



THE VISION OF A MODERN AND EFFECTIVE REGULATOR

2022

ANNUAL REPORT



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 7, 2023

The Honourable Ted Arnott

Speaker of the Legislative Assembly of Ontario

Dear Mr. Speaker,

I am pleased and honoured to share with you the IPC's 2022 annual report, *The Vision of a Modern and Effective Regulator*. It covers the period from January 1 to December 31, 2022, providing a summary of notable activities, initiatives, and recommendations from the past year.

As an organization that aspires to be a modern and effective regulator, the IPC is committed to working toward real world outcomes that benefit Ontarians. We strive to enhance Ontarians' trust that their privacy and access rights will be respected by: proactively advancing their rights in key strategic areas that impact their lives; addressing their complaints and appeals in a fair, timely and meaningful manner; and maintaining their confidence in the organizational excellence of the IPC.

Our work in 2022 resulted in noteworthy advancements for access and privacy rights in Ontario. This report provides an overview of our activities and accomplishments over the past year, highlighting our commitment to protect and promote the privacy and access rights of Ontarians.

Additional information, including statistics, analysis, and supporting documents is available on our website at www.ipc.on.ca/about-us/annual-reports.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Patricia Kosseim', with a stylized flourish underneath.

Patricia Kosseim

Information and Privacy Commissioner of Ontario



IN THIS REPORT

Commissioner's message	02
IPC vision	04
Advocacy	
Privacy and transparency in a modern government	08
Children and youth in a digital world	10
Trust in digital health	14
Next-generation law enforcement	18
Responsiveness	
Reducing the file backlog	22
Notable tribunal trends	23
Notable examples of cases	23
Accountability	
Transform the IPC into a modern, digital organization	28
IPC as an employer of choice	28
Strengthen IPC governance and accountability	29
Compliance	30
IPC outreach by the numbers	35
IPC's year in summary	36
Statistical highlights	38
Organizational chart	44
Financial summary	45



COMMISSIONER'S MESSAGE

Throughout my career, I have had the honour of working with different regulators who shoulder great responsibility for ensuring compliance with privacy and access laws in a rapidly evolving digital world. I have also worked with public institutions who must implement requirements in the real world, as well as astute practitioners who have a very practical sense of the opportunities and challenges at play, academics who have devoted their careers to advancing knowledge in this critical field, and dedicated civil society groups who play such a vital role in advancing access and privacy rights for the benefit of us all.

This broad experience has taught me to listen to and appreciate the many diverse perspectives that come to bear on the complex issues we deal with. It has instilled a sense of humility with which I approach my work and a natural inclination to consult and collaborate with others to reach pragmatic solutions with beneficial impacts.

This is why, when I began my mandate as Information and Privacy Commissioner of Ontario, I came with a vision of a modern and effective regulator dedicated to supporting compliance and promoting public trust in our public institutions.

To achieve this vision, my office aims to be consultative and constructive in our engagement with institutions. Two thousand twenty-two presented many such opportunities. We reached out to organizations in the sectors we regulate to let them know how they can tap into the IPC's access and privacy expertise as they develop new programs and initiatives by requesting a **policy consultation** with my office. When organizations proactively engage with us, we can better understand their realities, provide comment on the adoption and deployment of new technologies, and help address potential concerns upstream before they become real problems downstream.

Being a modern and effective regulator also means being well-measured and balanced in our interventions and taking a risk-based approach to our oversight role. Our role is not just to make orders and wield fines and penalties when problems occur, but to help organizations learn from their

This broad experience has taught me to listen to and appreciate the many diverse perspectives that come to bear on the complex issues we deal with. It has instilled a sense of humility with which I approach my work and a natural inclination to consult and collaborate with others to reach pragmatic solutions with beneficial impacts.”

mistakes and prevent them from recurring. This practical and proportionate approach to our regulatory role was exemplified in our **review** of a regional hospital's high number of privacy breaches due to misdirected faxes, our **collaborative efforts with a government ministry** to address their unique freedom of information challenges and our **response** to a serious cyberattack at a regional municipality.

To realize our vision of a modern and effective regulator, the IPC is committed to working toward real-world outcomes that benefit Ontarians. Our **four strategic priorities** guide our proactive work and help keep us focused on the most relevant issues to Ontarians and in areas where we can have the greatest positive impact. Providing thought leadership and having influence in these novel and emerging areas requires bringing many great minds together and hearing from a plurality of external voices.

To help us do this, the IPC convened a permanent **Strategic Advisory Council**, composed of twenty-five privacy and access experts across all sectors we regulate. To ensure the voices of young people are also at the table, we recruited a new **Youth Advisory Council** to address the unique needs of Ontario's children and youth. In September 2022, we welcomed the IPC's **first Scholar-in-Residence**, Professor **Teresa Scassa**, Canada Research Chair in Information Law and Policy, at the University of Ottawa. This new program provides a unique opportunity for thought leaders like Professor Scassa to apply their extensive academic knowledge and expertise to concrete policy development in key priority areas.

As a modern and effective regulator, we must also strive to meet the highest standards Ontarians expect of us. With that objective in mind, we have worked extensively over the past year to provide digitally-friendly services to Ontarians while improving their user experience when interacting with our office. We have undertaken a review of our tribunal processes and procedures and developed a concrete plan to enhance our capacity to provide timely resolution to appeals and complaints, render plain-language decisions, and develop practical and actionable guidance by drawing on lessons learned from individual cases for the benefit of others.

Finally, in our journey to becoming a modern and effective regulator, we have introduced innovations into our own workplace. We're modernizing how we work and using online collaborative tools to enhance employee engagement as part of our new reality of hybrid work. We have ensured best practices in fiscal management, comptrollership, and internal governance to strengthen our accountability to the people we serve.

As we reflect on the past year, I would like to express my sincere gratitude to my staff. Their in-depth knowledge, hard work and dedication have been instrumental in achieving our goals and advancing our mission.

Our work in 2022 resulted in noteworthy advancements for access and privacy rights in Ontario. This report provides an overview of our activities and accomplishments over the past year, demonstrating our commitment to protect and promote the privacy and access rights of Ontarians.



Patricia Kosseim

Information and Privacy Commissioner of Ontario



IPC VISION

TO BE A MODERN AND EFFECTIVE REGULATOR

MISSION

ENHANCE ONTARIANS' TRUST THAT THEIR PRIVACY AND

GOALS



Proactively advancing their rights in key strategic areas that impact their lives



Advance Ontarians' privacy and transparency rights in a modern government by working with public institutions to develop bedrock principles and comprehensive governance frameworks for the responsible and accountable deployment of digital technologies.



Champion the access and privacy rights of Ontario's children and youth by promoting their digital literacy and the expansion of their digital rights while holding institutions accountable for protecting the children and youth they serve.



Contribute to building public trust in next-generation law enforcement by working with relevant partners to develop necessary guardrails for the adoption of new technologies and community-based approaches that protect both public safety and Ontarians' access and privacy rights.



Promote confidence in digital health by guiding custodians to respect the privacy and access rights of Ontarians, and supporting the pioneering use of personal health information for research and analytics to the extent it serves the public good.

CROSS-CUTTING STRATEGIES

1. We will consider accessibility and equity issues to help reduce disparate outcomes for marginalized groups.
2. We will strive to be consultative and collaborative with relevant partners and stakeholders.

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.

REGULATOR WITH REAL-WORLD IMPACT

ACCESS RIGHTS WILL BE RESPECTED BY:



Addressing complaints and appeals in a fair, timely and meaningful manner



Provide timely resolution to Ontarians' access appeals and privacy complaints by defining and upholding applicable service standards.



Issue concise and plain language decisions that are fair and meaningful to the parties and support compliance with the law.



Support understanding of the law and participation in the IPC appeals process by publishing actionable guidance based on trends and lessons learned from individual cases.



Maintaining their confidence in the organizational excellence of the IPC



Transform the IPC into a digitally friendly organization by delivering services more effectively and efficiently online, while improving user experience.



Build the IPC into an employer of choice by attracting and retaining high quality talent and developing a positive corporate culture through enhanced employee programs and engagement.



Strengthen IPC governance and accountability through modern controllership best practices and prudent fiscal management.

zed communities.

3. We will develop the knowledge, skills, and capacity needed, both internally and externally, to advance IPC's goals.
4. We will be bold and aspirational in our vision, but also stay grounded in pragmatism.

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.



PRIVACY AND TRANSPARENCY IN A MODERN GOVERNMENT

Our goal is to advance Ontarians' privacy and access rights by working with public institutions to develop bedrock principles and comprehensive governance frameworks for the responsible and accountable deployment of digital technologies.



TRANSPARENCY CHALLENGE

On International Right to Know Day 2022, the IPC launched a **Transparency Challenge**, calling on public institutions subject to the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) to share their innovative programs that improve government transparency for the benefit of Ontarians.

We invited creative examples of programs that modernize and improve government transparency, promote civic engagement, and show how proactive disclosure and open data initiatives can have tangible and positive impacts. The Transparency Challenge provided a way to increase awareness and understanding of the benefits of proactive disclosure and open data in improving the day-to-day lives of Ontarians.

Institutions rose to the challenge and submitted many exciting and innovative projects. These submissions, from provincial ministries and agencies, municipalities, universities, and police services, were featured in a digital **Transparency Showcase**, unveiled in spring 2023. The showcase illustrates compelling examples to help encourage and inspire other public institutions toward greater openness and transparency.



FPT DIGITAL ID RESOLUTION

Proposals for digital identity or other forms of digital credentials are emerging in Canada and around the world to make it easier for individuals, businesses, and governments to confirm identity information and conduct online transactions more seamlessly and efficiently.

In October, the IPC joined its federal, provincial, and territorial counterparts to call on governments and relevant partners to ensure that privacy and transparency rights are respected throughout the design, operation, and evolution of digital identity ecosystems in Canada. **Privacy and transparency** must be at the core of any digital ID system people will trust and adopt. The **joint resolution** set out the conditions necessary for nurturing that trust. Among these conditions:



It means working for the common goals of providing access to information and encouraging privacy protective measures for Ontarians.”

Digital ID systems should be optional and equitably accessible to all. They should only collect, use, or share the minimum amount of personal information needed to confirm identity and must not be used to create any central databases. They shouldn't force people to identify themselves when it isn't necessary to access a product or service and must not allow tracking or tracing of credential use for other purposes.

These systems must be secured from identity theft, fraud or other harms, and, most importantly, governments and organizations must be held accountable for their use and subject to independent oversight.



TRUSTWORTHY AI FRAMEWORK

Rapid developments in artificial intelligence (AI) offer tremendous opportunities to address many of society's most complex problems across all sectors of society. AI technologies can be used to fast-track the delivery of government services, solve major public health issues, and reconfigure our cities. They can improve public safety, respond to global emergencies, enhance commercial innovation, and bolster our economy.

Yet, without appropriate guardrails, AI technologies risk crossing the lines beyond what Ontarians consider legally, socially, and ethically acceptable. Irresponsible uses of AI can trample privacy and other fundamental human rights by attempting to predict human behaviour and making consequential decisions based on potentially flawed predictions. AI technologies have begun generating new “machine-made” knowledge, images and voices that call into question the integrity and accuracy of information as we know it. They can persuade and nudge our behaviour in ways that can potentially jeopardize our fundamental sense of human agency. *(cont.)*

In July, Commissioner Kosseim wrote a blog, **Privacy and humanity on the brink**, outlining the risks inherent in too-rapidly adopting information technologies, especially when combined with biotechnologies, and the significant impacts these can have on our future generations.

In her blog, the commissioner urged the government to intensify its consultation efforts, particularly among marginalized groups and communities that are most impacted by algorithmic decision-making. She also called for increased investments into developing the capacity required to carry out privacy and human rights impact assessments. This includes practical educational guidance to support institutions and organizations in carrying out these assessments, funding for interdisciplinary research into the ethical, legal, and social impacts of AI, and foresight methodologies to anticipate and address future scenarios.

In 2021, the government considered an approach to govern public sector use of AI systems in a discussion paper, **Trustworthy Artificial Intelligence (AI) Framework**, to which our office **responded**. We urge the government to pursue its consultations on a trustworthy framework for AI and resume its leadership stance in this critically important area. A comprehensive legal or policy framework is urgently needed to govern public and private sector use of artificial intelligence within clear and transparent boundaries that align with Ontarians' rights and values, and, fundamentally, in a way that Ontarians can trust.

Being an IPC'er means taking pride in what I do. It means having the great privilege of working with smart, kind, and caring people, on fascinating issues, with common purpose and commitment to advance the public interest."



UPDATED RANSOMWARE GUIDANCE

In its National Cyber Threat Assessment 2023-2024, the Canadian Centre for Cyber Security cites ransomware as a continuing and persistent threat to Canadian organizations, particularly critical infrastructure used to support essential services like health and other government services. Ransomware is a type of malicious software or "malware." Once attackers gain access to an organization's systems, they can prevent an organization from accessing their data holdings and threaten to publish confidential data unless the organization pays the attackers a hefty fee.

