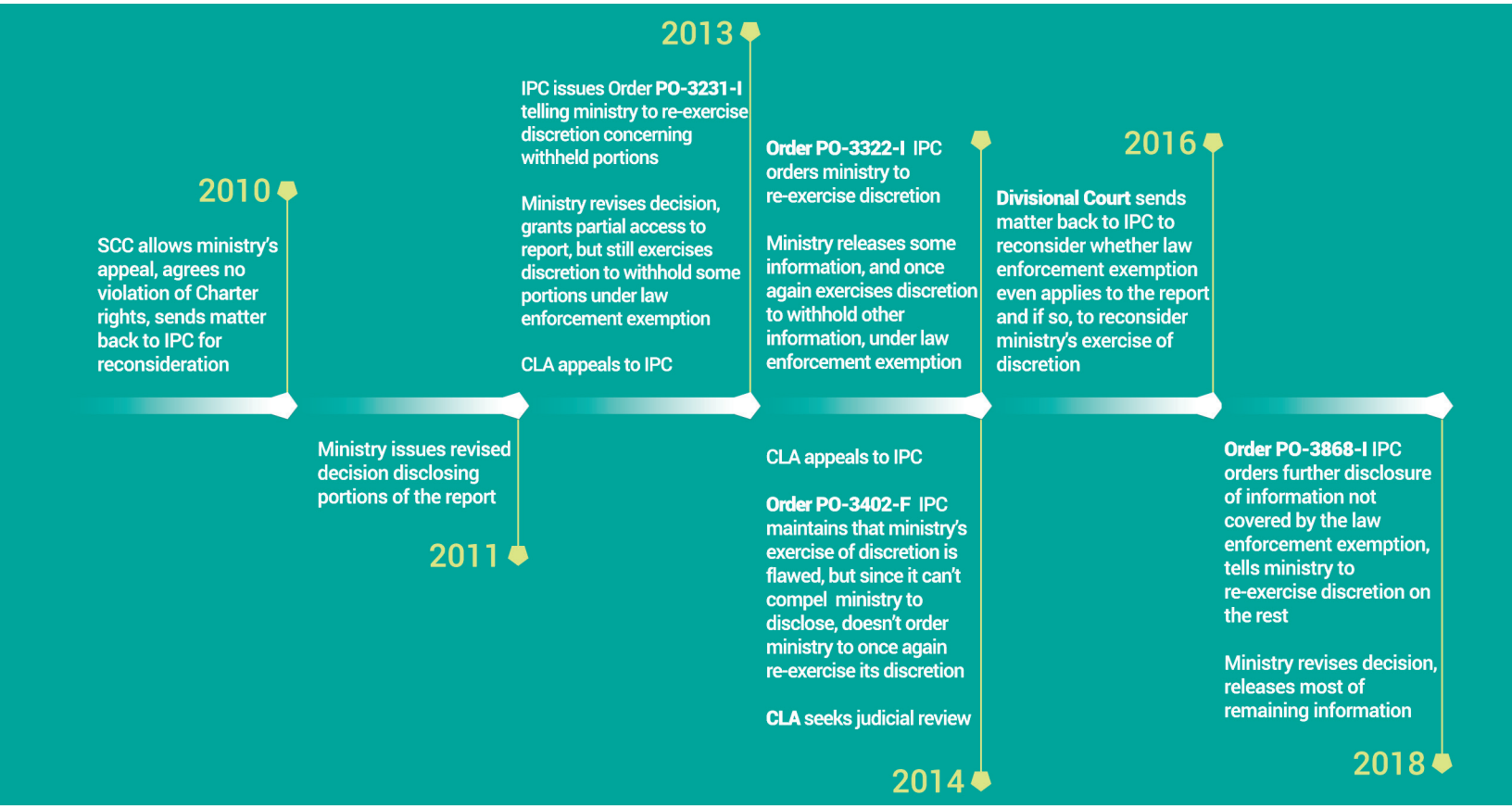
On appeal to our office, the IPC decided that, given the serious misconduct described by Justice Glithero, a lack of explanation from the OPP, and the public discussion that resulted, there was a compelling public interest in the information that would justify disclosure, despite privacy considerations. However, because the law did not permit the public interest to override the law enforcement exemption, the IPC upheld the ministry's initial decision not to release the information.

The result was that all the information remained under wraps.

In 2010, after a series of court cases, the Supreme Court of Canada confirmed that the public interest override in Ontario's access laws did not apply to the law enforcement exemption. It also decided that it was within the ministry's power to exercise discretion to release the information anyway – even though the information was exempt from disclosure under the law enforcement exemption. Astonishingly, it took another eight years, four orders from our office, and another decision by the Divisional Court to convince the ministry to properly use its discretion and release the information.

In 2018, 20 years after the date of the initial request, the ministry disclosed the remaining information at issue. The OPP investigative report, "Project No Show," was finally released to the CLA.

Despite this long and complex process, there is a positive outcome for institutions in Ontario. They have clarity and they now know how the IPC, and the courts, expect them to exercise discretion in cases where there is a heightened public interest. The Supreme Court of Canada has also confirmed that, in some cases, the right to freedom of expression in the *Canadian Charter of Rights and Freedoms* can require governments to disclose information, even if it qualifies for exemption under access laws. At its core, this case affirms that 20 years is far too long to wait for access to government information.



Public health statistics

During the past year, some Ontarians were feeling a bit under the weather when it came to getting non-identifying statistical information about disease outbreaks in their communities. They reached out to our office for help, and we contacted public health officials to clarify that Ontario's privacy laws do not prohibit the release of this type of data. Our office followed up with a public statement emphasizing the public's right to know this information and encouraging institutions to be open and transparent with non-identifying health statistics. Institutions that adopt a proactive stance, one aimed at enhancing the public's right to access information, are supporting accountability and building trust in their organization.

Right to know

The IPC worked throughout 2018 to uphold the public's right to know and empower the public to exercise its access rights. As part of this work, we participate in public events and conferences, deliver presentations, and publish guides and fact sheets to help institutions and the public navigate the freedom of information process.

Among the materials we developed in 2018 was a guide on fees to assist institutions in calculating costs for access to information requests and a fact sheet about third party exemptions to help in determining if requested information is exempt.

Mediated appeals

The IPC settles many access to information appeals through mediation, a process that can save significant time and resources.

Our dedicated team of mediators work on a case-by-case basis, investigating the circumstances of each appeal, clarifying the issues and finding solutions to satisfy the needs of all involved. Here are a few mediation success stories from the past year that illustrate this vital work:

Institutions that adopt a proactive stance, one aimed at enhancing the public's right to access information, are supporting accountability and building trust in their organization.

- The City of Toronto received a request from a reporter for all drafts and the final version of the city's long-term financial plan, as well as any notes and tracked changes associated with the documents. The city denied access because the plan is publicly available. During mediation, the city noted the large size of the request, indicating more than 200 staff had provided input into more than 300 draft versions of the document. Of these drafts, about 70 per cent did not contain significant changes. Based on this information, the reporter narrowed the request to specific versions of the plan, receiving a fee estimate of $450 to process the request. To reduce the fee, the reporter narrowed the request further to only the four to five iterations of the plan held by the city manager's office — resulting in a $120 fee estimate. After receiving a deposit, the city issued a decision granting partial access, resolving the appeal.

- The Ministry of Infrastructure received a request from an Indigenous organization for the floor plan of a new police detachment. The ministry denied access to the information, declaring that releasing the document could present a danger to safety or health. During mediation, the ministry also added law enforcement reasons for denying access. During a conference call with the mediator, the requester, and the ministry, the requester explained they needed the material to explore housing issues for Indigenous police officers and changed the scope of the request. Rather than asking the individual to submit a new request, the ministry included the new search considerations within the appeal, conducted another search and

found new records. The ministry disclosed the newly located records and the file was closed.

- An individual was denied security clearance and lost her job at an airport when her name appeared in several police occurrence reports. She made a request to the police for access to the reports so she could submit them to her employer for review. The police denied access to the reports on the grounds they did not relate to the requester and provided a printout showing she had no record with the police. Her employer did not accept this information. During mediation, the police agreed to provide the requester with a letter containing specific information that could assist the individual in the situation with her employer. After giving this letter to her employer, the requester received the security clearance necessary to get her job back.

- The Toronto Transit Commission received a request from a reporter for all emails, briefing notes and reports relating to the Scarborough subway and light rail transit line between 2010 and 2017. The TTC issued a fee estimate of more than $30,000 (which included a 50 per cent reduction for duplicate pages) and an estimate of one to three years to complete the request. During mediation, a teleconference with a number of individuals, including the reporter, the project manager, freedom of information analysts and IT staff resulted in the reporter repeatedly narrowing the scope of her request and the TTC reducing the fee. The appeal was eventually resolved and the final fee estimate reduced to $707.

- A ministry received a request from a landlord's representative for police reports and officer's notes relating to a search warrant issued for his property. The requester wanted the information to prepare for a Landlord and Tenant Board hearing. The ministry denied access for law enforcement and personal privacy reasons, and the requester appealed. During mediation, the requester told the mediator that the board hearing was coming up in a week. The mediator then spoke to the ministry, letting them know that the requester needed the information as quickly as possible. The ministry restated its decision not to disclose but agreed to provide the name and contact information of the investigating officer. Through communications with the investigating officer, the individual was able to get the information, and it was no longer necessary to pursue access to the withheld record.

Significant access decisions

Our adjudication team continued to provide leadership on the application of provincial and municipal access laws. Decision highlights from the past year include:

Order PO-3871 – An environmental organization made a request to Ontario Power Generation for access to the table of contents of an analysis of the Darlington Nuclear Generating Station. Our office rejected the OPG's claim that disclosure of the table of contents could endanger building security or prejudice the defence of Canada and ordered its release. Exceptions were made for sections of the document identifying sensitive "release category" and "plant damage state" numbers.

Order MO-3684-I – An individual requested access to information related to a specific employment opportunity with the City of North Bay. The city withheld access to the employment agreement for the position, arguing that its disclosure would reveal discussions held at a closed meeting and invade personal privacy. Our office did not uphold the city's decision. Although the agreement revealed the results of the closed meeting discussion, it did not contain the deliberations that occurred during the meeting. There was a compelling public interest in disclosure of the salary information in the agreement, and personal privacy considerations did not justify withholding it.

Order MO-3685 – Our office ordered the disclosure of a chart relating to the seizure of marijuana plants from various addresses in the Sudbury area. Although the addresses were considered personal information, factors favouring disclosure outweighed privacy considerations. These included public scrutiny, consumer protection and the promotion of public health and safety.

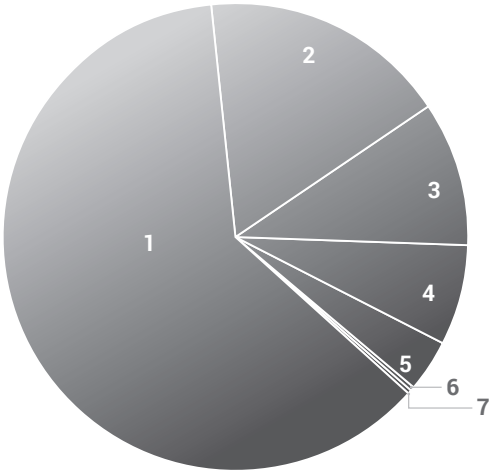
Order PO-3905 – A former inmate requested video footage of their interactions with correctional officers at a maximum-security correctional facility from the Ministry of Community Safety and Correctional Services. The IPC accepted the ministry's position that disclosure of some of the video footage could jeopardize the security of the facility. Our office determined that exempt portions of the footage could be redacted or blurred, allowing some parts of the video to be released.

Order PO-3862 – An individual requested access to records held by Health Sciences North relating to requests for assisted death. The hospital refused to confirm or deny their existence on the basis that doing so would be an invasion of privacy and could compromise law enforcement activities and security at the hospital. Our office ordered the release of the records; their disclosure would not affect hospital security or law enforcement and the requester was not seeking access to any information that could be used to identify patients or staff.

Order PO-3861 – A former patient of the Ottawa Hospital requested access to information relating to his complaints about a medical resident, the medical chief of staff and several physicians. The hospital claimed most of the records were excluded from release because they dealt with employment or labour relations matters. Our office found the individual had a right to some of the information under Ontario's health privacy legislation. In addition, many of the records were not employment-related because they were created in response to the patient's complaints and not for an employment-related purpose.