In 2022, the Ontario government's Broader Public Sector Cyber Security Expert Panel released a **report** on the current state of cybersecurity in Ontario. The report highlights the range of cyber risks, including ransomware, facing the broader public service. With **risks increasing**, particularly for municipalities, universities, schools, and hospitals, the IPC updated its **ransomware guidance** to focus on new threats and the obligations to prevent, detect, and respond to attacks. It offers tips on how organizations can avoid falling for common traps through increased awareness and prevention. It also describes the many proactive steps organizations should take to strengthen their security posture and be in a good position to mitigate impacts of attacks when they happen.

Organizations must take reasonable measures to ensure that any personal information in their custody and control remains secure and protected from escalating risks. When it comes to cybersecurity, **an ounce of prevention is worth a pound of cure**.



INFO MATTERS

In 2022 the IPC's *Info Matters* podcast ranked 13 on a list of 60 top data privacy podcasts. Season two featured discussions with compelling thought leaders on issues related to privacy and transparency.

In episode three, Commissioner Kosseim and author Dave Meslin explored the role of civic engagement in fostering greater government transparency and user-friendly privacy policies in ***Power to the people! Access, privacy, and civic engagement.***

Episode five, ***In conversation with Jim Balsillie***, featured a discussion with the founder of the Centre for International Governance Innovation about the impact of digital transformation on our human rights, collective well-being, and democracy.

In episode nine, ***Back to the Future: Using strategic foresight in the new digital age***, Commissioner Kosseim spoke with the IPC's Assistant Commissioner, Eric Ward, about how strategic foresight can be used to anticipate and address emerging technological issues to better prepare for and enhance policy making in Ontario.



CHILDREN AND YOUTH IN A DIGITAL WORLD

Our goal is to champion the access and privacy rights of Ontario's children and youth by promoting their digital literacy and the expansion of their digital rights while holding institutions accountable for protecting the children and youth they serve.

- Members of the IPC's Youth Advisory Council.



PRIVACY DAY 2022

The IPC began 2022 by focusing its annual Privacy Day event on empowering a new generation of digital citizens. Our **webcast** featured a panel of experts, each with unique perspectives as educators, students, researchers, policymakers, regulators and activists, brought together to discuss three themes:

- How are children and youth experiencing the digital environment? How can we protect and empower them to think critically about their personal information online?
- Has the time come to prioritize privacy education as an integral component of digital literacy and citizenship school curricula?
- What is the role of laws, regulations and non-regulatory mechanisms, like codes of practice, in protecting and promoting children’s privacy rights?

Nearly 1,000 people tuned in to watch the live webinar. Since then, it has been viewed nearly 1,000 more times on the IPC’s **YouTube channel**.

These Privacy Day discussions inspired us to expand our outreach to children and youth with new ideas for empowering Ontario’s next generation of digital citizens.



Members of the IPC’s Youth Advisory Council.



YOUTH ADVISORY COUNCIL

In September 2022, the IPC issued a call to Ontario youth, inviting them to join the IPC’s new **Youth Advisory Council**.

Our goal was to bring together a group of young people from different communities across the province, with diverse backgrounds, experiences, and outlooks, to share their views about digital literacy, access, and privacy rights in Ontario.

This group of highly engaged youth will help the IPC develop education and outreach materials that are even more relevant to young people. Their work over the coming years will help us guide the next generation through the opportunities and risks of the online world. By broadening the conversation and engaging young people with a seat at the table, we can learn from them and enhance our efforts to make the digital world a better place for future generations.



IPC ON INSTAGRAM

After careful deliberation, in 2022, the IPC launched an Instagram account to connect with Ontario’s children and youth. Our

objective is to teach them about privacy risks and how to protect themselves online. Our account, [@IPC.Ontario](#), is a trusted online space where young people can get useful and age appropriate tips on how to protect their privacy online and access their records from a government institution, health care provider or children’s aid society.

The account features eye-catching, bite-sized content. For example, Halloween-themed posts warned about some of the “privacy monsters” lurking in the digital world and Santa’s little helpers offered kids helpful tips on privacy settings for their new electronic games and toys. Colourful characters, infographics, and [@IPCOntario whiteboard videos](#) make learning fun and easy.



PRIVACY PURSUIT! LESSON PLANS

Throughout 2022, the IPC worked with [MediaSmarts](#), Canada’s Centre for Digital Literacy, to develop lesson plans for teachers,

parents and caregivers, building on the critical messages contained in [Privacy Pursuit! Games and Activities for Kids](#). The carefully designed lesson plans, aimed at grades two through eight, will be released in time for the 2023-24 academic year. These include how to use, strengthen, and protect passwords, limit what information they share online, avoid online scams, and protect themselves against cyber threats. They also contain critical lessons to help kids develop privacy empathy and learn how to respect the privacy of others.



I joined the IPC Youth Advisory Council because I believe that youth voices are essential in decision-making processes, especially regarding their privacy.”

KEITH BAYBAYON, CHAIR, IPC YOUTH ADVISORY COUNCIL



INFO MATTERS

In 2022, we dedicated several episodes of the *Info Matters* podcast to issues affecting children and youth.

In episode six, ***Giving foster kids a fair shot in life***, Commissioner Kosseim discussed helping former foster kids reclaim control over their personal information so they can get a fresh start in life with Jane Kovarikova, founder of the Child Welfare Political Action Committee.

In episode seven, ***From high school to university: a young person's perspective on digital privacy***, Keith Baybayon, former president of the Ontario Student Trustees' Association and chair of the IPC Youth Advisory Council, shared his views on young people's use of digital technologies, how they view privacy, and how parents, teachers, and regulators can help them develop the skills to be informed digital citizens.

In episode eight, ***Seeing privacy through an equity lens in the child welfare sector***, Commissioner Kosseim spoke to Nicole Bonnie, CEO of the Ontario Association of Children's Aid Societies, about our shared role in supporting vulnerable children, youth, and families, particularly from BIPOC communities. The conversation explored the concept of privacy through an equity lens, and how race-based data is providing the evidence needed to fuel positive change.



TRUST IN DIGITAL HEALTH

Our goal is to promote confidence in the digital health care system by guiding custodians to respect the privacy and access rights of Ontarians, and supporting the pioneering use of personal health information for research and analytics to the extent it serves the public good.



AXE THE FAX

Statistics collected by our office in 2022 revealed a continuing concern with misdirected faxes in the health sector, representing almost 40 per cent of health privacy breaches in Ontario.

Using outdated and vulnerable technologies such as faxes and unencrypted email threatens to erode public confidence that personal health information is secure. In September, the IPC joined its federal, provincial, and territorial counterparts in issuing a **joint resolution** addressing insecure methods of transmitting personal health information. The resolution calls on governments and relevant partners in the health sector to replace traditional faxes and unencrypted email with more secure forms of digital communication. The resolution is an urgent call to action given what we know to be the largest source of health data breaches reported to our office over several years.

In the resolution, the IPC and our counterparts urge governments to address the issue by coordinating a strategic plan and providing institutions with appropriate supports, such as funding or other incentives, to phase out traditional fax and unencrypted email. The resolution asks governments to promote the adoption of more modern and secure digital alternatives that are equitably available and accessible to all, and calls on health sector organizations and providers to do their part as well. Finally, the resolution commits the IPC and our counterparts to collaborate with

interested parties to support this transition and to provide relevant privacy and security guidance and public education about the risks and opportunities associated with digital communications and virtual health care.

In February 2023, the government announced a plan to phase out faxes in the health sector over a five-year timeline. Our office applauds this initiative and stands ready to assist the government and other interested parties in implementing this plan in a manner that supports public trust. We look forward to seeing the health care sector continue to decrease its dependency on faxes in favour of more secure forms of digital communication.



ONTARIO HEALTH DATA COUNCIL AND PHIPA REFORMS

Commissioner Kosseim is a non-voting, ex officio member of the Ontario Health Data Council (OHDC). The OHDC was created in 2021 to advise the Minister of Health on managing Ontario’s health data. The council’s mission is to “enable ethical, timely, and responsible access to and use of health data for people, communities, and populations in Ontario.” The OHDC also serves as the advisory committee to the minister on the implementation of the provincial electronic health record under section 55.11 of the *Personal Health Information Protection Act* (PHIPA).

It means working for an organization that supports its employees and acting as an independent watchdog on access and privacy rights for the people of Ontario.”



In November 2022, the OHDC published its report, ***A Vision for Ontario's Health Data Ecosystem***. The report describes the system's current state and provides recommendations for action, including to:

- Integrate and use health data to advance health and equity outcomes for people, communities, and populations
- Promote health equity through appropriate data collection, analysis, and use
- Establish system-level trustworthy governance and policies for health data as a public good
- Respect and support First Nations, Inuit, and Métis data sovereignty
- Build data stewardship capacity and enable sharing by default

Further to its report of November 2022, the OHDC continues to provide input to the ministry on possible data governance and stewardship models and how PHIPA could be improved to facilitate data sharing between different actors in the health system.

The IPC strongly urges the government to ensure that any new data governance framework or changes to PHIPA intended to increase the sharing of personal health information be counterbalanced by robust accountability and transparency measures to protect Ontarians' privacy and support public trust.

To start, the IPC strongly encourages the government to fully implement the PHIPA reforms adopted back in 2019 and 2020 dealing with electronic audit logs, consumer electronic service providers, de-identification standards and administrative penalties by proclaiming those sections of PHIPA into force and adopting the necessary regulations to enable them to finally come into effect.



ONGOING ADVOCACY FOR ADMINISTRATIVE PENALTIES

In our 2021 annual report, the commissioner **recommended** the government set out the details of PHIPA's administrative penalty scheme in regulations. The purpose of these administrative penalties is to encourage compliance and prevent persons from deriving, directly or indirectly, any economic benefit as a result of contravening Ontario's health privacy law or its regulations. This would enable the IPC to impose monetary consequences on the few bad actors who unfortunately undermine Ontarians' trust in the entire health system.

We expect the government to release the proposed regulation for public comment, setting out the criteria to be considered by the IPC when imposing a penalty and the maximum dollar amounts. We look forward to seeing this regulation come into force and giving Ontarians confidence that there are effective mechanisms in place to promote positive behaviour, while stamping out the bad.

In keeping with our vision of a modern and effective regulator, the IPC will apply a proportionate approach to administrative penalties. We intend to adopt the principles and philosophy of a just culture approach by applying different levels of intervention based on the nature and circumstances of the contravention. The choice of enforcement tool (whether it be education, corrective measures, recommendations, orders, administrative penalties or referral to the Attorney General for prosecution of an offence) will depend on a range of factors, including the conduct of the person or organization in question. Such conduct could range from a single honest mistake to a repetitive pattern based on carelessness; from a minor error in judgment to a more serious one; from recklessness or disregard for the rules to deliberate intent to break the rules for malicious or profit-seeking motives. Where appropriate, we will also look at the organization's governance structures and processes in place to determine to what extent, if any, these (or the lack thereof) may have contributed to the conditions that enabled the contravention to take place.



INFO MATTERS

Season two of *Info Matters* featured discussions about the use of data for better health outcomes.

Artificial intelligence technologies now make it possible to create fake versions of personal information that look and feel like the real thing but are different enough to protect individual privacy. In the first episode of season two, ***Real or fake? The buzz about synthetic data***, Commissioner Kosseim spoke with Dr. Khaled El Emam about how synthetic datasets can be used to advance important health research while minimizing privacy risks.

Health influences happiness and overall well-being, but not everyone has fair access to resources that support good health. Disparities persist, influenced by age, education, gender, income, and race. We ended season two with a conversation with Dr. Kwame McKenzie, CEO of the Wellesley Institute, in ***Health equity: Using data to make a positive difference for communities***, to discuss how anonymized data can be used to advance equity in health care and health outcomes.



NEXT-GENERATION LAW ENFORCEMENT

Our goal is to contribute to building public trust in law enforcement by working with relevant partners to develop the necessary guardrails for the adoption of new technologies and community-based approaches that protect both public safety and Ontarians' access and privacy rights.



FACIAL RECOGNITION TECHNOLOGY

In May 2022, Canada's federal, provincial, and territorial privacy commissioners issued a **joint statement**, recommending a legal framework specific to facial recognition (FR) technologies. Such a law should clearly define the purposes for which police can use FR and those for which they can't. It should also require that the use be necessary and proportionate for the proposed purpose and provide for appropriate privacy protections to mitigate the risks involved.

In the absence of a comprehensive legal framework and in light of the significant uncertainty that remains about the lawfulness of FR use by police and in which circumstances, the privacy commissioners released accompanying **privacy guidance on facial recognition** for police agencies. The purpose of this guidance is to clarify police agencies' privacy obligations under current laws, with a view to helping them ensure that any purported use of FR technology complies with existing law, minimizes privacy risks, and respects privacy rights.

Building on our work with our federal, provincial, and territorial counterparts, and in response to requests by interested parties, the IPC began developing Ontario-specific guidance on one particular use case of FR: police use of facial recognition technology for searching mugshot databases. In 2022, our office engaged in ongoing consultations with representatives from police services, academia, government ministries, and civil society groups to receive their input on our approach to developing the guidance.



This guidance will build on the national guidelines and focus in on the key privacy, transparency and accountability recommendations and best practices to guide police when designing this specific type of program. The guidance will help police services and police services boards comply with their obligations under Ontario's access and privacy laws and contribute to the adoption of up-to-date and consistent police practices for programs across Ontario. We will report back on the results of this initiative in our next annual report.

It means being someone who does interesting and challenging work for an organization that makes a difference in many people's lives in terms of helping them to access or protect information that is important to them. It means being a part of a community of good people whose interests are aligned in helping the public understand the importance of access and privacy laws."



CORONER RECOMMENDATIONS TO ADDRESS INTIMATE PARTNER VIOLENCE

In August 2022, the Office of the Chief Coroner provided the IPC with the jury recommendations of an inquest into the murders of three women in rural eastern Ontario. Recommendation 78 called on the IPC to work with the Domestic Violence Death Review Committee, justice partners, and intimate partner violence service providers to develop a plain language tool to empower intimate partner violence professionals to make informed decisions about privacy, confidentiality, and public safety. Our office **readily agreed** to carry out this critically important recommendation.

Protecting personal information from unauthorized collection, use, and disclosure is essential. However, privacy must not be used as an excuse to prevent the lawful sharing of information, particularly when it is necessary to prevent serious harm. To implement recommendation 78, the IPC began consultations with intimate partner violence professionals to identify the dominant privacy issues and help balance the values, objectives and interests at play. We will report on outcomes in our next annual report.



INFO MATTERS

Episode two of *Info Matters*, **Family ties: Using investigative genetic genealogy to solve crimes**, featured a discussion with Dr. Frederick Bieber about the use of DNA technology by police and the potential privacy risks for people who use recreational genealogy services, and their family members.

In **episode four**, Dr. Alana Saulnier, an assistant professor in the Department of Sociology at Queen's University, joined Commissioner Kosseim to discuss the benefits and risks of police use of body-worn cameras and how they impact police-community relations.



RESPONSIVENESS

ADDRESSING COMPLAINTS AND APPEALS IN A FAIR, TIMELY AND MEANINGFUL MANNER

To provide Ontarians with more timely resolution of their appeals and complaints, our office has undertaken efforts to review its tribunal processes and procedures, some of which are highlighted on the next few pages.

REDUCING THE FILE BACKLOG


To clear the backlog resulting from the pandemic office closures, the IPC built on the headway made in 2021 by hiring temporary staff and further streamlining processes to enhance efficiencies and reduce processing time.

Both mediation and adjudication queues were reduced by approximately 50 per cent and the teams are well on their way to eliminating them, with a view to meeting the ultimate goal of delivering timely service to the people of Ontario.

The number of files closed relative to the number of files opened is a key indicator in the success of the backlog reduction. It is also a measure of the sustainability of our operations and our ability to stay ahead of public demand. In 2022, the tribunal achieved the notable goal of closing 2,878 files, compared with 2,574 files opened that year. Closing 304 files more than were opened, or a ratio of 1.12 files closed for every one file opened, represents the tribunal's best performance in this metric in at least six years and illustrates the positive impacts of the process enhancements and investments made in 2022.

MEDIATION PILOT PROJECT

To streamline processes, the mediation team launched a pilot project in 2022 where parties in select sole-issue appeals were invited to participate in a half-day teleconference. The goal was to resolve the appeal during or shortly after the teleconference.



It means belief in and commitment to the work we do. Continually learning from each other and building skills in our professions.”

Almost all of the institutions contacted had great interest in participating as they recognized the benefits of avoiding a lengthy back and forth through protracted discussions and correspondence between the parties, with a view to enhancing the likelihood of a quick resolution when all parties work together in real time.

This project was a resounding success, with 90 per cent of files resolved before, on the day of, or shortly after the teleconference. On average, these files took 75 per cent less time to process relative to files that proceeded through the regular mediation stream. Both appellants and institutions enthusiastically endorsed this shortened process for appropriate files. The team looks forward to expanding on the success of this project in the year ahead.

IPC INTRODUCES E-APPEALS

In August 2022, and as part of our efforts to modernize and provide digital services to Ontarians, the IPC launched a new service for **filing and paying for appeals online**, making it easier for people to file an appeal with our office — online, anytime. Since the launch of this new online service, we have seen a rapid uptake in the number of appellants who have taken advantage of this convenient means to submit and pay for their FIPPA and MFIPPA appeals. From August to December 2022, the IPC received 275 appeals (51 per cent) electronically compared to 264 (49 per cent) through other methods.

UPDATES TO M/FIPPA CODE OF PROCEDURE

Throughout 2022, the IPC undertook a thorough review of its FIPPA and MFIPPA Code of Procedure and associated practice directions. These key documents that guide the appeals process had not undergone a significant review and revision since 2004.

Since then, the tribunal has embraced the use of electronic methods of communication and records submission which requires revisions to the code of procedure. The code of procedure also needs to better reflect the current state of the tribunal's operations and procedures, which have evolved to become more streamlined and efficient while still respecting rules of procedural fairness. We expect to implement a new code of procedure in 2023, following a reasonable advance public notice period.

NOTABLE TRIBUNAL TRENDS

With the rapid adoption of technology and digitization of services, protecting privacy is more vital than ever to maintain Ontarians' confidence in their public institutions. Throughout 2022, cyberattack incidents reported to our office, including ransomware, were more complex than in previous years, and had greater impact on a broad range of institutions, including school boards, municipalities, and health care and child and family service providers.

The IPC continues to track these occurrences and encourages institutions to report these and other privacy breaches to our office so that we can advise on appropriate mitigation strategies.

Within the health sector, the IPC also saw about a 20 per cent rise in incidents involving snooping into electronic medical records (EMRs) by health care professionals outside of a patient's circle of care. All health care providers in the province must have the necessary safeguards to detect, report, and ultimately prevent snooping altogether, including through privacy security training, electronic system warnings, and automatic tracking within EMR systems.

Finally, the IPC continues to resolve issues with health care providers who abandon existing patient files after having either closed or moved their practice. The vast majority of health care providers take appropriate steps to ensure that patient files are archived, transferred to other providers, and made available to patients to ensure continuity of care. But those who don't leave patients in the lurch with no one obvious to turn to when seeking access to, or protection of, their health records. The IPC's guidance on **avoiding abandoned records** provides practical tips on managing the transfer of patient records when there is a change in practice.

NOTABLE EXAMPLES OF CASES

EARLY RESOLUTION

The early resolution team has the delegated authority and responsibility to resolve or dismiss appeals, complaints, and self-reported breaches right up front, in the most expedient and collaborative way possible. The goal of the early resolution team is to attempt to resolve them as early as



possible and if they cannot be resolved, determine whether there are sufficient grounds for the matter to proceed further. In 2022, the early resolution team successfully closed more than 53 per cent per cent of all IPC files across all sectors.

TO FAX OR NOT TO FAX ... DEFINITELY NOT

The IPC noted an unusually high number of reported breach incidents in a hospital's 2020 annual statistical report and opened a file to further enquire into the matter. After months of working with the IPC to get to the root cause of the issue, the hospital made great strides in mitigating the risk of sending faxes to the wrong individuals, responding more quickly when it does happen, and reducing its overall use of this outdated and insecure technology. The hospital has since put in place an "e-referral first" policy for referrals from primary care providers and is working with other health partners in the region to replace the use of faxes with more secure electronic solutions for transmitting personal health information.

This **IPC's report**, released in January 2023, shows the enormous potential for organizations to coordinate action and work together to move toward more secure communication technologies that will strengthen Ontarians' trust in the health care sector.

CYBERATTACKS THREATEN ESSENTIAL SERVICES

Three school boards, one college, and two universities contacted the IPC to report a ransomware attack on guard.me. Guard.me, a third-party company providing insurance coverage to international students at these institutions, experienced a ransomware attack that affected the personal information of some of their students.

At the time, a significant number of the institutions' international students were required or encouraged to provide personal information to guard.me to receive mandatory insurance coverage. In most cases, the student provided their claims information directly to guard.me and the institution only provided limited enrollment information. During its review, the IPC found that some of the institutions did not have a contractual agreement with guard.me to ensure the confidentiality and security of the personal information disclosed to the company. In addition, some of the institutions did not get the students' consent or provide clear notice to them before providing their personal information to guard.me. Following our review, the institutions have implemented or committed to implementing changes we recommended to address these and other gaps.

BACK TO BASICS

An individual filed a complaint against a county because their personal information was disclosed to another individual in response to an access request before the complainant could apply as a third party to the request.

The IPC found that the county lacked basic understanding about the third-party appeal process. As a result of the analyst's interactions with the county, the clerk's office sought out and completed further training and committed to reviewing IPC orders and guidance to ensure that they fully understood their obligations under MFIPPA. Based on the actions taken by the institution to contain the breach and prevent similar incidents in the future, the complaint was successfully screened out without needing further IPC review. This complaint demonstrated a need for the county to improve its freedom of information process and training programs to ensure its staff fully understand their responsibilities. The county's response will benefit all of its residents making access requests in the future.



MEDIATION

When files are streamed to mediation, our team of professionally trained mediators facilitate negotiations and discussions between the parties, with the goal of reaching a mutually acceptable agreement or resolution. IPC mediators create an environment for parties to communicate and express their needs, concerns, and perspectives. The mediator educates the parties and, wherever possible, provides advisory opinions. When appeals are resolved, or partly resolved, at mediation, fewer cases need to go to formal adjudication.

MORE THAN MEETS THE EYE

Over two months, a city received requests from a legal clinic for information relating to poverty, homelessness, encampments, overdose prevention, and race-based data. The city denied five of the requests outright on the basis that they appeared to be frivolous or vexatious. The parties agreed to participate in the expedited mediation pilot project and succeeded in quickly resolving the issues. During the teleconference, the appellant better explained the type of information they were seeking, and the city provided guidance on how to reformulate the request using certain keywords and timeframes. As a result of the mediation discussions, four appeals were resolved on the same day, and the fifth was resolved shortly after.

THE BENEFIT OF TALKING THINGS THROUGH

An individual requested historical records about a deceased family member who was institutionalized in psychiatric hospitals. The Archives of Ontario granted partial access to the requested records. Through mediated discussions, the appellant agreed that the exemptions applied to the severed information but believed that more records should exist. Archives staff conducted multiple searches and participated in a teleconference where the archivist provided details of their searches and the retention policies at various psychiatric hospitals, which explained why certain records would no longer exist. Archives staff also provided the appellant with resources for alternative sources of information. While no additional records were located, the appellant expressed gratitude and satisfaction with the mediation process and recognized the sincere efforts of the mediator and the archives staff.

ADDRESSING THE UNDERLYING QUESTION

An individual requested information about the number of public park garbage cans managed and operated by the city. They sought information by location and for a specific ward for the past seven years. The city issued their decision, advising that they do not have any records that meet the description of the request. During the appeal, the mediator worked with the city and the individual to help reformulate and narrow the scope of the request. The appellant narrowed their request to the previous two years and several specific parks. During mediation, the appellant explained that their underlying concern was a perceived lack of garbage bins in public parks. The city conducted more searches, granted access to records responsive to the revised request, and answered specific questions about how the parks are serviced. The appellant was satisfied with the disclosure of records from the city and the answers provided to his questions.

PRIVACY INVESTIGATIONS

IPC investigators work to resolve privacy complaints and investigate privacy breaches. After an investigation, they issue recommendations to the institution or organization that are most often accepted and adopted to remediate the situation for the future.

SELLING DE-IDENTIFIED HEALTH DATA || PHIPA 175

After learning that a health information custodian was allegedly selling de-identified personal health information to a third party, the IPC opened an investigation. We found that de-identifying personal health information was a permitted use without consent under PHIPA, but subject to certain conditions, including transparency and safeguarding obligations. We found that custodians planning to de-identify and sell data must clearly and explicitly state this in their public notice to individuals. The custodian's security obligations also required that they take reasonable steps to protect and secure personal health information, including during the de-identification process and afterwards. Notably, sale agreements with third parties must include adequate security and privacy controls to ensure de-identified data remains de-identified, including a robust de-identification governance process with regular re-identification risk assessments.

COVID-19 AND THE USE OF VACCINE CERTIFICATES

For the 2021-2022 academic year, a university required students to be fully vaccinated against COVID-19 to live in residence. Students had to complete and submit a questionnaire to prove their vaccination status. The parents of three students complained to the IPC that the collection of students' COVID-19 vaccination status information through its mandatory questionnaire was inappropriate. The IPC found



It means being part of a strong and close-knit community of people who are committed to supporting each other and Ontarians.”

that within the context of the pandemic, particularly during the start of the 2021-2022 academic year, the university's collection of this information complied with provincial public health directives applicable at the time and was necessary within the meaning of FIPPA.