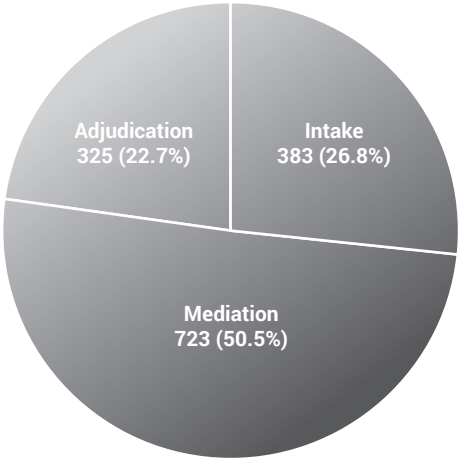
Order PO-3865 – The Ministry of the Attorney General received a request for copies of completed eviction forms. The ministry denied access to these forms because they were not within its custody or control. The IPC upheld the ministry's decision because the documents were court records and not in any way mixed in with ministry records.

OUTCOME OF APPEALS



1. Mediated in full: 885 (61.8%)
2. Order/Decision issued: 245 (17.1%)
3. Screened out: 142 (9.9%)
4. Withdrawn: 100 (7.0%)
5. Abandoned: 55 (3.8%)
6. Dismissed without inquiry/ review: 2 (0.1%)
7. Dismissed without order/ decision: 2 (0.1%)

APPEALS CLOSED BY STAGE



Judicial reviews and interventions

Our legal department represents the commissioner in judicial reviews and appeals of the IPC's decisions, and interventions in certain court cases involving access and privacy issues.

In 2018, the IPC was granted intervenor status in two matters before the courts.

Here are some highlights of this year's work.

Top doctors' billings

A journalist asked the Ministry of Health and Long-Term Care for the names of the top 100 OHIP billers, their medical specialties, and the total dollar amounts they received, for the years 2008-2012. The ministry disclosed the dollar amounts and most of the specialties but withheld the physicians' names and some of the specialties under the personal privacy exemption in *FIPPA*. Some of the parties to the appeal also raised the third party business information exemption in *FIPPA*. The appellant claimed that the public interest override applied.

In Order PO-3617, the IPC decided that the record does not contain personal information, but rather professional or business information, and therefore, the personal privacy exemption does not apply. The IPC also found that the third party exemption did not apply and that there was a compelling public interest in the disclosure of the information. The IPC ordered the ministry to disclose the record in its entirety to the journalist.

Ontario's Divisional Court dismissed three applications by doctors' groups to overturn the order, ruling that it was reasonable. The court agreed that the names of the doctors, together with the amounts they receive in OHIP payments and their medical specialties, are not "personal information."

The compelling public interest in the activities of an institution often outweighs the personal privacy of senior public officials.

The Ontario Court of Appeal heard appeals from this decision in June 2018 and upheld the IPC's order. The OMA and two doctors' groups made a joint application for leave to appeal to the Supreme Court of Canada, which the court dismissed in April 2019.

Office of the Children's Lawyer for Ontario

In Order PO-3520, the Ministry of the Attorney General received a request for information about services provided to the requester's two children by the Office of the Children's Lawyer for Ontario. The OCL took the position that *FIPPA* does not apply to litigation files where it provides services to children. The ministry claimed that the files were not in its custody or control and denied the request.

We found that records of the OCL covered by the request were in the custody or control of the ministry and ordered the ministry to issue an access decision to the requester. The access decision could be made by the OCL.

The OCL filed an application for judicial review, which the Ontario Divisional Court dismissed. The Ontario Court of Appeal heard the OCL's appeal in late 2017 and issued a decision in 2018 that allowed the appeal and overturned the IPC's order. The IPC sought leave to appeal this decision to the Supreme Court of Canada, which was denied in March 2019.

Algoma Public Health report on allegations of wrongdoing

Algoma Public Health received a request for access to the "final report of [the] 2015 KPMG Forensic Review." The report related to whether there was a conflict of interest in the appointment of APH's former interim Chief Financial Officer and whether any funds

were misappropriated or lost by APH. While APH determined that an exemption for personal privacy under *MFIPPA* applied, it decided to grant access to the report under the public interest override. An affected party appealed APH's decision, claiming disclosure would expose her to civil liability. The affected party also claimed that the public interest override did not apply. In Order MO-3295, the IPC decided that the personal privacy exemption applied, but agreed with APH that there was a compelling public interest in disclosure of the report. Accordingly, the IPC ordered APH to disclose it to the requester.

The affected party sought a judicial review of the order and its associated reconsideration order. The Divisional Court overturned both. The appeal was sent back to the commissioner for a new hearing.

The IPC appealed the Divisional Court's decision to the Ontario Court of Appeal. The appeal was heard at the end of 2018, and on April 9, 2019, the court released its judgment, finding that the IPC's decision in Order MO-3295 is reasonable. The court agreed with the IPC's conclusion that, in this case, the compelling public interest in the activities of the institution and whether there was a conflict of interest outweighs the personal privacy of senior public officials.

Schools are not "privacy-free zones"

Police arrested a high school teacher in 2011 after learning he had used a pen camera to secretly record female students' chests and cleavage. The recordings took place in school common areas, such as the cafeteria, classrooms, hallways, and outdoor grounds.

The teacher was acquitted, with the judge ruling that while the videos were an invasion of privacy, they weren't made for a sexual purpose.

The decision was appealed to the Ontario Court of Appeal, where the acquittal was upheld, for different reasons: the court ruled that while the videos were made for sexual purposes, the students did not have a reasonable expectation of privacy in the school, where video surveillance cameras, used for security purposes, were already in use.

In an appeal to the Supreme Court of Canada, the IPC intervened to assist the court in determining whether the recordings were made in a situation where the students would reasonably expect privacy.

The IPC position, presented to the court, was that students have a reasonable expectation of privacy in school, even in the common areas of the building where the school has lawful video surveillance cameras.

The IPC argued that people have the right to go about their daily activities — including in public spaces — without the threat of being secretly recorded for unauthorized, sexual purposes. Schools, colleges, universities, hospitals, libraries, town halls and other public facilities are not privacy-free zones, regardless of the presence of security cameras.

Consistent with the IPC's submissions, the SCC found that the students reasonably expected that they would not have been recorded in the way that the teacher had done so (including for sexual purposes). This expectation of privacy exists even when students are in outdoor and indoor common areas subject to video surveillance. The SCC convicted the teacher of voyeurism.

The open court principle and administrative tribunals

The Ontario Superior Court granted the IPC intervenor status at a hearing involving the Toronto Star and the Ministry of Attorney General in April 2018.

Under Ontario's provincial access law, the public has a right of access to documents held by governments and broader public sector organizations, including adjudicative tribunals such as the Human Rights Tribunal of Ontario and the Ontario Labour Relations Board.

However, because of the personal information exemption under *FIPPA*, institutions have refused requests for certain information, including adjudicative records that contain personal information. Adjudicative records include such documents as applications or complaints

and responses to them, evidence filed by parties to the proceeding, schedules of hearings, and transcripts of hearings.

The Toronto Star brought an application to challenge the use of this law to deny access to the adjudicative records of certain administrative tribunals. Its position was that using the personal information exemption violates the open court principle, which is a key part of freedom of expression. Freedom of expression is guaranteed by the *Canadian Charter of Rights and Freedoms*. The Toronto Star argued that the procedure and processing time for access requests, as set out under *FIPPA*, also violated the open court principle.

The IPC provided the court with details of the rules under *FIPPA*, including how certain provisions can apply to the adjudicative records of administrative tribunals.

The Ontario Superior Court found that the application of *FIPPA*'s personal information exemption to the adjudicative records of the tribunals is unconstitutional and therefore can't be enforced. The court gave the ministry 12 months to amend the law (if it chooses to do so) before it will declare it invalid.

While the court found that *FIPPA*'s procedure and processing time also breached the open court principle, it ruled that these provisions resulted in only minimal delays and are therefore not unconstitutional.

New judicial reviews, applications and IPC interventions in 2018	5
Launched by:	
Institution	1
Requester / Complainant	2
Affected party	1
IPC intervened in other application or appeal in 2018	1

Ongoing judicial reviews, applications and IPC interventions in 2018 (as of December 31, 2018)	10
Launched by:	
Institution	2
Requester / Complainant	2
Affected party	3
IPC intervened in other application or appeal in 2018	3
IPC-initiated application	0

Judicial reviews and IPC interventions closed or heard in 2018	13
Abandoned or settled or dismissed for delay or Rule 2.1.01(3) – IPC order stands	3
IPC order upheld (or leave to appeal dismissed)	7
IPC order not upheld (or IPC's leave to appeal dismissed) and remitted back to IPC	0
Hearing held but decision on reserve	1
IPC order upheld on SCC appeal	0
IPC order not upheld on SCC appeal	0
IPC intervened in SCC or Federal Court appeal	1
IPC intervened in OSCJ	1

Privacy

In 2018, the IPC's work spanned a range of topics related to privacy protection in Ontario.

Smart cities

Smart city technologies have the potential to help cities better manage urban environments and deliver services in a more effective and efficient way. However, these technologies also bring privacy risks, since they can collect, use and generate massive amounts of data, including personal information. Strong safeguards are needed to ensure that these technologies are not used to track people as they go about their daily activities, or permit personal information to fall into unscrupulous hands as the result of a cyberattack.

In April, we invited privacy authorities from across Canada to join us in urging the federal government to take steps to ensure privacy and security are at the forefront of its Smart Cities Challenge. As a result of these efforts, the federal government included requirements to protect privacy as part of the selection criteria.

Throughout 2018, we lent our voice and expertise to the smart city discussion through engagement with and advice to municipalities involved in smart city projects. Our recommendations have been consistent:

- define smart city goals from the outset
- ensure lawful authority to collect, use and disclose personal information

Outsourcing data management services does not relieve public sector organizations of accountability for protecting personal information. It always remains the responsibility of the organization.

- avoid "tech for tech's sake"
- accountability rests with the institution if outsourcing to external service providers
- de-identify personal data where possible
- engage the community
- be transparent

In 2018, we issued the fact sheet, *Smart Cities and Your Privacy Rights*, which aims to help the public understand smart cities and how to build them in a way that protects privacy.

We continue to engage the municipal and provincial governments actively as we move into this new frontier of smart city technologies for improved public service.

Cyberattacks

Ransomware is a type of malicious software designed to block access to a computer system until the victim pays a sum of money. These kinds of cyberattacks have become an increasingly common and serious threat to the security of electronic records. As long as technology and data integration projects evolve and become more complex, so will the sophistication of hackers, leaving institutions vulnerable to cyber- and ransomware attacks.

This year saw a rise in the frequency of ransomware incidents and Ontario municipalities were targeted. Both the towns of Wasaga Beach and Midland reported falling prey to cyberattacks and both paid to regain access to their data. In addition, 15 privacy breaches resulting from cyberattacks were reported to the IPC from the health care sector.

Institutions and custodians need to plan for cyberattacks by having measures in place to secure their systems and enable early detection. These systems need to be continually updated to ensure they meet security industry standards and best practices. For organizations and custodians that rely on external data management services, it is important to remember that outsourcing these functions does not relieve them of accountability for protecting personal information. It always remains the responsibility of the organization.

In 2018, the commissioner addressed cyberattacks and ransomware in many of his public presentations, driving home the point that institutions need to have appropriate security measures in place and a privacy breach protocol. These measures are laid out in more detail in our technology fact sheet, *Protecting Against Ransomware*.

Disclosure of personal information to law enforcement

In Ontario, privacy rights are protected by rules limiting the collection, use, and sharing of personal information. However, there are exceptions, including when law enforcement is involved.

Generally, public sector organizations should only disclose personal information to police when required to do so by law, such as in response to a court order.

There are some exceptions to this rule. For example, in cases where the health or safety of individuals hangs in the balance or information is available that could assist an investigation, an organization can disclose personal information without a court order.

In November, we released the fact sheet, *Disclosure of Personal Information to Law Enforcement*, which explains the factors that public organizations must consider when deciding whether to disclose personal information. The fact sheet also outlines the steps an institution should take in responding to these requests, best practices for documenting them, and how to provide greater transparency to the public about these types of disclosures.

Surveillance

The increased use of video surveillance by the government and private sector has resulted in the increased collection of personal information and tracking of individuals as they go about their daily activities. Privacy implications associated with surveillance technologies include the potential to collect large amounts of personal information and track the whereabouts of law-abiding individuals.

Over the years, the IPC has made recommendations aimed at balancing public safety with individual privacy when using video surveillance. Organizations can achieve this balance by limiting surveillance and the amount of personal information collected and retained.

In February, Commissioner Beamish spoke out against a City of Hamilton proposal to amend its bylaw prohibiting homeowners from pointing their CCTV cameras at the street.

The proposed amendment of the bylaw would permit homeowners to position their cameras to capture public spaces, rather than just their property. It would also allow for the collection of personal information from private home surveillance systems for use by the police.

In a letter to the mayor and police chief, Commissioner Beamish reminded the city of its responsibility under the municipal privacy law to protect the privacy rights of Ontarians. Permitting or encouraging the use of private video surveillance cameras for collecting personal information to aid in law enforcement would undermine those rights.