TORONTO POLICE SERVICE SNOOPING INCIDENT

A police employee ran police database searches on their neighbours, and one of those neighbours complained to the IPC. A police audit during the IPC investigation found that the employee had inappropriately accessed the complainant's personal information and disclosed it to another police service employee without authorization. The investigation also found that the employee had conducted similar searches on several other individuals. The IPC determined that the police did not have reasonable measures in place to prevent unauthorized access to personal information and made recommendations for improvement, including protocols for audits and guidance on how to respond to unauthorized access. The IPC also recommended the police notify the other individuals whose information was inappropriately accessed.



ADJUDICATION

When a resolution cannot be found through early resolution, mediation or investigation, files go to an adjudicator who decides whether to conduct a formal inquiry or review. The adjudicator collects and reviews evidence and arguments from the parties and issues a final and binding decision that may include an order.

RECORDS OF POLICE USE OF FACIAL RECOGNITION || MO-4269 + MO-4286

An adjudicator ordered two police forces to partially waive fees relating to a request for records about their use of Clearview facial recognition technology due to the significant public health and safety ramifications of using the technology. The adjudicator referred to the ongoing and significant concern and controversy around the privacy and safety implications of Clearview AI's facial image scraping practices, and found that the records would promote informed debate about these issues.

MULTIPLE REQUESTS FOR SIMILAR INFORMATION || MO-4241 + MO-4257

Within a relatively short period, requesters made dozens of multi-part, excessively detailed, and significantly overlapping requests for records relating to a class-action lawsuit against a town. The requesters were acting on behalf of the plaintiffs in the class action lawsuit. The town denied the requests on the basis that they were frivolous or vexatious, and the requesters appealed. The adjudicator found that the appellants' pattern of conduct — the filing of an inordinate number of detailed and repetitive requests — was an abuse of the right of access found in MFIPPA, and that the requests were frivolous or vexatious. The adjudicator upheld the town's decisions to deny the requests and placed limits on the appellants' future access requests and appeals.

LEGAL FEES RELATED TO REQUEST FOR GOVERNMENT MANDATE LETTERS || PO-4285

A journalist requested access to the total number of Crown counsel hours spent on proceedings related to the IPC's **order** to Cabinet Office to disclose the Premier's mandate letters. The request was denied by the Ministry of the Attorney General, citing the solicitor-client privilege exemption. The adjudicator rejected the ministry's claim, finding that in the circumstances, disclosure of the total number of Crown counsel hours would not reveal solicitor-client privileged communications, and ordered disclosure of the information. The ministry has brought an application to the Divisional Court for judicial review of the order, which is pending.

ACCESS RIGHTS TO A REPORT ON PARAMEDIC CONDUCT || PHIPA DECISION 194

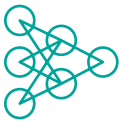
An individual was tasered while in police custody, and paramedics provided treatment. The individual complained to the professional standards department of the paramedic service (part of the Region of Peel) about the care they received, which was investigated. The individual sought a copy of the resulting investigation report. The region denied access, citing some exemptions from the right of access in PHIPA. It also cited the exclusion in MFIPPA for employment records. The adjudicator found that the individual had a right to access the full report under PHIPA and that MFIPPA was irrelevant in the circumstances. The IPC ordered the region to provide the report to the complainant.

A teal-tinted photograph of two rowers in a boat on water. The rowers are in a crouched position, holding oars. The water shows ripples and reflections. The overall image has a strong teal color cast.

ACCOUNTABILITY

MAINTAINING ONTARIANS'
CONFIDENCE IN THE
ORGANIZATIONAL
EXCELLENCE OF THE IPC

The third pillar of IPC's mission is dedicated to holding ourselves to the high standards of organizational excellence and accountability that Ontarians expect of us. Two thousand twenty-two represented a pivotal year in terms of modernizing our organization's digital capacity, designing a new hybrid work reality, and enhancing our internal management, governance, and accountability measures.



TRANSFORM THE IPC INTO A MODERN, DIGITAL ORGANIZATION

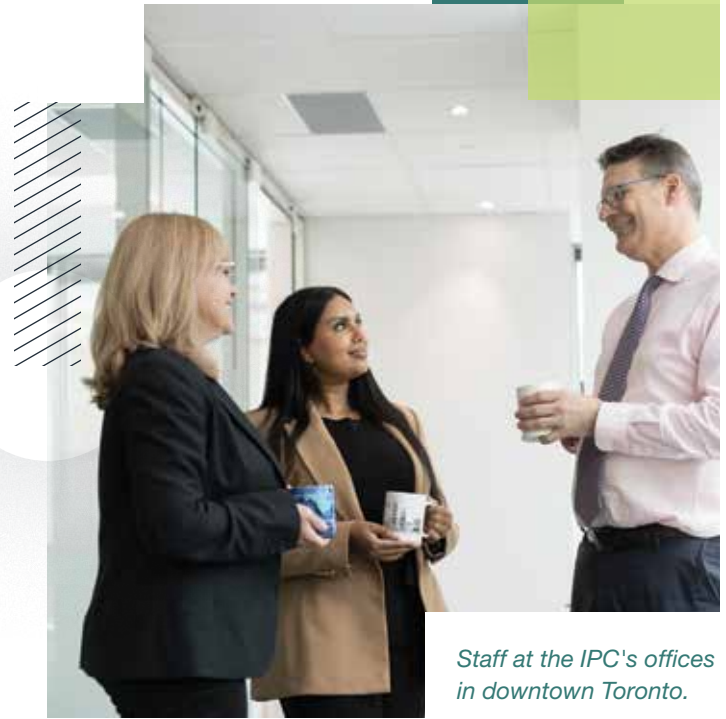
In 2022, we addressed the findings of our 2021 threat risk assessments by implementing key IT upgrades and cyber security enhancements. We launched a new online appeal service, allowing Ontarians to securely file and pay for their appeals electronically. We implemented a corporate wireless network to enable greater in-office mobility and inter-departmental collaboration between IPC employees. We launched a pilot for a new Office 365 solution and prepared the necessary groundwork to securely move IPC's information holdings to the cloud. In 2023, we will continue to enhance our digital services with a project to implement a new IPC website built on modern technologies, featuring greater potential for interactivity and an improved user experience.



IPC AS AN EMPLOYER OF CHOICE

Throughout 2022, the IPC slowly and gradually returned staff to the office for certain in-person activities. We worked towards an eventual hybrid work model, which evolved over three phases, beginning with those activities that staff felt would be best carried out in person

It means delivering high-quality work in a collaborative, supportive and professional work environment. Learning and growing professionally, every day."



Staff at the IPC's offices in downtown Toronto.

to promote greater employee collaboration, cohesion, and sense of community. Each phase built upon the previous one, incorporating staff feedback while ensuring support for the effective delivery of our mandate and offering flexibility for employees. The IPC implemented permanent hybrid work arrangements in spring 2023, that balance in-office business and operational requirements, while providing staff with flexible work from home arrangements and quality work-life balance.

As part of our employee engagement efforts, the IPC launched both a formal and informal employee recognition program to celebrate significant milestone achievements and to express particular appreciation for employees and teams who best exemplify IPC values.

In 2022, the IPC also established a new IPC Champion program, comprising individuals and teams among our ranks who volunteered to actively promote bilingualism; community giving; health and wellness; inclusion, diversity, equity and accessibility. In addition, the IPC re-established and reconfigured its Joint Health and Safety Committee, Social Committee, Equity and Accessibility Committee, Green Committee, and Learning Committee. These staff-led initiatives provide new leadership and learning opportunities, help spark creative and innovative ideas, promote a shared spirit of collaboration, and foster a sense of purpose and camaraderie that bring out the best of IPC.

We also developed a virtual suggestion box to allow employees a safe space to provide anonymous, unsolicited feedback to senior management. Ongoing and constructive input from our staff on how we can continually improve as an organization will help build the IPC's potential and reputation as an employer of choice.



STRENGTHEN IPC GOVERNANCE AND ACCOUNTABILITY

In 2022, the IPC continued to strengthen its internal management and governance capacity by building new leadership and management training programs for its senior leaders and managers.

The IPC continued to enhance its modern controllership and fiscal best practices to ensure responsible use and greatest value of public funds. In this regard, the IPC met our financial target of a year-end balanced budget by spending within one per cent of our budget. As per the *Freedom of Information and Protection of Privacy Act*, the financial statement of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario.

As part of our 2022-2023 annual planning cycle, we proposed further enhancements and changes to our organizational structure and operations to enhance accountability and deliver on the IPC's evolving and growing mandate effectively. We look forward to implementing these improvements in 2023 and will report further on them in our next annual report.





COMPLIANCE

COMPLIANCE REVIEWS

ADDRESSING COMPLIANCE RATES AT THE MINISTRY OF THE ENVIRONMENT, CONSERVATION AND PARKS

For the past 25 years, the Ministry of the Environment, Conservation and Parks (MECP) has had the highest number of access requests received annually, when compared to all Ontario institutions. Businesses file a majority of these requests. In 2021, MECP's reliance on paper-based records meant that during COVID-19 closures, it could not process access requests. Its response rate for the year plunged to under 1.5 per cent for 30-day and extended compliance.

MECP's leadership was proactive in responding to the drop, and receptive to the IPC's request to engage directly with them on the issue. Throughout 2022, the IPC supported the ministry's improvement efforts by monitoring its backlog reduction progress and advising on current and proposed plans to provide information through other channels.

Overall, MECP's response rate for 2022 remains low since they are still tackling their backlog. However, a significant majority of new requests received in the second half of the year were completed on time, with the number continuing to trend upward month by month.

MECP has also begun to offer alternatives to freedom of information (FOI) requests by creating alternative channels to access information. Its **Environmental Property Information Program**, launched in March 2022, has reduced by 20 per cent the number of requests that would otherwise have come through the FOI process.

The IPC commends MECP for its proactive and innovative responses to its FOI challenges and encourages the ministry to keep pursuing its efforts. The IPC will continue to engage with the ministry as it continues its journey to improving Ontarians' access to environmental information.

UPDATED MANUAL FOR THE REVIEW AND APPROVAL OF PRESCRIBED PERSONS AND PRESCRIBED ENTITIES

In 2022, we worked toward finalizing revisions to the Manual for the Review and Approval of Prescribed Persons and Prescribed Entities under the *Personal Health Information Protection Act* (PHIPA). In their roles under PHIPA, prescribed persons and entities are entrusted with large volumes of personal health information. The manual is a tool to ensure that prescribed persons and entities have practices and procedures in place to protect the privacy of the individuals whose personal health information they receive and to maintain the confidentiality

of the data. These practices and procedures are subject to scrutiny by our office every three years.

The new revised manual will significantly modernize the security requirements for these organizations in light of evolving industry standards and best practices. It will also introduce a new risk-based approach to IPC's three-year reviews that will bring more focused and in-depth review of those key areas determined to be of highest risk.

IPC REVIEW OF INTER-MINISTERIAL DATA INTEGRATION UNITS

Under FIPPA, inter-ministerial data integration units (IMDIUs) enable the Ontario government to join data sets and use the combined data for the public good. IMDIUs have the authority to collect personal information indirectly, link different data sets for analysis and disclose the resulting data in de-identified form to support government decision-making.

Under the law, the IPC must review the practices and procedures of IMDIUs before they can begin collecting personal information. In 2022, the IPC completed its first review of the IMDIU in the Capacity Planning and Analytics Division of the Ministry of Health.

During the review, the IPC assessed the practices and procedures governing the lifecycle of information collected, including collecting, using, and disclosing personal information; linking and de-identifying personal information; security; retention periods; and public reporting.

The Ministry of Health IMDIU was generally responsive and amended its practices and procedures following most of IPC's comments. However, because some of the outstanding issues would take more time and were of significance, we issued formal orders to ensure compliance. A full description of the IPC's orders and recommendations can be found in the IPC's [Review of the Practices and Procedures of the Ministry of Health's Inter-ministerial Data Integration Unit](#). The IPC continues to monitor the ministry's progress towards full compliance.

CORONERS ACT REVIEW

The *Coroners Act* allows the Office of the Chief Coroner to disclose personal information to prescribed entities for research, data analysis, or the compilation of statistical information related to the health or safety of the public. In 2022, the IPC concluded its first [review](#) of a prescribed entity under the act, the Institute for Clinical Evaluative Sciences

(ICES). The IPC was satisfied with, and approved, ICES' practices and procedures for protecting individuals' privacy and maintaining confidentiality.

ACCESS AND COMPLIANCE TRENDS

Provincial and municipal institutions, health information custodians that are also institutions under FIPPA, and child and family service providers are required to submit annual access to information statistics to the IPC.

In 2022, Ontarians filed 58,461 freedom of information requests, representing a five per cent increase from the previous year. Response rates, in terms of percentage of access requests completed within 30 days, continued to vary by sector. For provincial institutions, only 51.2 per cent of access requests were completed within 30 days. This represents a decrease of 12.6 per cent since 2021.

Municipal institutions maintained an 81 per cent response rate within 30 days, up slightly from 80.4 per cent in 2021.

Ontarians made 100,031 requests for access to personal health information in 2022. Health information custodians were able to maintain a 30-day response rate at an impressive rate of 99 per cent.