In January 2019, Hamilton's city council decided to maintain its existing bylaw banning CCTV cameras from pointing at the street. The commissioner stated that the bylaw strikes a good balance between homeowner security and privacy and that "Hamilton's bylaw provides a good blueprint for other municipalities that want to regulate private CCTV cameras."

In response to concerns and questions around the correct use of video surveillance, our office hosted a webinar in October on the *Do's and Don'ts of Video Surveillance*. The webinar advised public organizations on ways to implement a video surveillance program that respects and protects individual privacy. Our work in this area is ongoing, and our policy department routinely guides provincial and municipal organizations considering video surveillance programs.

Education

In June, the IPC worked with Canada's federal, provincial, and territorial privacy authorities to release a three-volume set of lesson plans on privacy:

- Getting the Toothpaste Back into the Tube: A Lesson on Online Information
- Know the Deal: The Value of Privacy
- Privacy Rights of Children and Teens

These lesson plans help educators teach students about their privacy rights and how to navigate the digital environment safely.

We also co-chaired a task force with the Office of the Privacy Commissioner of Canada to research, create and sponsor a resolution at the 40th International Conference of Data Protection and Privacy Commissioners. The *Resolution on E-learning Platforms* includes 24 recommendations and guidance to protect privacy when developing, implementing, and using online educational services.

The IPC continued its work in the education sector throughout 2018 and into early 2019, issuing four fact sheets and the guidance document, *A Guide to Privacy and Access to Information in Ontario Schools*.

At conferences and in consultations with education stakeholders, we continue to promote digital literacy skills, responsible use of online educational services, and compliance with Ontario's privacy and access laws.

Anti-Racism Act data standards

Ontario's anti-racism legislation was designed to help public-sector organizations identify and monitor racial disparities to eliminate systemic racism and advance racial equity. The law affects Ontarians of all ages who engage with organizations such as municipalities, ministries, school boards, universities, colleges and child and family service providers.

In April, Ontario launched the *Data Standards for the Identification and Monitoring of Systemic Racism*. The standards define additional requirements and provide guidance for public sector organizations that collect, manage and use race-based data.

In 2018, our office provided advice on the data standards for the collection, use, disclosure, de-identification, management, publication and reporting of race-based data.

The anti-racism regulation was approved in April 2018. It defines when public sector organizations are authorized or required to collect race-based data. As of May 1, 2018, Ontario schools or boards are authorized to collect Indigenous identity, race, religion and ethnic origin of pupils according to the data standards.

An Ontario model for sexual violence case review

In 2018, the IPC continued its engagement with police and violence against women stakeholders on the implementation of the US-based Philadelphia Model. Under this model, police appoint women's advocates as agents to review closed sexual violence files. The aim is to identify any investigative shortcomings related to, for example, biases, or stereotypes.

Communities across the province are now using a memorandum of understanding and confidentiality agreement, originally developed by the IPC, the Kingston Police, and Sunny Marriner, the Provincial Lead-Violence Against Women Advocate Case Review, to help ensure the Philadelphia Model is applied within a framework that ensures the protection of individual privacy.

In 2018, the Ontario Association of Chiefs of Police endorsed this approach to sexual violence case review. Throughout the year, the IPC worked closely with Staff Sergeant Valerie Gates (Barrie Police) and Sunny Marriner on the case review elements of the OACP's guidance document that sets best practices for police response to sexual violence.

Europe's General Data Protection Regulation

Implemented in May 2018, the European Union privacy law may apply to institutions in Ontario in certain circumstances, such as when offering goods and services to people in the EU, or when monitoring the behaviour of people in the EU. While the IPC does not oversee or enforce the GDPR, we developed a fact sheet, *General Data Protection*

Regulation, to provide general information about the application of this law, and its key requirements.

Privacy issues dealt with by the tribunal

Our intake department serves as our front-line response to privacy breaches and complaints and is often able to resolve them before they reach the investigation stage. Below are some privacy matters closed at intake.

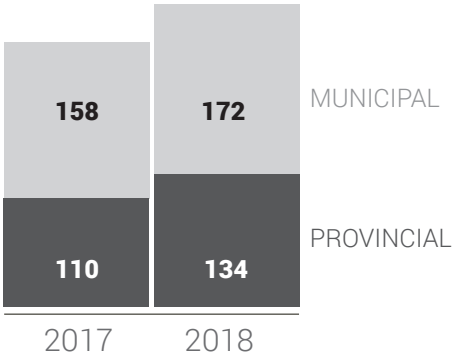
Breach of Ontario Cannabis Store contact information

The Ontario Cannabis Store contacted our office in early November when they became aware of a data breach. A hacker accessed a Canada Post delivery-tracking tool and exposed the names, postal codes, delivery dates and reference and tracking numbers of over 4,500 individuals who signed for OCS packages delivered by Canada Post. The OCS took prompt action by notifying its affected customers and encouraging Canada Post to do the same. The IPC was satisfied that the breach was the result of a hack of Canada Post's system, which falls under federal privacy laws.

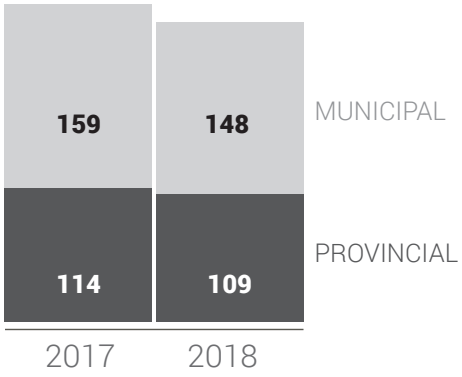
Disclosure of utility bills to a property owner

An individual submitted a privacy complaint regarding the disclosure of his water and waste bills by a municipality to his landlord. The municipality explained that under the *Municipal Act*, all charges concerning these utilities are ultimately the responsibility of the property owner. Residents must be aware, before being added to an account, that the property owner will be notified if the tenant is in arrears. The municipality explained further that all water and wastewater billing accounts are registered to the property owner. Tenants are authorized by their landlords to be added to the account for bill payment, with the condition that the landlord is notified if their account goes into arrears. The IPC was satisfied; this disclosure was authorized under the law, and the complaint was dismissed.

PRIVACY COMPLAINTS OPENED IN 2018



PRIVACY COMPLAINTS CLOSED IN 2018



Municipal files moved by former employee

A township reported that, after business hours, a staff member moved several boxes of municipal files, without authority, to an undisclosed location. The missing files contained documents with individuals' property taxes and utility billing information.

To contain the breach, the township sought legal advice and reported the incident to the OPP and the IPC. After several discussions between the township and the employee, the township discovered that the boxes were in an off-site storage unit. With the help and direction of the IPC analyst, the township communicated with the employee and was able to get the missing files back. The IPC was satisfied that no records in the storage unit were compromised or tampered with and the township had taken steps to prevent a similar occurrence.

Cyberattacks on municipalities

Two municipalities were targets of sophisticated ransomware attacks that resulted in disruption to the delivery of municipal services. The municipalities were unable to decrypt the contaminated files and paid a ransom in the interest of resuming municipal operations quickly.

Our office reviewed the details of the ransomware attack and the measures adopted by each municipality to prevent similar incidents from occurring in the future. In both cases, the IPC was satisfied with the comprehensive responses of the municipalities.

Investigations

The IPC's investigators look into matters that cannot be resolved to the IPC's satisfaction at an early stage, and may issue public reports. Here are some privacy issues our investigators dealt with in 2018.

University of Windsor

The University of Windsor contacted our office in January to report a data breach after the personal information of law school applicants — including names, test scores, email addresses, and student numbers — were accidentally attached to a notice and posted online.

After a review of the circumstances, IPC investigators were satisfied with the steps taken, which included targeted privacy training and a requirement for all application data to be password protected by the university to prevent further disclosure of the information, limiting the risk of identity theft.

Police services leaks

In May, we became aware of two separate incidents involving the Toronto Police Service. In the first case, a member of the TPS accessed a document from the Police Information Portal, without authorization, and disclosed the information about the arrests of three people by another police service. The other incident involved the alleged unauthorized disclosure of a CCTV image of a member of the Toronto Blue Jays within a correctional facility. Both indicated the potential unlawful use and disclosure of personal information, sparking a review of the circumstances.

Following a review of TPS' practices, the IPC was satisfied that appropriate policies, procedures and training were in place to ensure personal information is handled appropriately.

Privacy reports

MC16-5 – school photos

The IPC received a complaint from a parent about a school board's picture-taking program when the personal information of students was shared with a third-party photographer. Upon investigation, the IPC found that the board's disclosure of students' personal information to the photographer was permissible, but had concerns about the photographer's participation in the Pictures2Protect Program. This program operates in partnership with the Canadian Centre for Child Protection, which raised concerns about who would have access to the students' personal information.

In our report, we recommended that schools allow parents to opt out of receiving marketing materials and tell them that they can ask the vendor to destroy their children's personal information, provided the board does not need it for its administration.

MI16-3 - Personal information of students used to market RESPs

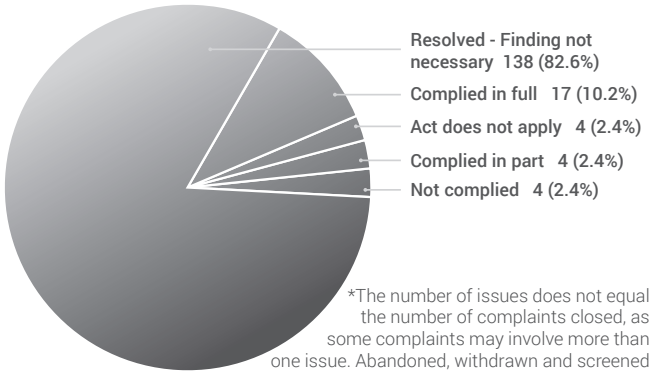
Our office was notified that the Peel District School Board might have violated Ontario's municipal privacy law when one of its teachers allegedly disclosed the names of students who had individual education plans to their spouse, a financial investment representative, for the purpose of marketing registered educational savings plans to parents.

We initiated an investigation and found that the disclosure of students' personal information from a special education teacher to another teacher, and the board's use of students' personal information, through the actions of the teacher, did not comply with the law.

The IPC recommended that the board require its staff to sign confidentiality agreements.

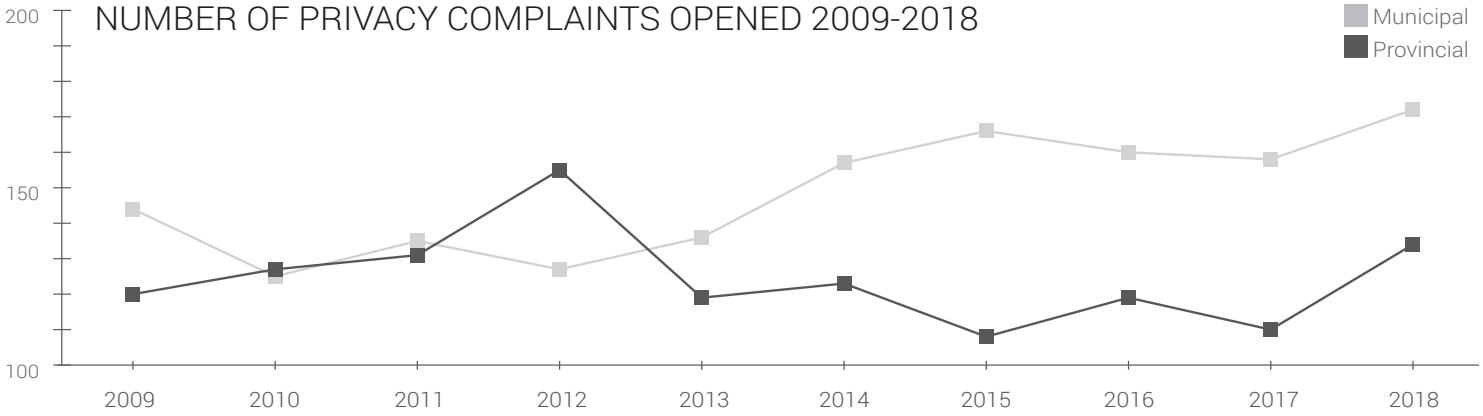
PRIVACY COMPLAINTS CLOSED BY TYPE OF RESOLUTION

OUTCOME OF ISSUES* IN PRIVACY COMPLAINTS

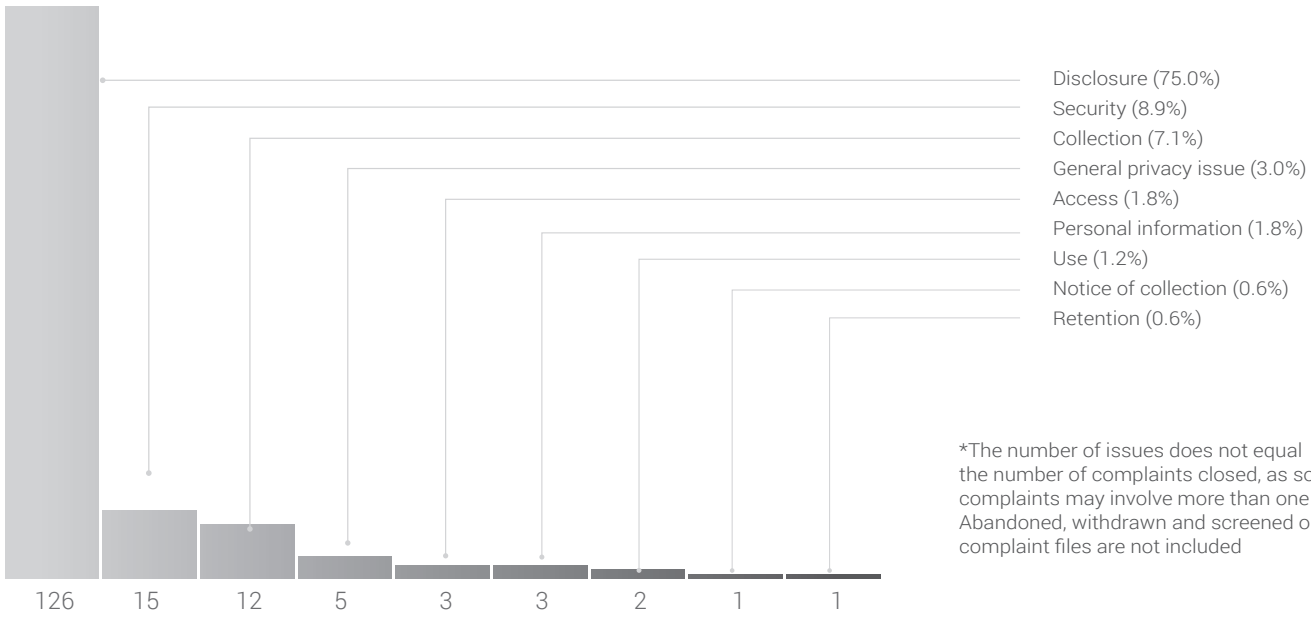


*The number of issues does not equal the number of complaints closed, as some complaints may involve more than one issue. Abandoned, withdrawn and screened out complaint files are not included.

NUMBER OF PRIVACY COMPLAINTS OPENED 2009-2018



ISSUES* IN PRIVACY COMPLAINTS CLOSED



*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

Consultations

The IPC is committed to engaging and collaborating with, organizations seeking expertise and insight into access and privacy issues.

Anti-Racism Directorate, Cabinet Office

- data standards established under the *Anti-Racism Act*

Canada Health Infoway

- updates to PrescribeIT

Children's Treatment Network of Simcoe York

- electronic services to custodians

City of Cambridge

- video surveillance system for use in the city's downtown core

City of Thunder Bay:

- planned creation of a Public Safety Command Centre coordinating video surveillance

City of Toronto

- Payment Card Industry compliance and email archiving

College of Physicians and Surgeons of Ontario

- closing a medical practice policy
- prescribing drugs policy
- disclosure of harm policy
- policies regarding continuity of care

College of Psychologists of Ontario

- language of records of personal health information

Financial Services Commission of Ontario and Ministry of Finance

- electronic proof of automobile insurance

Infrastructure Canada, Smart Cities Challenge Directorate

- Smart Cities Challenge

Justice Michael H. Tulloch

- Independent Street Checks Review

Kids Help Phone

- Crisis Text Line powered by Kids Help Phone

Mackenzie Health

- procurement of a smart auditing tool

Ministry of the Attorney General

- *Cannabis Licence Act*

Ministry of Children, Community and Social Services

- Part X of the *Child, Youth and Family Services Act* and its regulations

Ministry of Community Safety and Correctional Services

- *Police Record Checks Reform Act*
- *Safer Ontario Act*

Ministry of Education

- data sharing initiative with Kinoomaadziwin Education Body
- development of a truncated safety template for teachers and education workers

Ministry of Government and Consumer Services

- privacy management program review
- updated *Freedom of Information and Protection of Privacy Manual for Institutions*
- updated privacy breach protocol guidance

Ministry of Health and Long-Term Care

- regulation under *Health Sector Payment Transparency Act*
- regulation under *Immunization of School Pupils Act*
- Immunization Connect Ontario network
- Digital Health Strategy
- Digital Health Drug Repository

Ministry of Labour

- *Pay Transparency Act*

Ministry of Tourism, Culture and Sport

- regulation under *Rowan's Law (Concussion Safety)*

Office of the Privacy Commissioner of Canada

- co-chaired an international digital education working group to develop a resolution on e-learning platforms

Ontario Association of Children's Aid Societies

- Part X of the *Child, Youth and Family Services Act*

Ontario Cannabis Retail Corporation

- cannabis online sales

Ontario Provincial Police Service, Greater Sudbury Police Service and Community Sexual Assault Case Review Advisory Committee

- sexual violence case review, Philadelphia Model

Ottawa Hospital

- privacy breach management framework
- privacy breach detection software

Toronto Police Service

- Toronto Community Housing Corporation information sharing
- full body scanner pilot project

Toronto Transit Commission

- SafeTTC mobile app for reporting incidents
- external cameras on surface vehicles

Waterloo Regional Police Service

- unmanned aerial vehicles privacy impact assessment

Health Privacy

New breach reporting requirements

2018 was the first full year of mandatory *PHIPA* breach reporting, bringing increased accountability and transparency to Ontario's health care sector.

With this new reporting requirement in full swing this year, the IPC saw a considerable increase in the number of self-reported breaches, which rose to 506 in 2018, from 322 in 2017. Of this year's self-reported breaches, 120 were snooping incidents, 15 were ransomware and cyberattacks, and the remaining 371 were due to lost, stolen or misdirected health information, records not properly secured and other collection, use and disclosure issues.

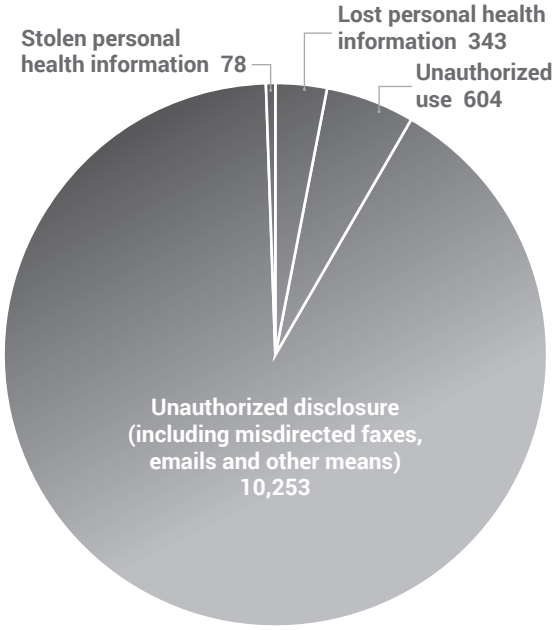
Self-reported privacy breaches

Snooping	120
Cyberattack	15
Other unauthorized collection, use and disclosure issues	371
Total	**506**

The marked increase in the number of snooping incidents reported was not necessarily an indication that snooping behaviours were on the rise. Custodians have increasingly effective methods of detection in place, and a growing number are turning to data analytics to monitor and audit health information systems for unauthorized access and other types of health privacy breaches. Also, custodians are now *required* to report breaches to the IPC, unlike in previous years where it was only strongly recommended to do so.

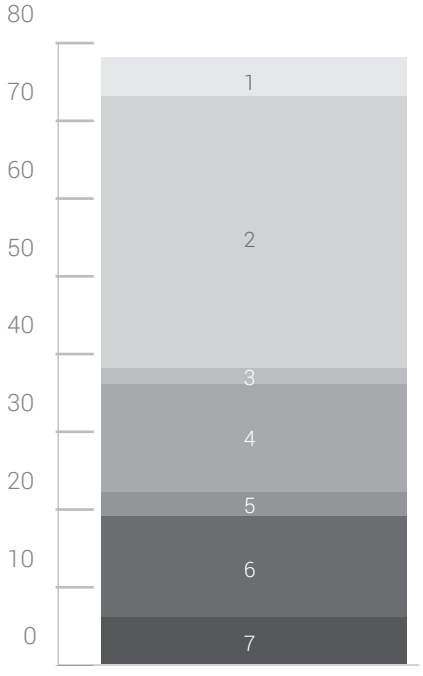
Overall, we were pleased with the high level of engagement from across Ontario's health sector. Custodians have an increasingly strong understanding of when, and in what circumstances, they must report breaches to the IPC and have responded to their new responsibilities with an obvious commitment to patient privacy.

HEALTH PRIVACY BREACHES BY CAUSE



Statistical reporting

As part of the new requirements under *PHIPA*, health information custodians were required to submit annual breach statistics to our office. Over 800 custodians



STOLEN PERSONAL HEALTH INFORMATION

1. Theft by an internal party (e.g. employee, affiliated health practitioner or electronic service provider): **5**
2. Theft by a stranger: **35**
3. Theft the result of a ransomware attack: **2**
4. Theft the result of another type of cyberattack: **14**
5. Unencrypted portable electronic equipment (e.g. USB keys, laptops) stolen: **3**
6. Paper records stolen: **13**
7. Theft a result of something else, by someone else or other items stolen: **6**

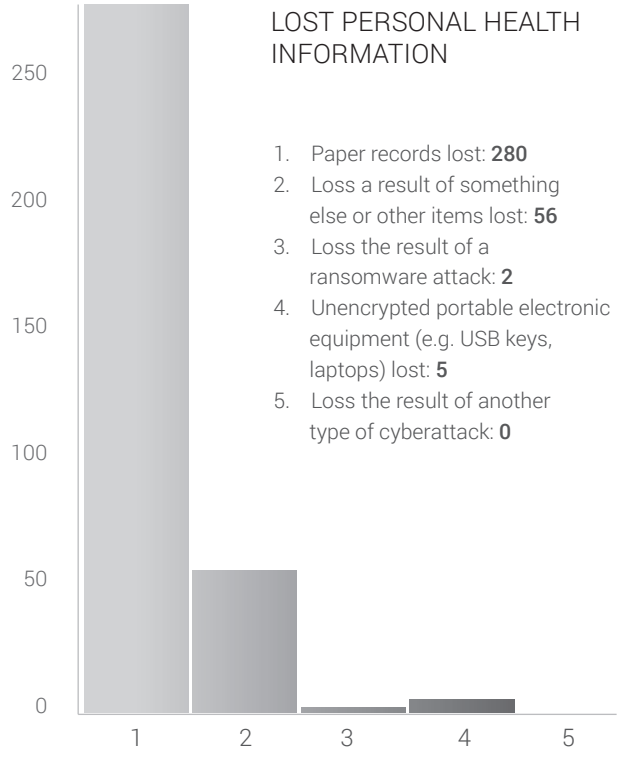
submitted reports on thefts, losses, and unauthorized uses or disclosures of personal health information, including those breaches that did not meet the threshold for reporting to the IPC at the time of the incident.

There were 11,278 incidences of personal health information breaches in 2018. Of those, over 10,000 were breaches involving unauthorized disclosure due to misdirected faxes, emails and other means.

Cyberattacks – a growing concern in health care

Cyberattacks have dominated the news in recent years, disrupting organizations in every industry and sector. In 2018, Ontario's health care sector was also a prime target: from local health integration networks to long-term care facilities, a growing number of custodians were victims of ransomware and other cyberattacks.

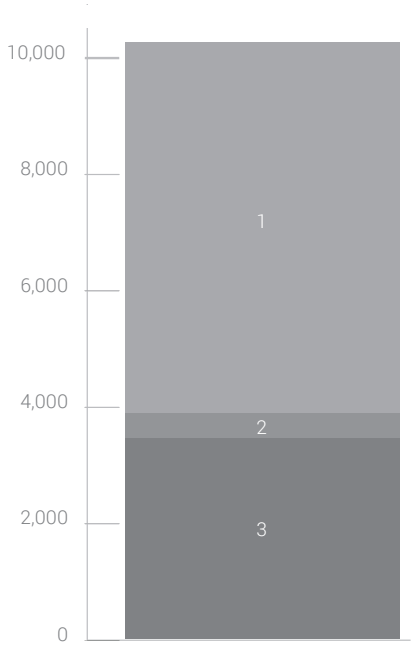
In June, CarePartners and the Central Local Health Integration Network notified the IPC of a cyberattack which resulted in a health privacy breach and sparked an investigation. Since then, the IPC has worked with both organizations to determine the extent to which health information was exposed, address weaknesses in the system and prevent future attacks.