Child and family service providers received 9,923 requests for access to personal information. Seventy-one per cent were completed within 30 days.

POLICY ADVICE AND CONSULTATIONS

FORMAL SUBMISSIONS TO GOVERNMENT

Through our advocacy work in 2022, the IPC submitted [comments, open letters, and recommendations](#) on various proposed laws and regulations having privacy implications, including in the following areas:

EMPLOYEE PRIVACY

Before the pandemic, relatively few Canadians regularly worked from home. During the first few months of 2022, about [46 percent of employees worked from home](#) at least some of the time. Demand for workplace monitoring and remote surveillance tools has dramatically accelerated as employers seek alternate ways of ensuring productivity and accountability in the workforce. Employee monitoring software — also referred to as “bossware” — can have many different capabilities, including the ability to: monitor all computing

COMPLIANCE

device activity; record employees through webcams and microphones; and track employee location, movements, and activities. When combined with powerful algorithms that can analyze patterns in the data and make inferences about employees' conduct, behaviours, and even their aptitudes and sentiments, the potential for privacy invasion and discriminatory practices can become very real, very quickly.

The government responded in part to these threats by introducing Bill 88, the *Working for Workers Act*, which requires employers with twenty-five or more employees to have a written policy explaining their electronic employee monitoring activities. In April, the commissioner presented her views on the bill to the Standing Committee on Social Policy at the Legislature of Ontario. While the commissioner acknowledged this important first step in increasing transparency of electronic monitoring practices, she pressed the government to go further by requiring greater accountability as well.

There must be clear boundaries around acceptable use of electronic surveillance and rules against monitoring employees surreptitiously or when not on the job. Ontario's workers must have mechanisms to complain when employers don't comply with these policies and ask for an investigation and redress if the policies aren't followed. Overly-invasive policies should be reviewed by an independent regulator with the power to effect course correction. Ultimately, these issues of electronic workplace monitoring should be governed by a more comprehensive Ontario private sector privacy law, similar to the one proposed in the government's 2021 white paper, **Modernizing Privacy in Ontario**. We urge the government to resume its bold and ambitious efforts to address glaring gaps in statutory privacy protections in Ontario, including for employee privacy.

OTHER FORMAL IPC SUBMISSIONS TO GOVERNMENT IN 2022 INCLUDED THE FOLLOWING:

- Submission on the **proposed amendments** to Ontario's health privacy law regarding the right to access records in electronic format
- Submission on Bill 106: **Obligations and authorities of Ontario Health Teams and access to records in electronic format**
- Comments on provisions of Bill 88 (the *Working for Workers Act*) regarding **Electronic monitoring of employees**
- Recommendations regarding **Proof of COVID-19 Vaccine Certificates** in Ontario
- **Letter to Dr. Catherine Zahn and Hillary Hartley** regarding Proof of Vaccination Certificates in Ontario
- Submission on Bill 106: **Obligations and authorities of Ontario Health Teams and access to records in electronic format**
- Submission on the **proposed amendment under PHIPA on the right to access records in electronic format**

RESOLUTIONS

The IPC frequently works with other regulators, within Canada and internationally, to coordinate policy positions and public education efforts. In 2022, the IPC led, co-led, sponsored and supported several national and international resolutions and joint statements.

INTERNATIONAL

- **Resolution on Principles and Expectations for the Use of Personal Information for Facial Recognition**, adopted by Global Privacy Assembly, November 2022
- **Resolution on International Cooperation Capacity Building for Improving Cybersecurity Regulation and Understanding Cyber Incident Harms**, adopted by the Global Privacy Assembly, November 2022
- **Access to information as a milestone of the digital age to guarantee human rights, the inclusion of groups in situations of vulnerability and the strengthening of democratic institutions in the 21st century**, statement by members of the International Conference of Information Commissioners, June 2022

NATIONAL

- **Ensuring the Right to Privacy and Transparency in the Digital Identity Ecosystem in Canada**, resolution adopted by Canada's federal, provincial, and territorial privacy commissioners, September 2022
- **Securing Public Trust in Digital Healthcare**, resolution adopted by Canada's federal, provincial and territorial privacy commissioners, September 2022
- **Recommended Legal Framework for Police Agencies' Use of Facial Recognition**, joint statement adopted by Canada's federal, provincial and territorial privacy commissioners, September 2022

INFORMAL POLICY CONSULTATIONS AND ENGAGEMENT

In 2022, and as part of our statutory power to offer comments on proposed government programs as well as custodians' proposed information practices upon request, we invited organizations to consult the IPC as they develop new programs, initiatives, projects or processes with implications for data privacy or transparency. Many organizations took us up on our offer and reached out to request a policy consultation with our office. For a full list of informal consultations, visit our [consultations webpage](#).

PUBLIC EDUCATION AND OUTREACH

Under her enabling laws, the commissioner may conduct public education programs and provide information concerning Ontario's access and privacy laws, her role and her office's activities. In 2022, the commissioner and her team issued a number of multimedia guidance materials, delivered over forty presentations to various audiences, posted monthly blogs, and released monthly podcasts on access and privacy issues that matter to Ontarians.

GUIDANCE

- [Privacy guidance on facial recognition for police agencies](#)
- [How to protect against ransomware](#)

WEBINARS

- [How to report PHIPA breach statistics](#)
- [How to report PHIPA access and correction statistics](#)
- [How to report access and correction statistics under FIPPA/MFIPPA](#)
- [How to report access, correction, and breach statistics under Part X of the CYFSA](#)
- 2022 Data Privacy Day, [Empowering a New Generation of Digital Citizens](#)

COMMISSIONER BLOGS

Commissioner Kosseim regularly blogs about issues relating to privacy, access, cyber safety, and more. For a full list of 2022 blogs, visit the [Commissioner's Blog](#).

VIDEOS

- [Privacy tips for kids](#)
- [How to file an FOI request](#)
- [Health information privacy rights](#)
- [How to protect yourself online](#)
- [How to avoid phishing attacks](#)

PRESENTATIONS

In keeping with our focus on outreach, engagement, and collaboration, the IPC actively participated in a number of events and conferences during 2022. The commissioner, assistant commissioners, and legal, policy, and tribunal staff delivered speeches and participated in several discussion panels. For a full list of 2022 presentations, visit our [media centre](#).

INFO MATTERS PODCAST

In 2022, the IPC released a second season of *Info Matters*, a podcast about people, privacy, and access to information. As host, Commissioner Kosseim spoke with experts about issues relating to synthetic data, police use of investigative genetic genealogy, body-worn cameras, youth privacy and digital literacy, and more. For a full list of podcast episodes, visit our [Info Matters webpage](#).

IPC IN THE MEDIA

The IPC responded to 73 media requests in 2022 and was mentioned in the media more than 600 times. We were front and centre in several high-profile matters in 2022, including:

- An [op-ed in the *Toronto Star*](#) on the dangers of employee privacy
- A radio interview with CHOQ-FM on Data Privacy Day for [Francophone audiences](#)
- A panel discussion on the use of DNA evidence in law enforcement on TVO's [The Agenda](#) with Steve Paikin
- Discussion about [designing a privacy regime for the age of artificial intelligence](#), on the Canadian Bar Association's podcast, *Modern Law*
- An [interview with *Municipal World*](#) about IPC's Transparency Challenge

IPC IN THE COURTS

3



LEGAL
HEARINGS

8



JUDICIAL
REVIEWS

CABINET OFFICE || P0-3973

The Court of Appeal dismissed the government's challenge of an IPC decision ordering Cabinet Office to disclose the Premier's mandate letters, which set out policy priorities that cabinet members were responsible for implementing following the 2018 election. The court held the IPC was reasonable in finding the mandate letters were not exempt under section 12 of FIPPA because they did not "reveal the substance of deliberations" of the Premier or cabinet. The Supreme Court of Canada granted the Ontario government leave to appeal the decision. The appeal was heard on April 18, 2023, and we await the court's decision.

CITY OF MISSISSAUGA || MO-4176

The Divisional Court dismissed a challenge of an IPC decision ordering the City of Mississauga to disclose a list of voters who received an election ballot in a particular electoral ward. The court found that the IPC's decision to order disclosure of the voters' list was reasonable in the circumstances based on the IPC's interpretation of section 14(1)(d) of MFIPPA, section 88(5) of the *Municipal Elections Act* and previous decisions of the IPC and the court.

YORK UNIVERSITY AND YORK UNIVERSITY DEVELOPMENT CORPORATION || P0-3922 + P0-4029-R

York University and the York University Development Corporation (YUDC) challenged an IPC decision that found the university had control over certain documents created by the YUDC. The Divisional Court dismissed both challenges. The court upheld the IPC's finding that York did have control over these YUDC documents. The court agreed the IPC was reasonable in holding that, in the context of their reconsideration request, York University and the YUDC were responsible for showing that the records were not in York University's control. The court further held the IPC was reasonable in identifying the appropriate legal test for control and applying that test to the facts.

UBER CANADA INC. AND UBER B.V. || P0-4149

Uber sought to judicially review the IPC's decision upholding a decision of the Workplace Safety and Insurance Board (WSIB) that



granted partial access to records contained in the WSIB employer account for Uber. The IPC concluded the records were in the custody and control of the WSIB and were not excluded under the labour relations exclusion of FIPPA. The IPC further found that the records were not exempt from disclosure under section 17(1) of FIPPA (third party records) and that Uber was not permitted to raise section 14(2)(a) of FIPPA (exemption for law enforcement reports) in the circumstances. Uber subsequently discontinued the application for judicial review, and the Divisional Court dismissed the application.

LIFELABS

In June 2020, the IPC and the Office of the Information and Privacy Commissioner for British Columbia (OIPC) completed a joint investigation into the cyberattack on LifeLabs' computer systems. The IPC and OIPC found that LifeLabs did not comply with its obligations under PHIPA and British Columbia's *Personal Information Protection Act*, including in its failure to take reasonable steps to safeguard the personal information and personal health information of millions of Canadians. The IPC and OIPC made several orders to address these failures. LifeLabs complied with the orders but challenged a procedural decision made by the IPC and OIPC that found the information contained in their joint investigation report was neither privileged nor confidential. The IPC and OIPC had advised LifeLabs that they intended to publish the joint investigation report but the IPC and OIPC must wait for the court's ruling on whether any of the information in the report is privileged or confidential.

LifeLabs brought a motion in the judicial review application for the production of certain internal IPC documents. In October 2022, a single judge of the Divisional Court dismissed the motion. Following a further motion by LifeLabs, the single judge's decision was upheld by a three-judge panel of the Divisional Court in January 2023. The underlying application for judicial review regarding LifeLabs' claims of privilege and confidentiality over some of the information in the investigation report is still ongoing.

IPC OUTREACH BY THE NUMBERS

10

INFO MATTERS PODCASTS

12

COMMISSIONER BLOGS

42

PRESENTATIONS

73

MEDIA STATEMENTS

493

YOUTUBE SUBSCRIBERS

635

MEDIA MENTIONS

2,000

PRIVACY DAY
WEBCAST VIEWERS

2,659

SUBSCRIBERS

3,500

INFO CALLS

4,010

PODCAST DOWNLOADS

4,778

TWITTER FOLLOWERS

8,000

INFO EMAILS

9,860

LINKEDIN CONNECTIONS

19,012

YOUTUBE VIDEO VIEWS

152,317

WEBSITE VISITS

As at December 31, 2022

THE IPC'S YEAR AT A GLANCE

JAN

Privacy Day:
Empowering a
new generation of
digital citizens

FEB

Reaching out to
Franco-Ontarians

MAY

First IPC review of
an Inter-ministerial
Data Integration
Unit under FIPPA

IPC releases PHIPA
Decision 175; Ripe
for public debate:
Legal and ethical
issues around
de-identified data

JUN

IPC invites policy
consultations and
sets out rules of
engagement

IPC sponsors
declaration at
International
Conference of
Information
Commissioners

OCT

IPC launches
Transparency
Challenge

IPC updates its
ransomware
guidance

IPC and FPT counterparts issue joint resolution,
Ensuring the Right to Privacy and Transparency in
the Digital Identity Ecosystem in Canada

MAR

Remarks to Legislative Assembly on employee monitoring

APR

Recommendations on proof of vaccination certificates in Ontario

Submission on Bill 106: Ontario Health Teams' access to e-records

Op-Ed: Bill 88 needs to go further to protect the privacy rights of workers

JUL

Commissioner's blog: Privacy and humanity on the brink

AUG

IPC launches secure e-appeals

SEP

IPC welcomes its first scholar-in-residence!