LOST PERSONAL HEALTH INFORMATION

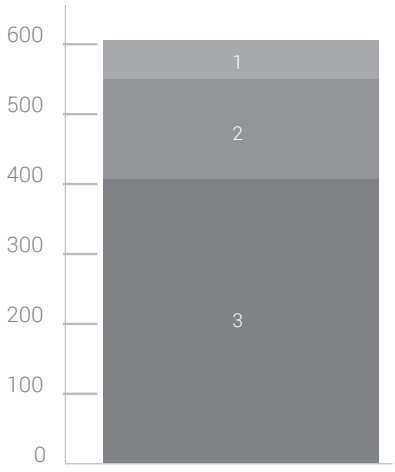
1. Paper records lost: **280**
2. Loss a result of something else or other items lost: **56**
3. Loss the result of a ransomware attack: **2**
4. Unencrypted portable electronic equipment (e.g. USB keys, laptops) lost: **5**
5. Loss the result of another type of cyberattack: **0**

Much of this work underscored the importance of employee training and awareness of the serious threat posed by ransomware, the tangible benefits of regular data backups of electronic files and the significant value of antivirus software that helps prevent, detect and remove malware through regular, real-time scans. The work also focused on the need for robust privacy policies and ensuring that custodians' audit solutions met industry standards.



UNAUTHORIZED DISCLOSURE

1. Unauthorized disclosure through misdirected faxes: **6,381**
2. Unauthorized disclosure through misdirected emails: **434**
3. Unauthorized disclosure through other means: **3,438**



UNAUTHORIZED USE

1. Unauthorized use through other records: **55**
2. Unauthorized use through paper records: **144**
3. Unauthorized use through electronic systems: **405**

Ransomware attacks can stop custodians in their tracks and affect the delivery of health care services. The IPC remains committed to helping the health care sector foil phishing and other types of malicious attacks so that custodians can protect patient privacy and meet their security obligations under the law.

PHIPA and artificial intelligence – a success atory

Patient privacy is part of the fabric of Ontario's health care sector. To this end, *PHIPA* sets the rules for how custodians and their agents may collect, use and disclose personal health information. Among other things, these rules prohibit unauthorized access to patients' health information, a pervasive privacy issue in health care settings. In the age of artificial intelligence and big data analytics, however, detecting and deterring unauthorized access and other types of privacy breaches is becoming easier to do.

In 2018, the IPC participated in a steering committee that resulted in the procurement of a smart auditing tool by Mackenzie Health. During a six-month pilot, the tool used big data analytics and artificial intelligence to study Mackenzie Health's workflows and privacy policies to determine appropriate accesses to health information and flag unexplained accesses for follow-up.

This auditing solution specifically focused on explaining accesses to a patient's health information by making an intelligent connection between the patient and staff who accessed the information. While Mackenzie Health detected numerous breaches in the initial stages of the pilot, the numbers decreased significantly as the solution was refined and more information, such as staff roles and schedules, was incorporated into the tool.

The pilot's findings were impressive. The results showed that the majority of the accesses were appropriate, while approximately two per cent were unexplained. With the addition of an even higher quality of input data and increased staff awareness, more accurate and sophisticated explanations for access are expected from this auditing tool in the future.

The IPC supports the rollout of this innovative and proactive solution across Ontario's health sector to help custodians better detect and minimize the risk of unauthorized access and improve patient privacy.

SUMMARY OF *PHIPA* COMPLAINTS

+28%	+21%	+57%	-19%
ACCESS/CORRECTION OPENED	**COLLECTION/ USE/DISCLOSURE OPENED**	**SELF-REPORTED BREACH OPENED**	**IPC INITIATED OPENED**
2018 199 2017 155	**2018 127** 2017 105	**2018 506** 2017 322	**2018 38** 2017 47
-2%	+1%	+41%	-26%
ACCESS/CORRECTION CLOSED	**COLLECTION/ USE/DISCLOSURE CLOSED**	**SELF-REPORTED BREACH CLOSED**	**IPC INITIATED CLOSED**
2018 160 2017 164	**2018 103** 2017 102	**2018 430** 2017 305	**2018 34** 2017 46

Video surveillance in long-term care settings

Throughout 2018, the IPC was regularly asked about the use of granny cams, a term that is commonly used to describe video surveillance systems installed by patients or their family members, most often in long-term care homes and out of concern for a resident's health or safety.

Ontario's health and public sector privacy laws generally do not apply to granny cams used in these situations. Nonetheless, all long-term care residents have a right to privacy, especially since a camera in a resident's room may record sensitive information about them, other residents, family members and visitors.

At a minimum, the IPC believes that granny cams should only be installed with the consent of the resident or their substitute decision-maker and the camera's view should specifically be limited to the resident's personal space.

Health privacy complaints resolved without formal review

Our office strives to resolve health privacy complaints at the intake stage, or through mediation, without the need for a formal review. Below are some of the cases closed through early resolution in 2018.

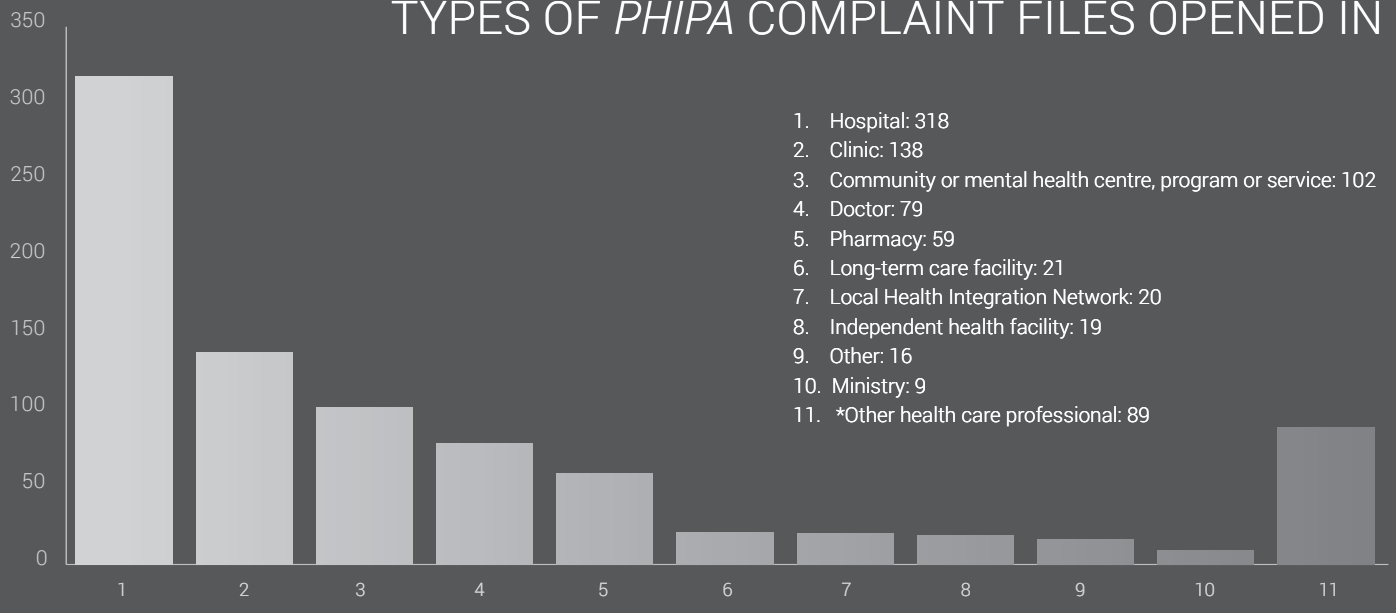
A hospital and a "code red" video

A hospital reported that three security officers employed by a security contractor and two registered practical nurses accessed a video of a "code red" incident without authorization. The hospital took several measures to address the breach and reduce the likelihood of a reoccurrence. These measures included restricting access to archived surveillance videos to the manager of security, and requiring additional privacy training and confidentiality oaths. The IPC was satisfied with the hospital's response to the breach.

Cyberattack at a family health team

A family health team reported to the IPC that it was the target of a cyberattack. Although the hacker did not seize any data, it encrypted the files so the health team could not access them. The health team was able to restore most of its data from backup files and intended to repopulate the rest of the data through chart reviews. In response

TYPES OF *PHIPA* COMPLAINT FILES OPENED IN 2018



* Respondent types representing less than one per cent of complaint files opened are not separately listed; information about a particular respondent type not shown is available on request.

to the attack, the health team implemented additional security measures, including blocking or quarantining emails from outside its organization with certain attachments. The IPC was satisfied with the steps taken by the health care team to respond to the breach and prevent future attacks.

A snooping receptionist

A patient complained to a medical clinic that its receptionist accessed and disclosed sensitive personal health information. The clinic investigated the complaint and reported the breach to the IPC. Its investigation confirmed that the receptionist had inappropriately accessed the personal health information of two patients known to her. As a result, the clinic dismissed the employee. The clinic took several steps to respond to the breach, requiring additional privacy training by all staff and changing the way that visits to the clinic are described in the appointment schedule. The IPC was satisfied with the clinic's response to the privacy breach.

Access to a deceased family member's information

An individual sought information from a hospital about his deceased father, stating that he required this information to make decisions about his health care. The hospital refused to disclose any of this information to the individual, who filed a complaint with the IPC. Our office worked with the parties to confirm that requester needed his deceased father's information to make decisions about his health care. The hospital agreed to revisit their original decision, and ultimately released the requested information to the individual's doctor.

Report to a children's aid society by a hospital nurse

An individual complained that a hospital nurse inappropriately reported her to a children's aid society, and in doing so, disclosed the complainant's personal health information. The hospital explained that its policy requires staff to notify the appropriate child welfare agency in cases of real or suspected child abuse. The IPC was satisfied that the health information custodian's disclosure to a children's aid society was permitted under *PHIPA*. Moreover, the requirement under the *Child, Youth and Family Services Act* to report a child in need of protection overrides privacy rules under *PHIPA*.

Significant *PHIPA* investigations and decisions

The IPC conducts investigations and may review and issue decisions on matters related to access to and correction of health information, as well as the privacy of that information. The following are some investigations and *PHIPA* decisions from 2018.

Surveillance camera in exam room

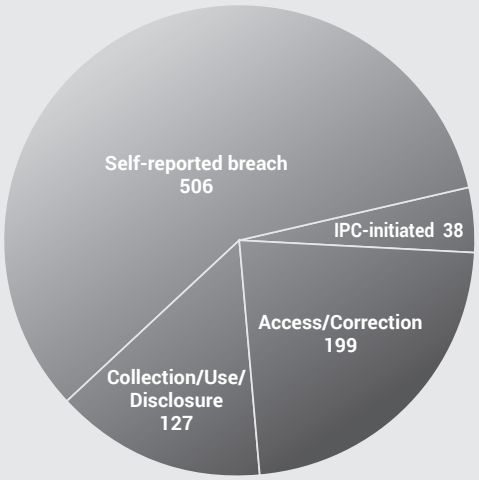
Towards the end of the year, our office received a call from a media outlet after they discovered a cosmetic surgeon's office had a security camera in an exam room. The camera was recording patient-staff interactions. In his interview, the commissioner expressed strong concerns about this use of video surveillance, noting, "each day in Ontario, tens of thousands of patients have an interaction with a health care professional … if every one of those health care practitioners decided to put a surveillance camera in their clinical room for legal liability reasons, that would be totally unacceptable." The investigation is still in progress.

Access under both *PHIPA* and *FIPPA*

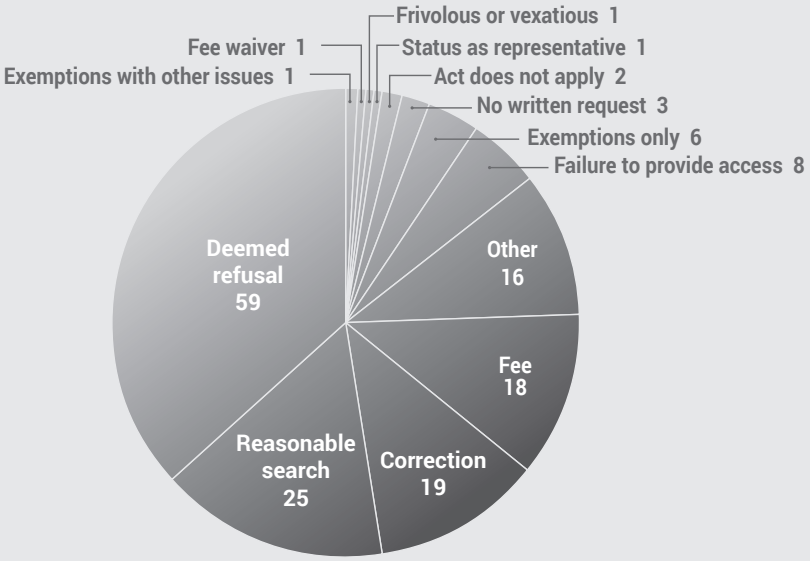
When an access request is made to an entity that is covered by both *PHIPA* and *FIPPA*, there may be rights of access under each law. In such cases, the IPC generally considers the extent of any right of access under *PHIPA* first, before considering any right of access under *FIPPA*.

In *PHIPA* Decision 73, a requester sought access to communications between a hospital and external parties about a relative who had been a patient at the hospital. The IPC found that under *PHIPA*, the requester was entitled to access the relative's personal health information. Further, the IPC decided that the requester was entitled to the rest of the record, under *FIPPA*.

SUMMARY OF *PHIPA* COMPLAINTS OPENED



ACCESS/CORRECTION COMPLAINTS CLOSED BY ISSUE



Correction of professional opinions not required

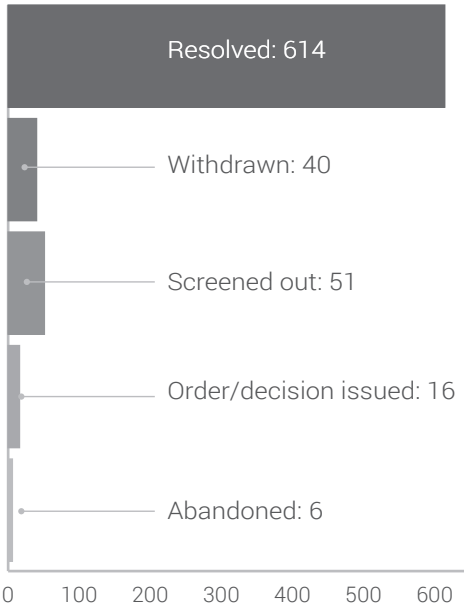
Ontario's health privacy law is patient-centric, giving Ontarians a number of rights, including the right to request a correction of their health information if they believe it to be incomplete or inaccurate for the custodian's purposes. Custodians can only deny such requests in specific circumstances. For example, they are not required to change professional opinions or medical observations that they made in good faith.

This decision involved a complainant who submitted a 62-part correction request to the Toronto Central Local Health Integration Network. Two of the requests were granted, but the remainder were denied because the complainant did not show that the information was incomplete or inaccurate for the purposes for which it is used, because the information consisted of professional opinions made in good faith. The IPC agreed with the TCLHIN and decided it was not required to make the corrections.

Unauthorized disclosure of health information to an estranged spouse

Except in certain circumstances, *PHIPA* prohibits custodians from disclosing a patient's health information to someone other than the patient without the express consent of that patient. To do so would constitute a privacy breach. In *PHIPA* Decision 68, the IPC found that a clinic failed to protect the complainant's health information after it disclosed it to her estranged husband without her consent, breaching its security obligations under the law. We ordered the clinic to review and revise its privacy policy and train its staff on their privacy obligations under *PHIPA*.

OUTCOME OF *PHIPA* COMPLAINTS CLOSED



Commissioner's Recommendations

Oversight of political parties

In my 2017 annual report, I called on the government to amend Ontario's privacy laws to include political parties. I renewed this call earlier this year, on a national level, with my counterparts from across Canada. I call on the government, once again, to address this very real privacy concern.

The large amount of sensitive personal information held by political parties, coupled with advances in the technologies enabling them to collect, integrate and analyze data in ways that we could not have previously imagined, reveals a widening gap in protection and oversight of individual privacy rights. Voters do not have the legal right to know if their information is collected from or shared with other parties, political interest groups or data mining organizations.

The need for transparency and oversight is clear. Increasingly sophisticated data practices, often undertaken without voters' knowledge or consent, can be used to target individuals and communities, manipulate public opinion and influence election outcomes. As hackers become more sophisticated and cyberattacks more common among public institutions, the risk of breaches, both intentional and through human error, rises. Because political parties work outside of privacy laws, there is little recourse for those affected by privacy breaches.

Ontario's political parties must be accountable for the privacy, ethical and security risks associated with how they collect, use, and disclose our personal information.

Smart city projects have the potential to unlock many benefits for communities. However, the enhanced use of data and technology must not come at the expense of privacy.

The most effective way of doing that is by making them subject to the privacy requirements set out in Ontario's access and privacy laws. Amendments to legislation to provide regulation and oversight would demonstrate a commitment to public accountability, and respect for individual privacy.

Smart cities

Smart cities dominated much of the news in Ontario in 2018. Data governance and protection of individual privacy rights were central to the debate; one of the major catalysts for this discussion was Toronto's Quayside initiative. Commentators have raised questions about potential gaps in the applicable privacy laws, including enforcement powers and transparency.

We have been following the public discourse on proposed data governance frameworks to address these gaps.

I believe that smart city projects have the potential to unlock many benefits for communities. However, the enhanced use of data and technology must not come at the expense of privacy.

Together, Ontario's municipal access and privacy law and the applicable private sector privacy law provide a foundation to allow us to realize the benefits of these technologies without sacrificing individual privacy. To comply with these laws, and to ensure the right of the public to know how their information is being collected, used, and disclosed, privacy cannot be an afterthought. From proposal to launch, measures to ensure compliance with our laws and best practices that protect the privacy and security of citizens must be front and centre in smart city projects.

While *MFIPPA* provides a foundation for privacy protections, it is outdated in the face of current digital technologies and practices such as sensors, big data analytics, and artifi-

cial intelligence. Therefore, I recommend that the Ontario government lead a comprehensive review of our privacy laws and modernize them to address the risks inherent in smart city technologies. This work should ensure that any new governance framework includes effective and independent oversight of practices related to personal information.

As municipalities plan and launch their smart city initiatives, I also recommend that they conduct thorough privacy impact assessments. Where projects involve complex privacy considerations, I recommend consultation with our office. Community engagement must also remain a priority because helping the public understand how smart city technologies might affect them increases transparency and builds public trust.

Artificial intelligence to curb unauthorized access

2018 was the first year of mandatory health privacy breach reporting by health information custodians in Ontario. My office received 506 reports, 120 of which cited unauthorized access as the cause. Snooping remains a persistent problem. However, I see evidence of a strong, sector-wide commitment to address the problem of unauthorized access and increasing sophistication of the tools used to detect it.

In the health privacy section of this annual report, we describe the IPC's work with Mackenzie Health on the development of its Privacy Auditing Innovation Procurement pilot. In this pilot, artificial intelligence technology was used to detect and interpret network activity in ways that would not be possible through manual auditing and other preventative mechanisms.

I am encouraged to see the results of the pilot and would like to see widespread use of the AI model across the health sector to enable efficient detection, improve the accuracy of results and address the ongoing problem of unauthorized access.

I expect as the appropriate and ethical use of AI becomes more widespread we will see a reduction in the number and frequency of personal health information breaches across Ontario.

When deployed properly, technology that identifies anomalous behaviour is a valuable tool for health information custodians, to not only detect and deter unauthorized snooping but to immediately identify and respond to cybersecurity threats.

When deployed properly, technology that identifies anomalous behaviour is a valuable tool for health information custodians, to not only detect and deter unauthorized snooping but to immediately identify and respond to cybersecurity threats.

Final thought

The 2018 statistics reveal that of the over 11,000 health information privacy breaches reported, over 6,000 were due to misdirected faxes. This is unacceptable when there are less error-prone, more secure methods of communication available.

In 2019, the Health and Social Care Secretary in the United Kingdom banned the National Health Service from buying fax machines and intends to phase out their use by March 2020. It is time for Ontario to follow this lead and implement a strategy to eliminate or reduce dependence on fax machines in the delivery of health care.

Statistics

YEAR AT A GLANCE

PROVINCIAL

PERSONAL INFORMATION	GENERAL RECORDS	TOTAL
+14%	-7%	-0.5%
REQUESTS	**REQUESTS**	**TOTAL REQUESTS**
2018 8,221	**2018 15,487**	**2018 23,708**
2017 7,220	2017 16,605	2017 23,825
+6%	+3%	+4%
APPEALS OPENED	**APPEALS OPENED**	**TOTAL APPEALS OPENED**
2018 164	**2018 464**	**2018 628**
2017 154	2017 450	2017 604
-28%	+2%	-6%
APPEALS CLOSED	**APPEALS CLOSED**	**TOTAL APPEALS CLOSED**
2018 141	**2018 500**	**2018 641**
2017 196	2017 489	2017 685
+256%	+20%	
AVERAGE COST	**AVERAGE COST**	
2018 $14.31	**2018 $30.74**	
2017 $ 4.02	2017 $25.53	

MUNICIPAL

PERSONAL INFORMATION	GENERAL RECORDS	TOTAL
+1%	-8%	-4%
REQUESTS	**REQUESTS**	**TOTAL REQUESTS**
2018 18,670	**2018 16,434**	**2018 35,104**
2017 18,301	2017 17,681	2017 35,982
+20%	-2%	+3%
APPEALS OPENED	**APPEALS OPENED**	**TOTAL APPEALS OPENED**
2018 233	**2018 581**	**2018 814**
2017 194	2017 594	2017 788
+8%	+9%	+8%
APPEALS CLOSED	**APPEALS CLOSED**	**TOTAL APPEALS CLOSED**
2018 210	**2018 580**	**2018 790**
2017 195	2017 534	2017 729
+4%	-9%	
AVERAGE COST	**AVERAGE COST**	
2018 $10.37	**2018 $22.20**	
2017 $ 9.92	2017 $24.50	

SUMMARY OF *PHIPA* COMPLAINTS

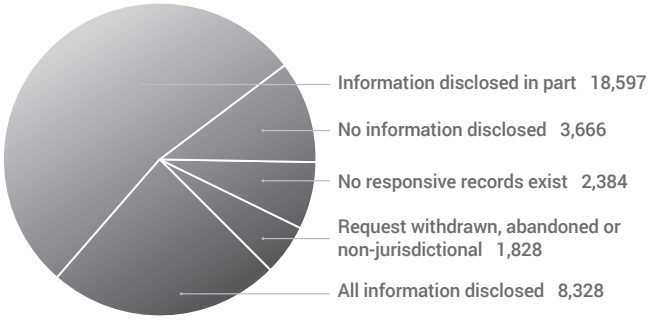
+28%	+21%	+57%	-19%
ACCESS/CORRECTION OPENED	**COLLECTION/ USE/DISCLOSURE OPENED**	**SELF-REPORTED BREACH OPENED**	**IPC INITIATED OPENED**
2018 199	**2018 127**	**2018 506**	**2018 38**
2017 155	2017 105	2017 322	2017 47
-2%	+1%	+41%	-26%
ACCESS/CORRECTION CLOSED	**COLLECTION/ USE/DISCLOSURE CLOSED**	**SELF-REPORTED BREACH CLOSED**	**IPC INITIATED CLOSED**
2018 160	**2018 103**	**2018 430**	**2018 34**
2017 164	2017 102	2017 305	2016 46

PRIVACY COMPLAINTS

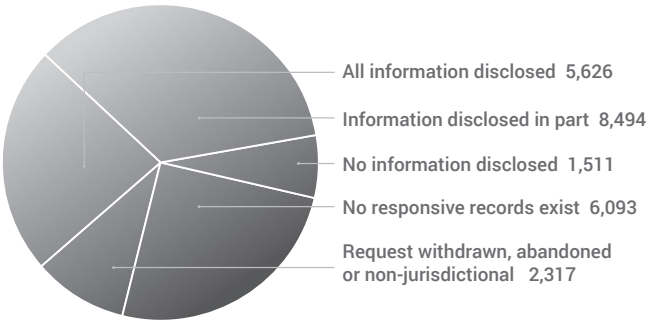
PROVINCIAL	MUNICIPAL
+21%	+9%
OPENED	**OPENED**
2018 134	**2018 172**
2017 110	2017 158
-4%	-7%
CLOSED	**CLOSED**
2018 109	**2018 148**
2017 114	2017 159