IPC joins national call to retire fax machines and secure digital communications in health care delivery

NOV

IPC co-led resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology adopted by Global Privacy Assembly

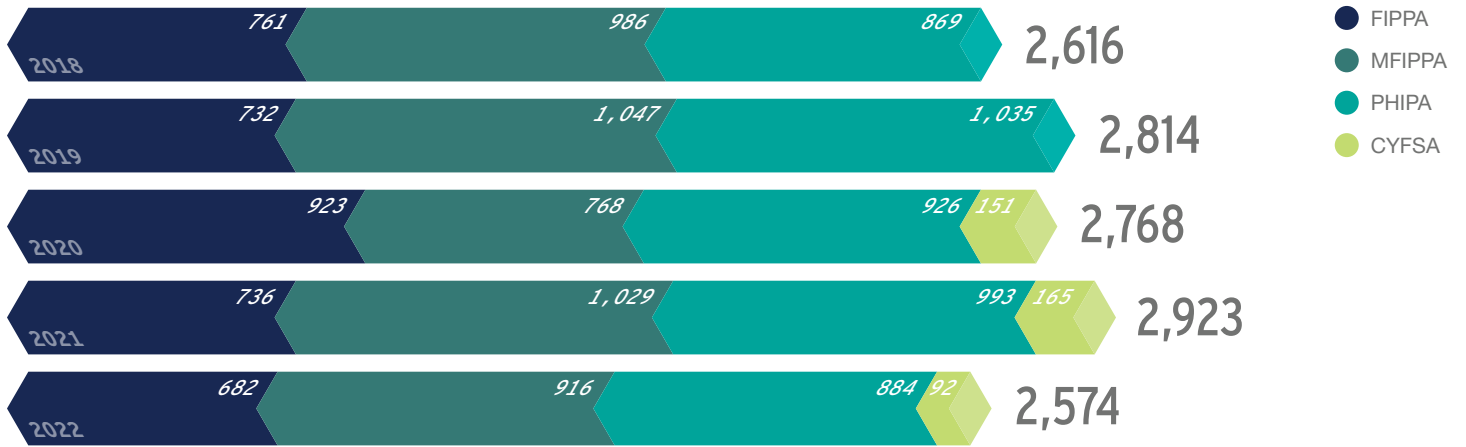
DEC

IPC on Instagram!

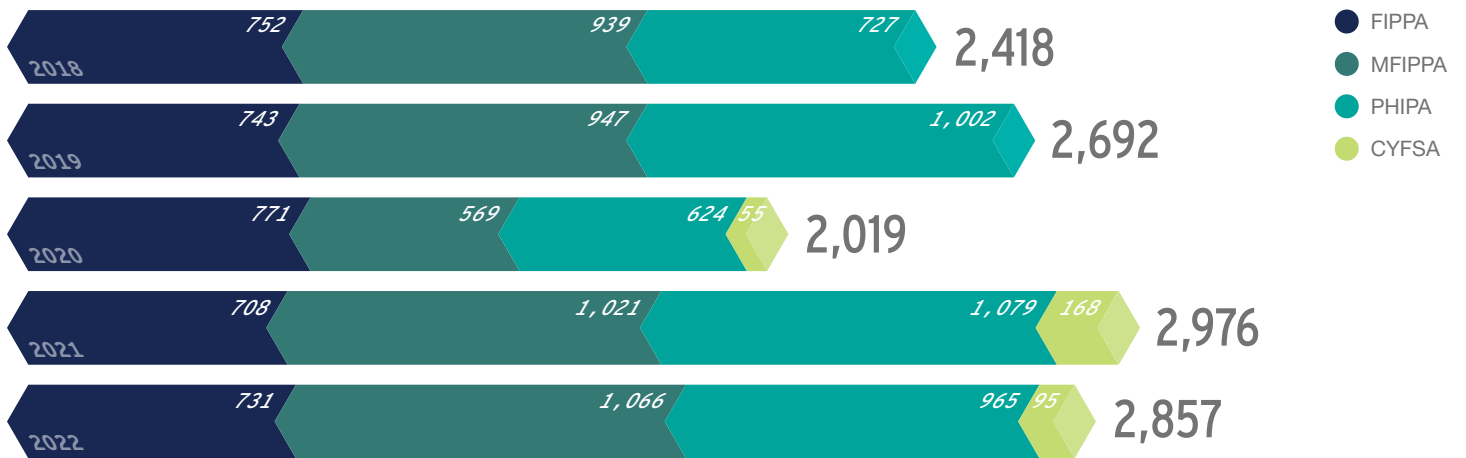
Commissioner's reflections on 2022: We listened, we learned, we did things

OVERALL FILES

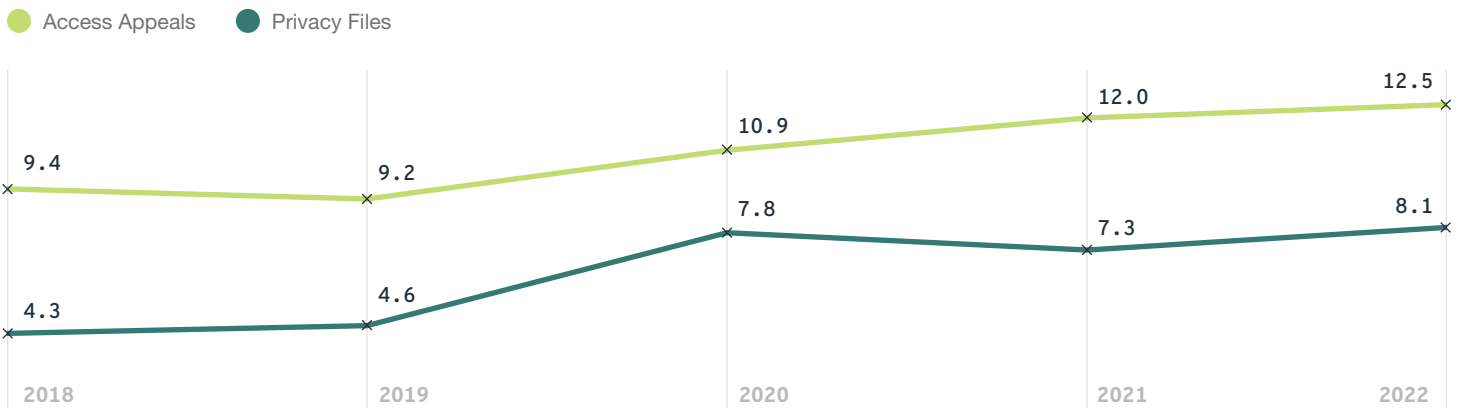
OVERALL OPENED FILES 2018-2022

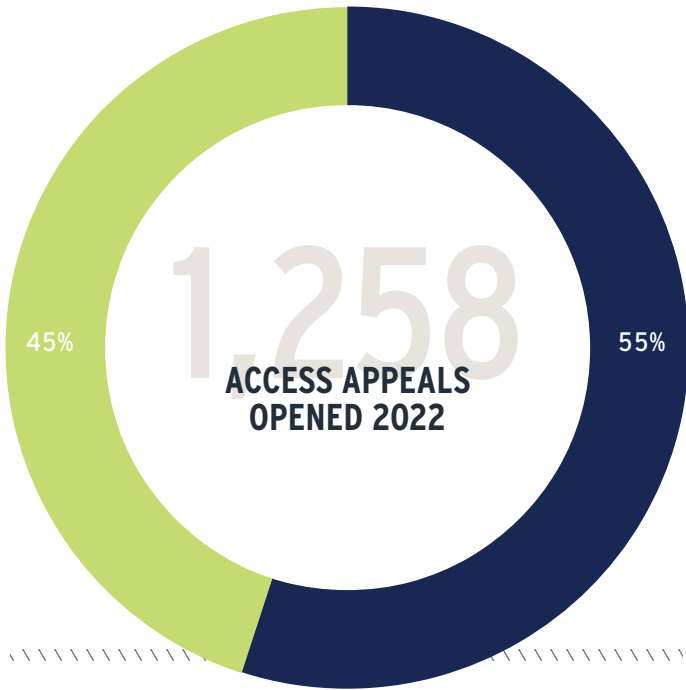


OVERALL CLOSED FILES 2018-2022



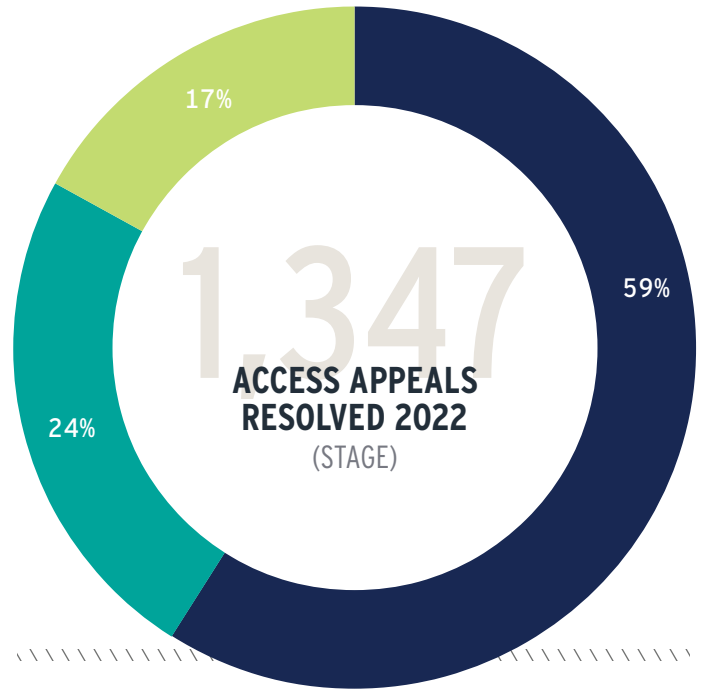
AVERAGE DURATION TO PROCESS AND CLOSE A FILE 2018-2022 (MONTHS)