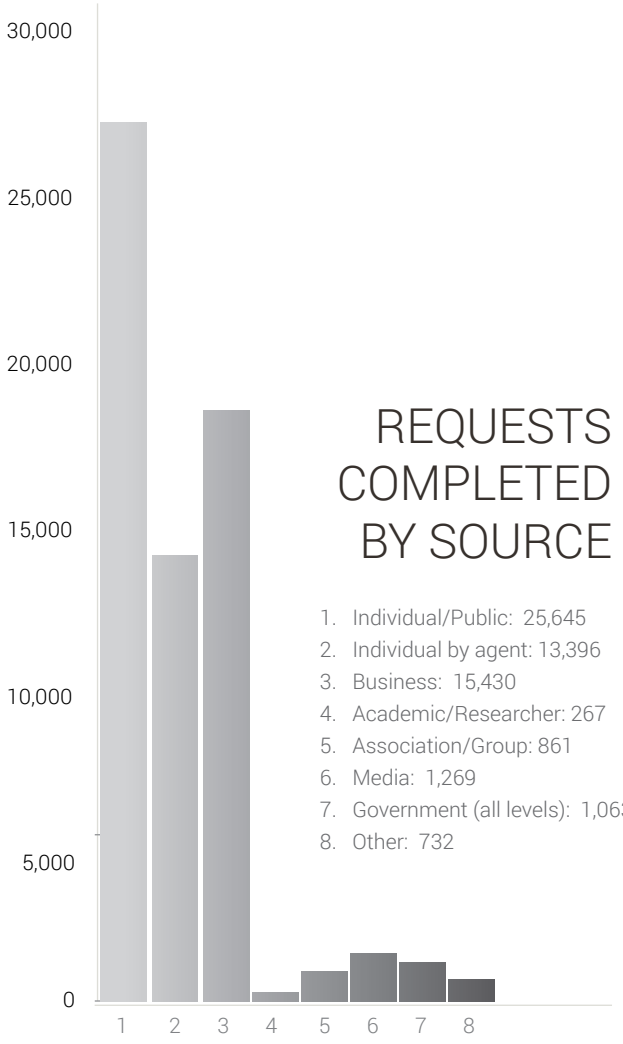
OVERALL REQUESTS

OUTCOME OF REQUESTS: MUNICIPAL



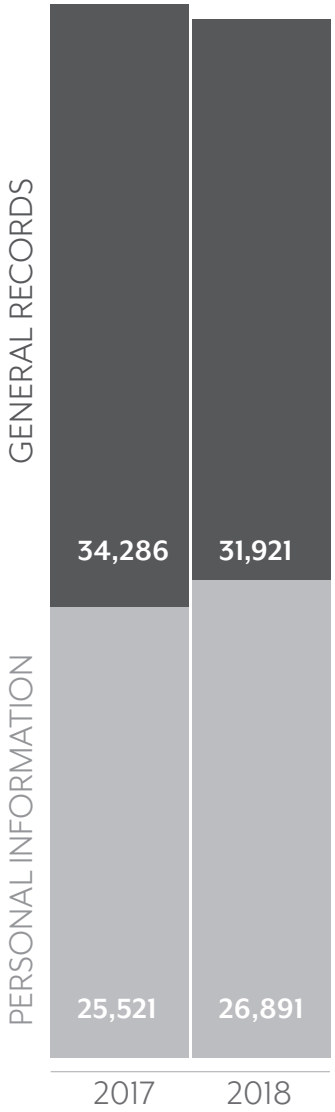
OUTCOME OF REQUESTS: PROVINCIAL





REQUESTS COMPLETED BY SOURCE

1. Individual/Public: 25,645
2. Individual by agent: 13,396
3. Business: 15,430
4. Academic/Researcher: 267
5. Association/Group: 861
6. Media: 1,269
7. Government (all levels): 1,063
8. Other: 732



TOTAL

-2%

REQUESTS
2018 58,812
2017 59,807

GENERAL RECORDS

-7%

REQUESTS
2018 31,921
2017 34,286

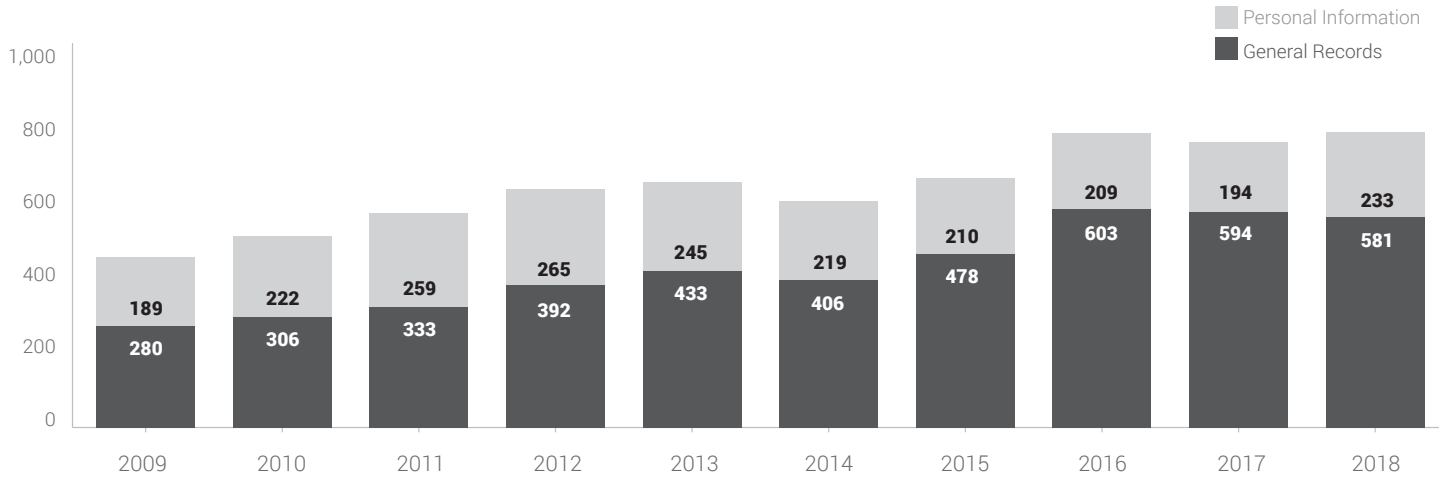
PERSONAL INFORMATION

+5%

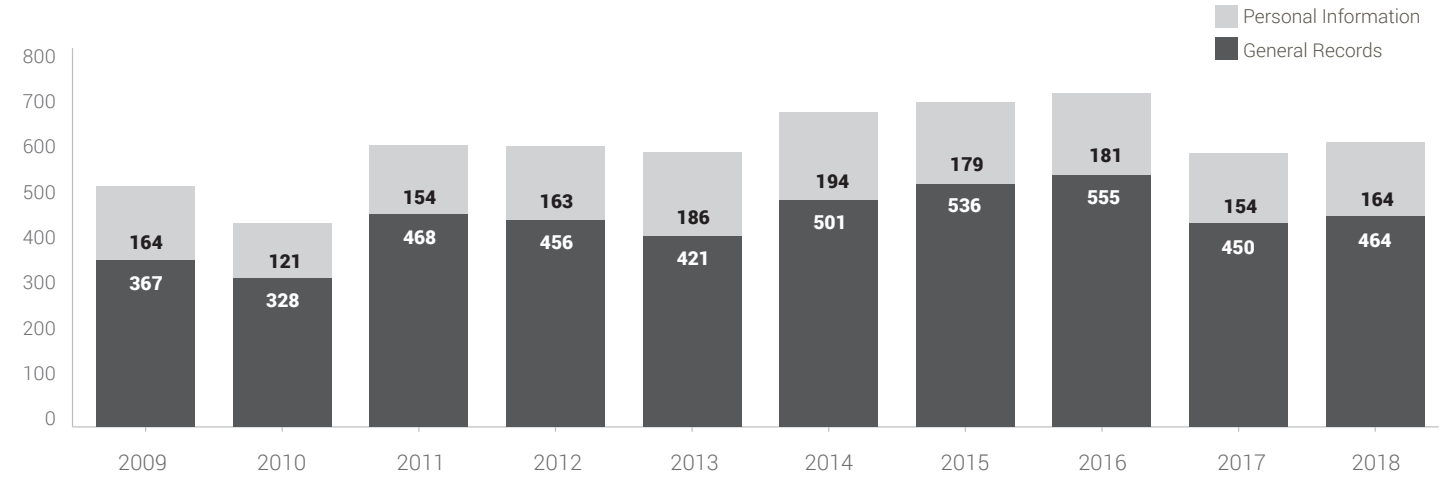
REQUESTS
2018 26,891
2017 25,521

Statistics

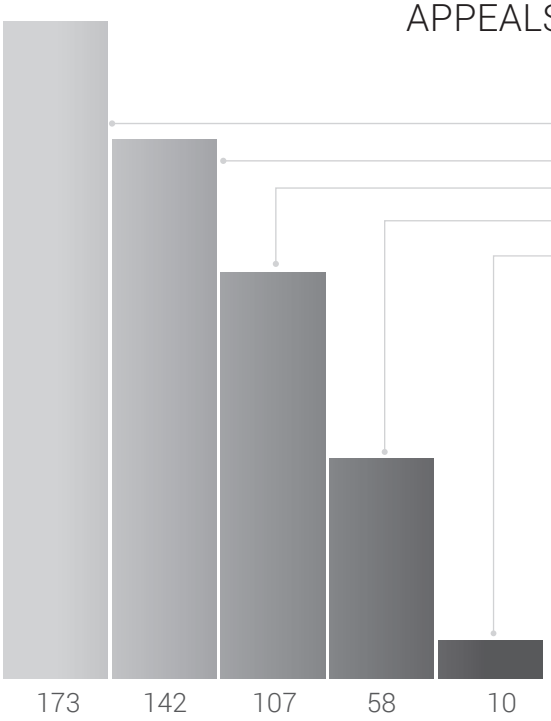
NUMBER OF MUNICIPAL APPEALS OPENED 2009-2018



NUMBER OF PROVINCIAL APPEALS OPENED 2009-2018

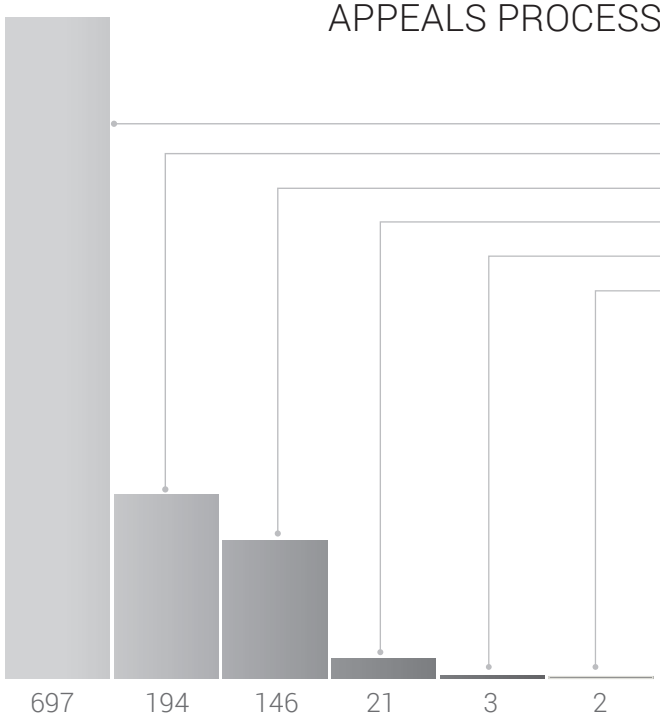


APPEALS PROCESSED* IN INTAKE BY DISPOSITION



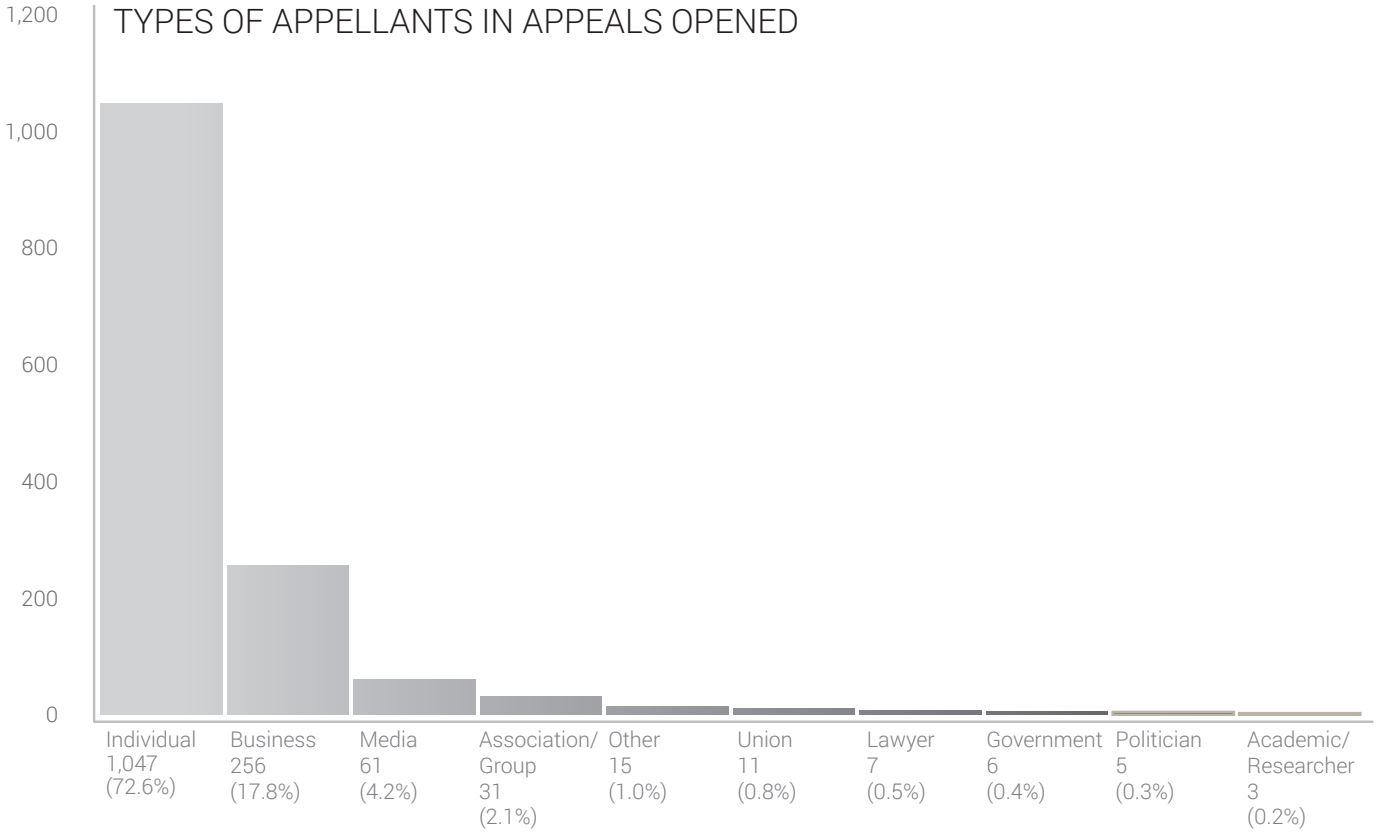
* "Processed" refers to those files that completed the intake stage somewhere between January 1, 2018 and December 31, 2018 and includes files that are still open in the mediation and adjudication stages

APPEALS PROCESSED IN MEDIATION BY DISPOSITION*

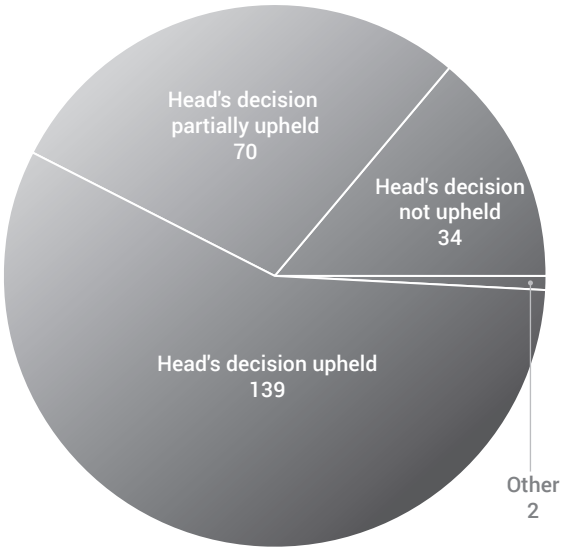


* These orders arise out of time extension appeals in which a mediator can act as an adjudicator and issue an order.

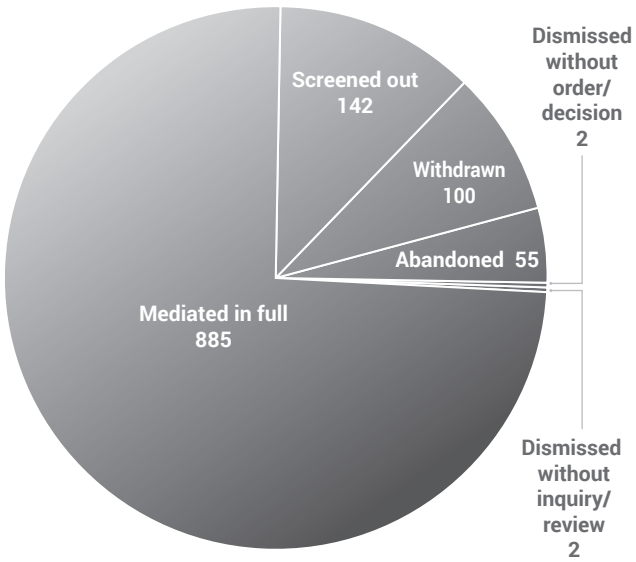
Statistics



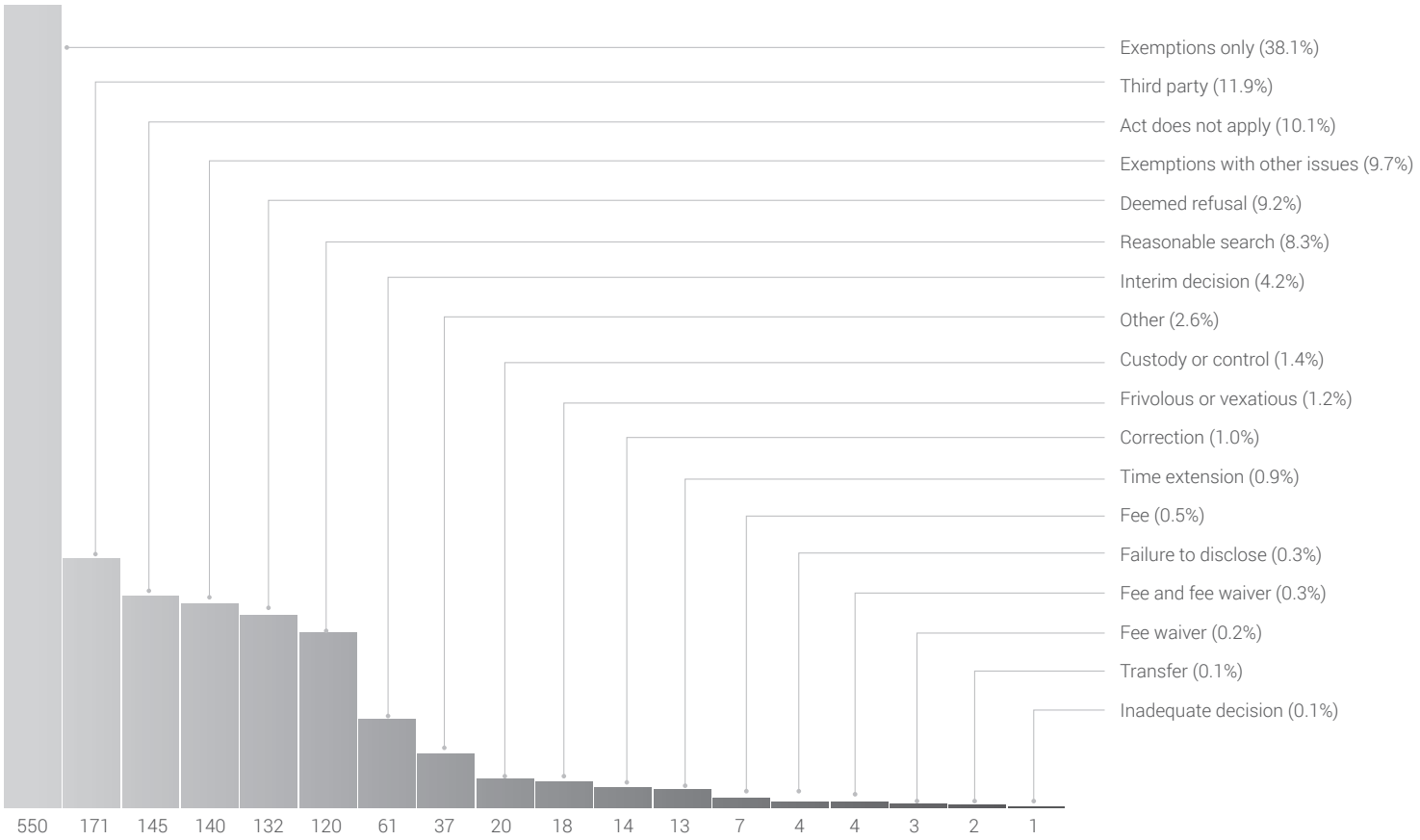
NUMBER OF APPEALS CLOSED BY ORDER, BY ORDER OUTCOME



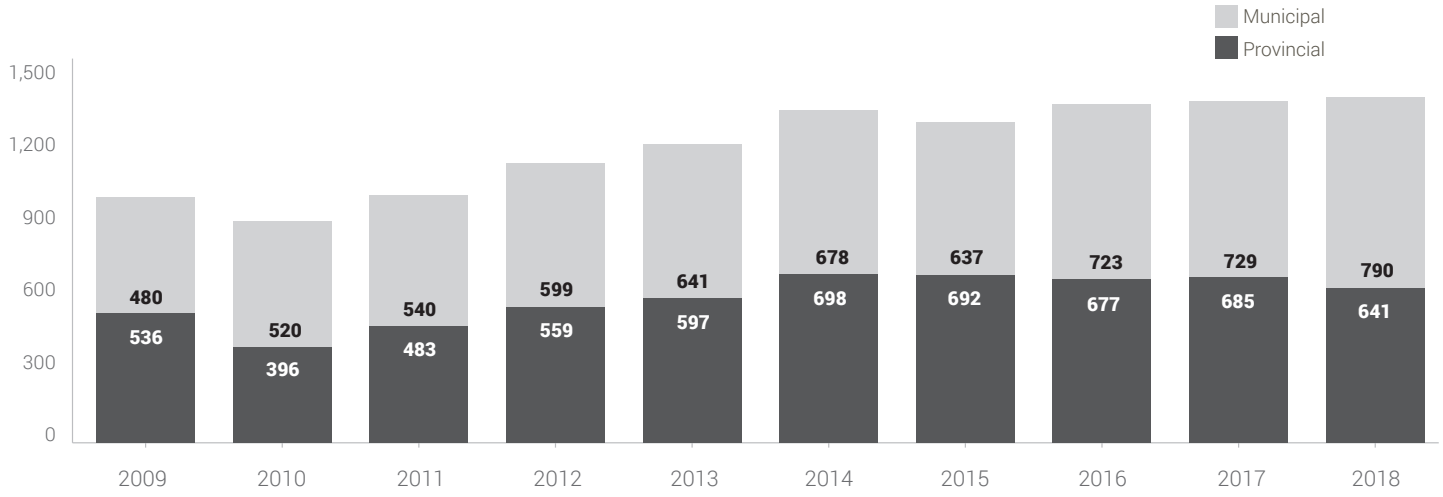
NUMBER OF APPEALS CLOSED OTHER THAN BY ORDER, BY OUTCOME



ISSUES IN APPEALS OPENED



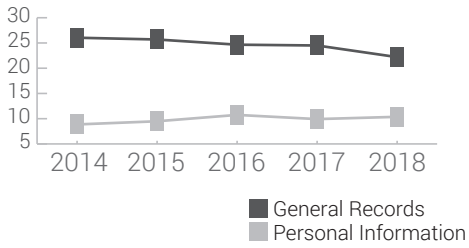
NUMBER OF APPEALS CLOSED 2009-2018



Statistics

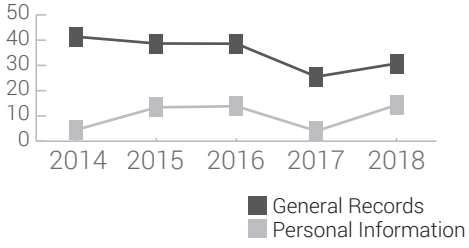
AVG COST OF MUNICIPAL REQUESTS

PERSONAL INFORMATION	GENERAL RECORDS
$10.37	$22.20



AVG COST OF PROVINCIAL REQUESTS

PERSONAL INFORMATION	GENERAL RECORDS
$14.31	$30.74



TOTAL FEES COLLECTED AND WAIVED

MUNICIPAL	PROVINCIAL	TOTAL
$172,959.88 TOTAL APPLICATION FEES COLLECTED	$116,783.52 TOTAL APPLICATION FEES COLLECTED	$289,743.40 TOTAL APPLICATION FEES COLLECTED
$377,399.30 TOTAL ADDITIONAL FEES COLLECTED	$493,244.75 TOTAL ADDITIONAL FEES COLLECTED	$870,644.05 TOTAL ADDITIONAL FEES COLLECTED
$550,359.18 TOTAL	**$610,028.27** TOTAL	**$1,160,387.45** TOTAL
$49,694.66 TOTAL FEES WAIVED	$18,942.95 TOTAL FEES WAIVED	$68,637.61 TOTAL FEES WAIVED

Financial Statement

	2018-2019 Estimates $	2017-2018 Estimates $	2017-2018 Actual $
SALARIES AND WAGES	13,404,400	13,404,400	11,463,811
EMPLOYEE BENEFITS	3,217,000	3,083,600	2,267,209
TRANSPORTATION AND COMMUNICATIONS	286,700	286,700	190,399
SERVICES	2,475,900	3,123,900	3,532,565
SUPPLIES AND EQUIPMENT	322,000	489,000	772,372
TOTAL	**19,706,000**	**20,387,600**	**18,226,356**

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.

2018 APPEALS FEES DEPOSIT

(Calendar year)

GENERAL INFORMATION	PERSONAL INFORMATION	TOTAL
$17,190	$3,365	$20,555

2018

ANNUAL REPORT

Office of the Information and Privacy Commissioner of Ontario

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

www.ipc.on.ca