- Municipal 697
- Provincial 561

Access appeals opened, by jurisdiction



- Mediation 794
- Adjudication 326
- Early Resolution 227

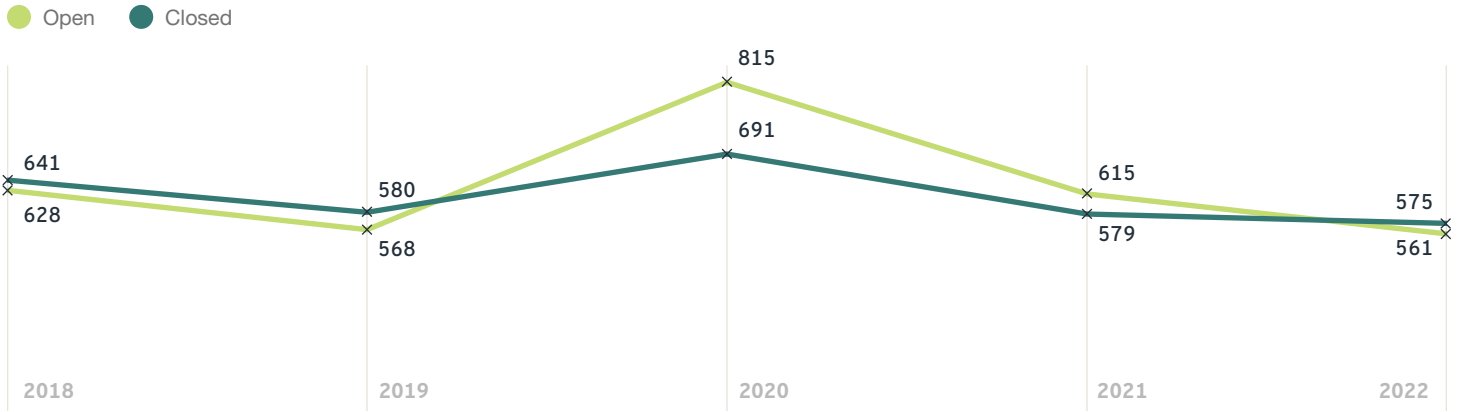
Access appeals resolved, by stage

ISSUES IN ACCESS APPEALS OPENED IN 2022

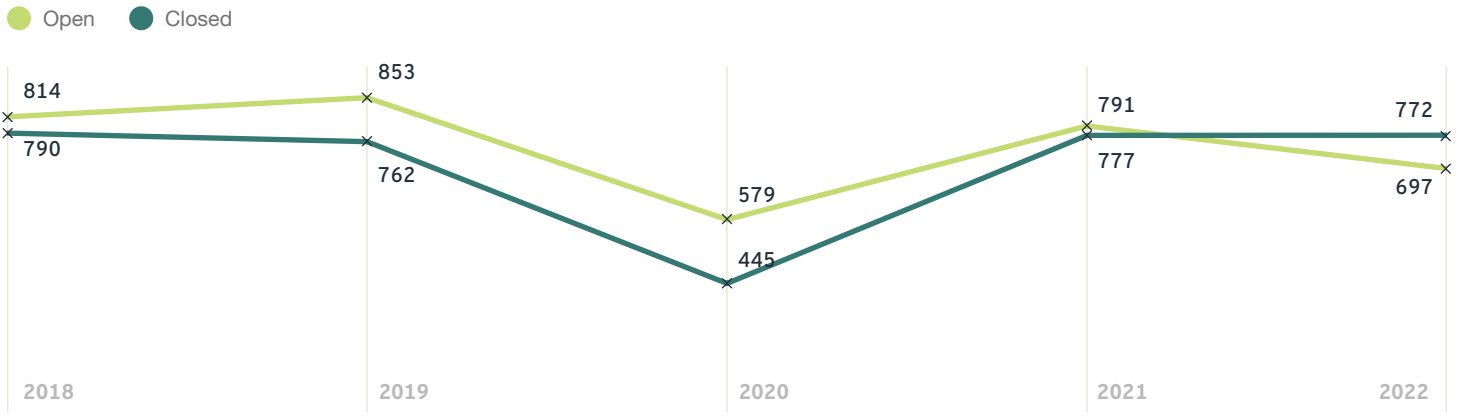


FIPPA / MFIPPA FILES

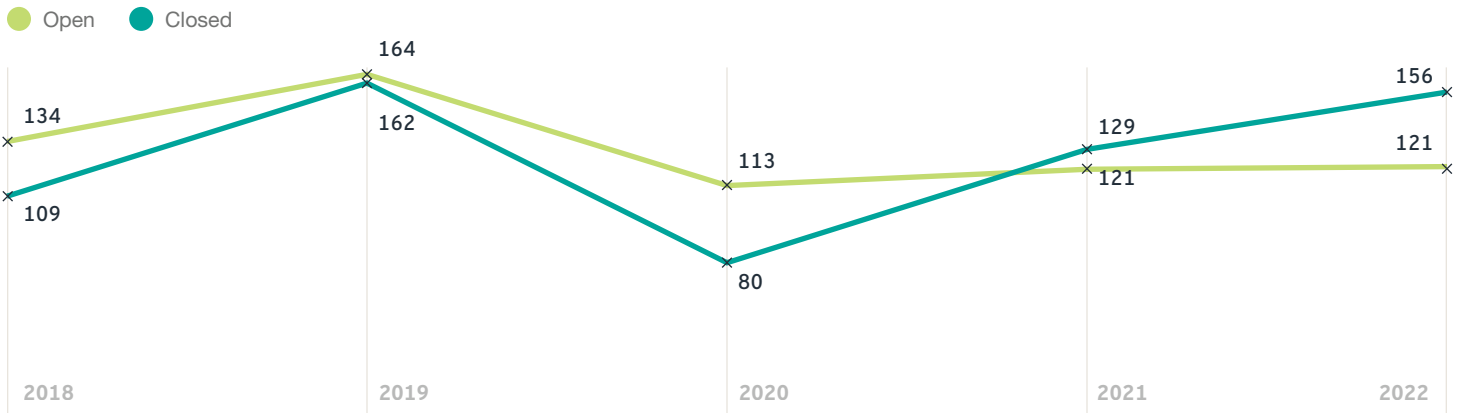
PROVINCIAL ACCESS APPEALS OPENED/CLOSED 2018 - 2022

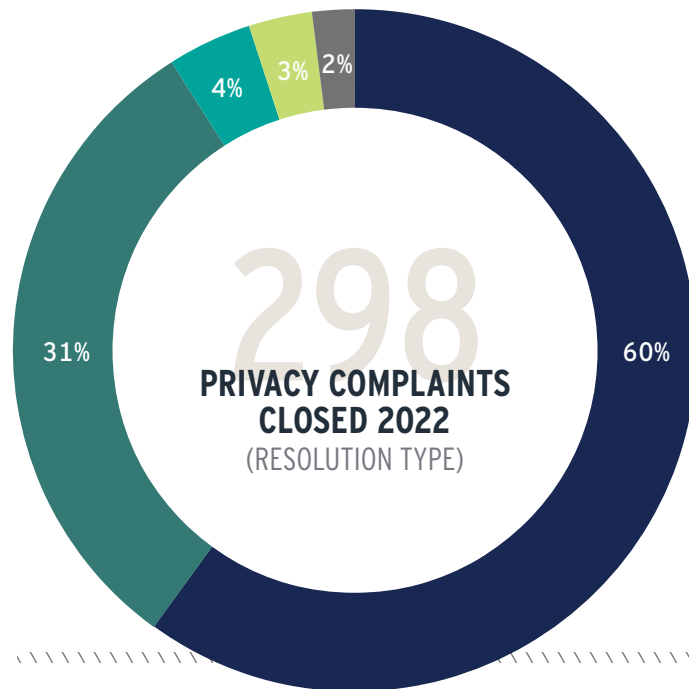
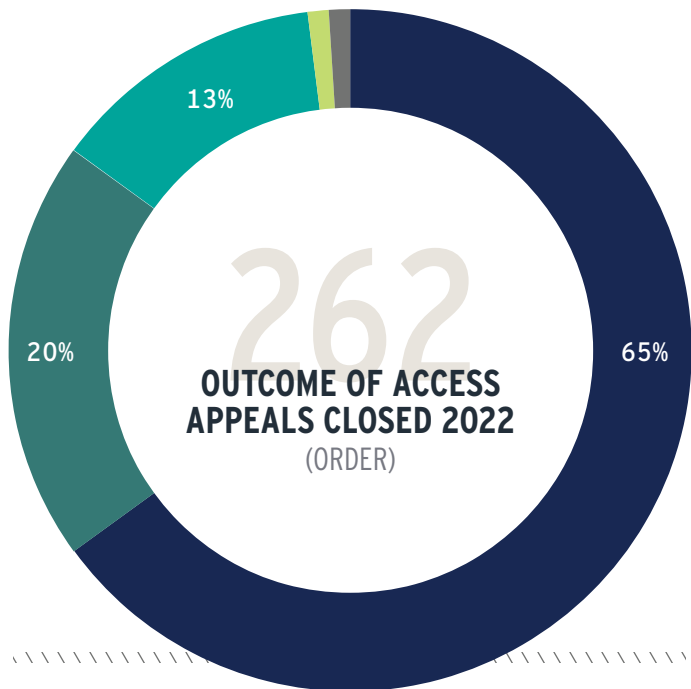


MUNICIPAL ACCESS APPEALS OPENED/CLOSED 2018 - 2022



PROVINCIAL PRIVACY COMPLAINTS & SELF-REPORTED BREACHES OPENED/CLOSED 2018 - 2022





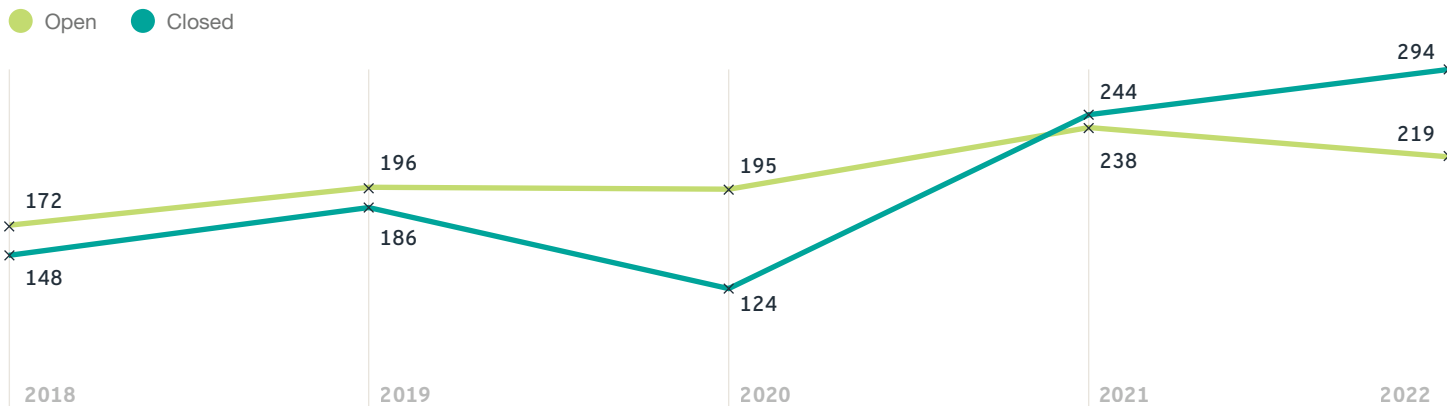
- Institution's decision upheld 170
- Institution's decision partially upheld 52
- Institution's decision not upheld 35
- Dismissal after representations 2
- Other 2
- No Inquiry 1

- Screened Out 179
- Resolved 92
- Withdrawn 13
- Report 8
- Abandoned 6

Does not include files that were resolved, abandoned, withdrawn or dismissed without an inquiry during adjudication

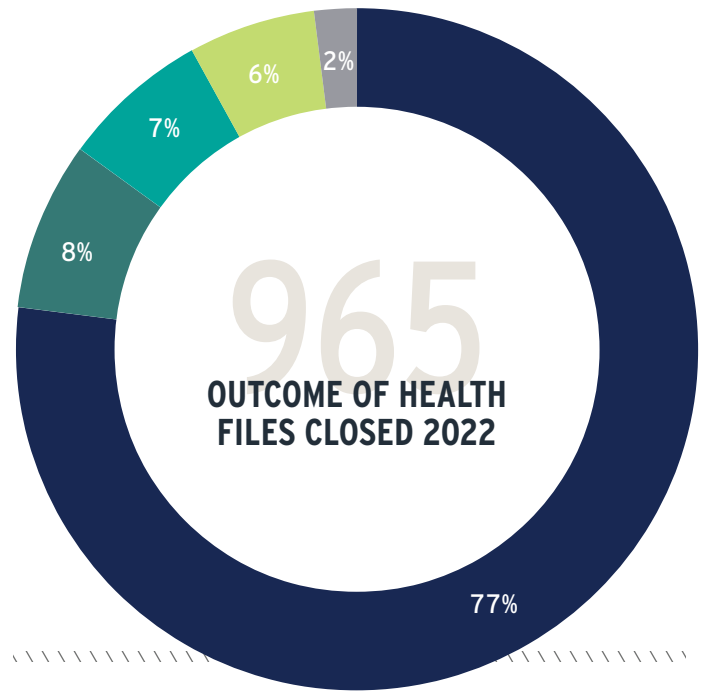
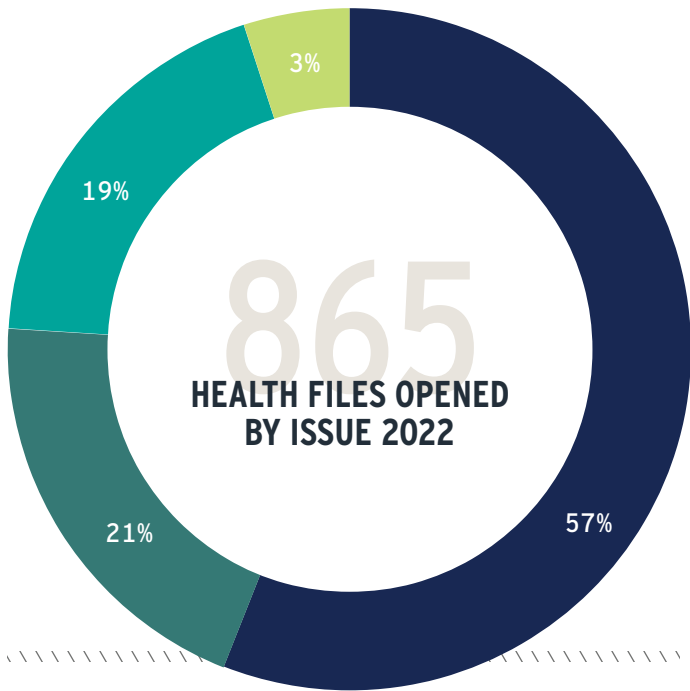
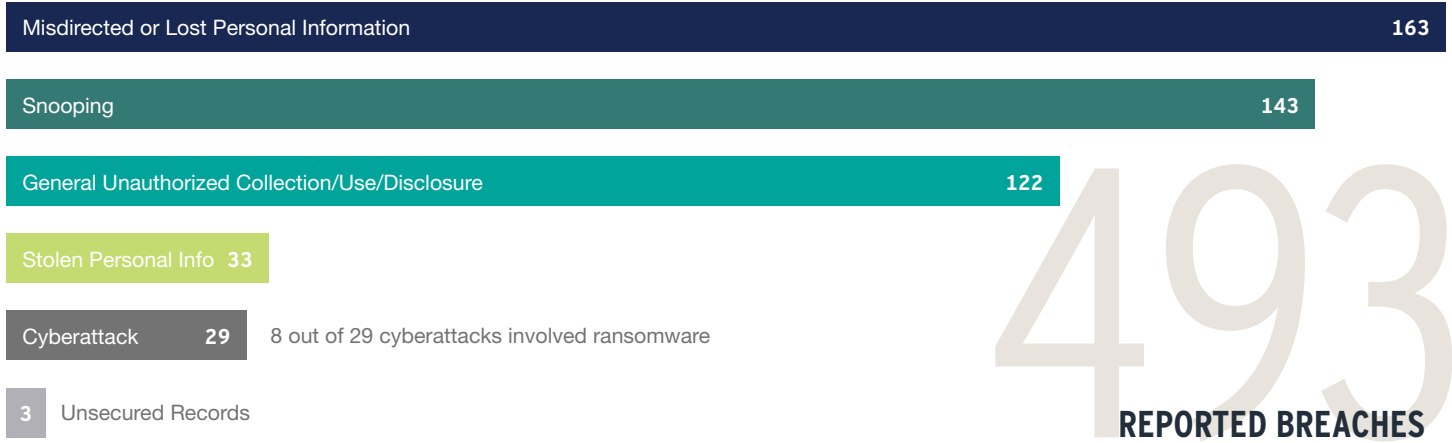
Self-Reported Breaches were processed separately. The total of 152 self-reported breaches closed in 2022 included 150 resolved, 1 screened out and 1 withdrawn

MUNICIPAL PRIVACY COMPLAINTS & SELF-REPORTED BREACHES OPENED/CLOSED 2018 - 2022



PHIPA FILES

SELF-REPORTED HEALTH PRIVACY BREACHES BY CAUSE 2022

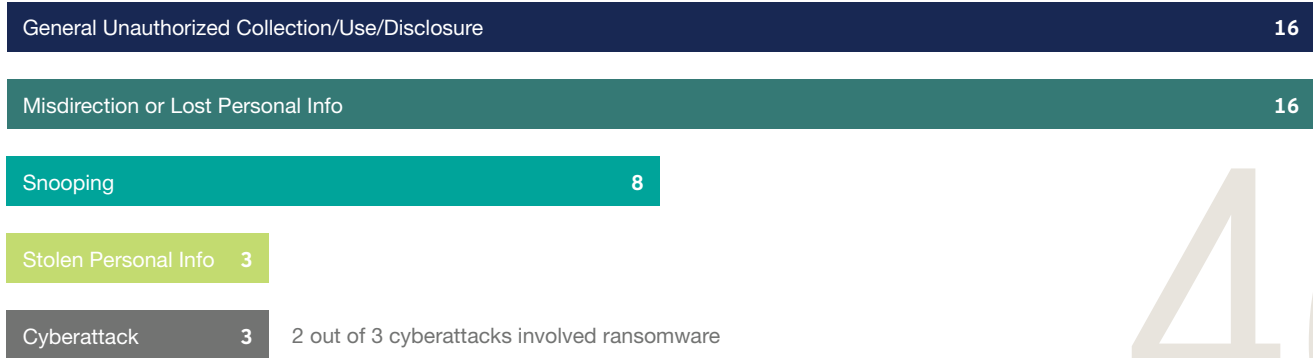


● Reported Breach	492
● Access/Correction Complaint	180
● Collection/Use/Disclosure Complaint	163
● IPC-initiated	30

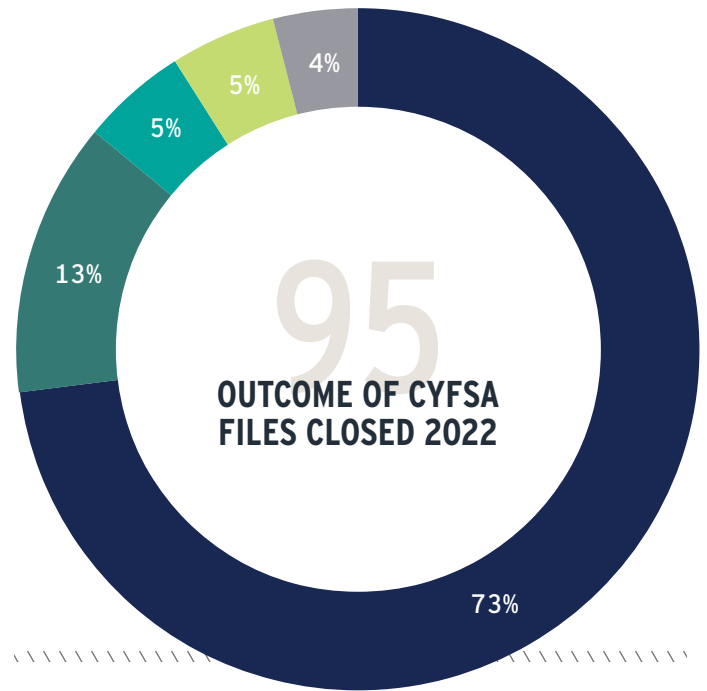
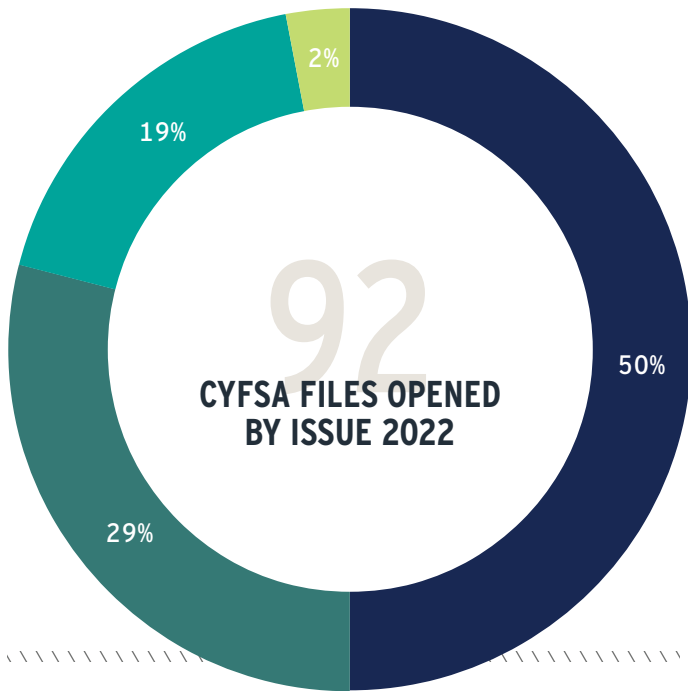
● Resolved	745
● Screened Out/Dismissed	75
● Withdrawn	67
● Abandoned	58
● Order/Decision Issued	20

1 out of 20 orders/decisions issued was an interim order

SELF-REPORTED CYFSA PRIVACY BREACHES BY CAUSE 2022



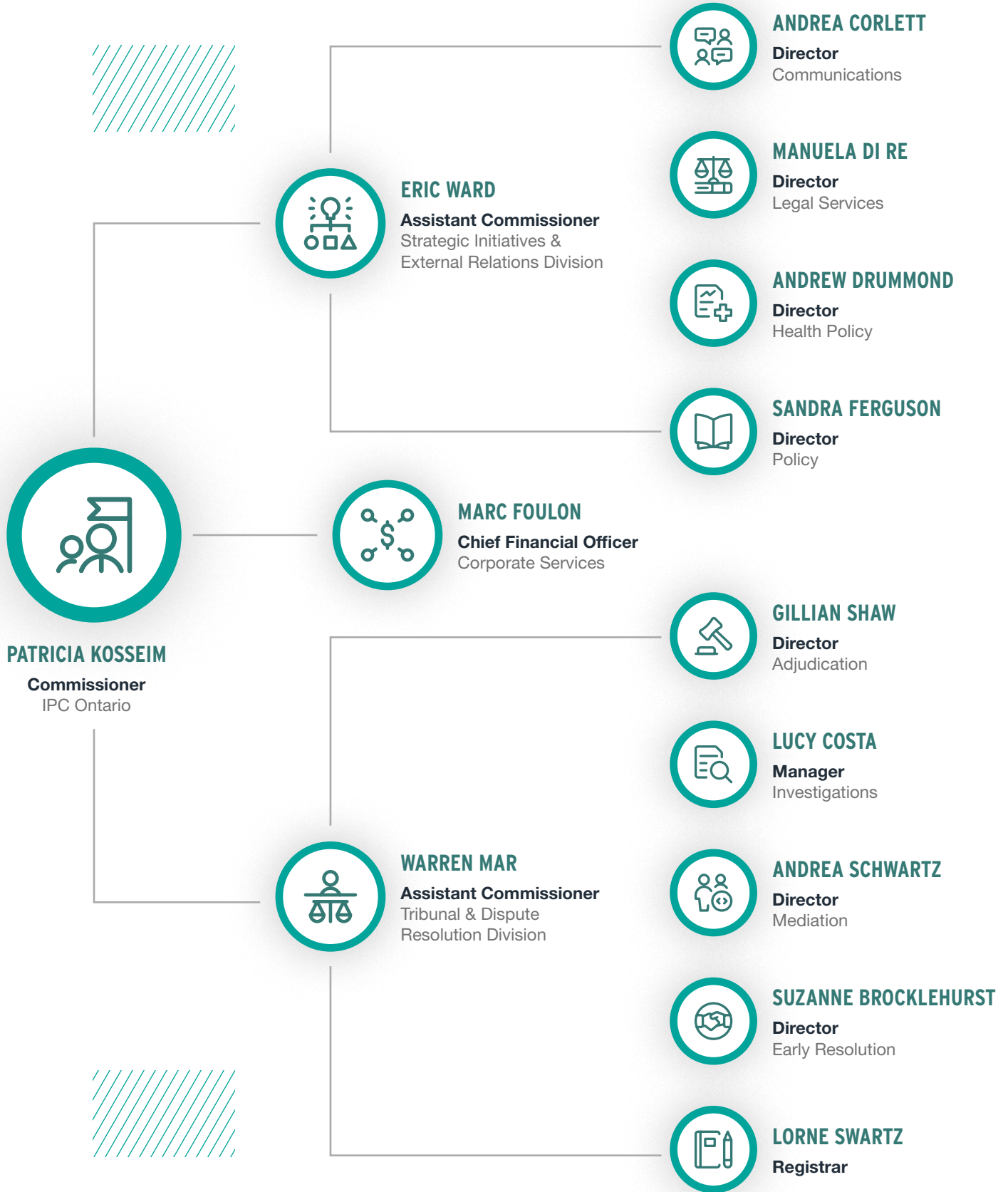
46
REPORTED BREACHES



● Reported Breach	46
● Access/Correction Complaint	27
● Collection/Use/Disclosure Complaint	17
● IPC-Initiated Collection/Use/Disclosure Complaint	2

● Resolved	69
● Screened Out	12
● Withdrawn	5
● Abandoned	5
● Order/Decision Issued	4

YOUR IPC TEAM



STRENGTHEN IPC GOVERNANCE AND ACCOUNTABILITY

In 2022, the IPC continued to strengthen its internal management and governance capacity by providing leadership and management training programs to its senior leaders and managers.

The IPC continued to enhance its modern controllership and fiscal best practices to ensure responsible use and greatest value of public funds. In this regard, the IPC met our financial target of a year-end balanced budget by spending within one per cent of our budget. As per the *Freedom of Information and Protection of Privacy Act* R.S.O. 1990, CHAPTER F.31, the financial statement of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario.

As part of our 2022-23 annual planning cycle, we proposed further enhancements and changes to our organizational structure and operations to enhance accountability and deliver on the IPC's evolving and growing mandate effectively. We look forward to implementing these improvements in 2023 and will report further on them in our next annual report.



FINANCIAL SUMMARY	2022-2023 ESTIMATE (UNAUDITED)	2021-2022 ESTIMATE (UNAUDITED)	2021-2022 ACTUAL (UNAUDITED)
SALARIES AND WAGES	\$14,900,500	\$14,433,300	\$14,322,327
EMPLOYEE BENEFITS	\$3,980,400	\$4,138,200	\$3,325,188
TRANSPORTATION AND COMMUNICATIONS	\$122,000	\$132,900	\$124,202
SERVICES	\$3,492,400	\$3,125,700	\$3,737,032
SUPPLIES AND EQUIPMENT	\$137,000	\$122,500	\$184,591
TOTAL	\$22,632,300	\$21,952,600	\$21,693,340

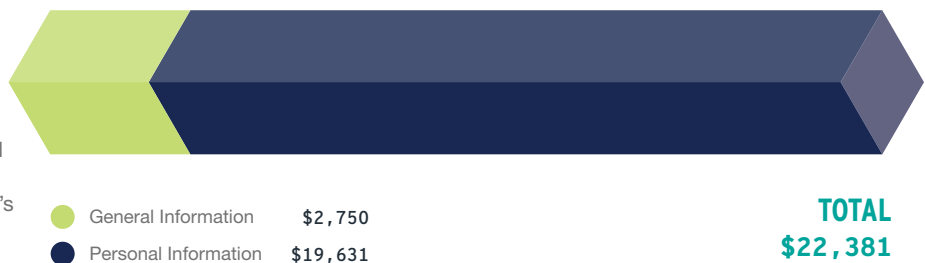
Notes:

1. The IPC's fiscal year begins April 1 and ends March 31.
2. Financial figures are rounded to the nearest dollar and are prepared on a modified cash basis.
3. The financial statement of the IPC is audited on an annual basis by the Office of the Auditor General of Ontario

2022 APPEALS FEES DEPOSIT (CALENDAR YEAR)

Note:

Appeal fees are payable to the Minister of Finance and these fees are not transferred to the Information and Privacy Commissioner of Ontario (IPC). Therefore, IPC's Financial Statement does not include appeal fees.





Information and Privacy
Commissioner of Ontario

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

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

(416) 326-3333

info@ipc.on.ca

www.ipc.on.ca