



BEYOND IMAGINATION: PLANNING FOR ONTARIANS' DIGITAL FUTURE

2023 Annual Report

Advocacy
Responsiveness
Accountability



Information and Privacy
Commissioner of Ontario

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

Letter to the speaker

June 5, 2024

The Honourable Ted Arnott
Speaker of the Legislative Assembly of Ontario

Dear Mr. Speaker,

I am honoured to present the IPC's annual report for 2023, *Beyond Imagination: Planning for Ontarians' Digital Future*. This report covers the period of January 1 to December 31, 2023.

As a regulator that strives to be modern and effective with real world impact, the IPC is committed to supporting a secure digital future for Ontario, where residents have confidence in the protection of their privacy and access rights. We aim to strengthen trust in public services by proactively advancing their access and privacy rights in key areas that significantly impact Ontarians' daily lives, resolving their complaints and appeals in a fair, timely, and meaningful manner, and upholding the IPC's reputation for organizational excellence.

The year 2023 marked significant strides in advancing access and privacy rights in Ontario. This report offers an overview of our work over the past year and our strategic plans and recommendations to help Ontarians embrace their digital future with confidence, hope, and optimism.

For further details, including comprehensive statistics and in-depth analyses, please visit our website at ipc.on.ca/about-us/annual-reports.

Yours sincerely,



Patricia Kosseim
Information and Privacy Commissioner of Ontario

Contents

Commissioner's message	2	Accountability:	
Innovation meets accountability.....	4	Maintaining Ontarians' confidence in the organizational excellence of the IPC	28
Advocacy:		The IPC's digital transformation in action	29
Proactively advancing Ontarians' rights in key strategic areas that impact their lives	6	Cultivating the best: The IPC's journey as an employer of choice	31
Privacy and transparency in a modern government	7	Continuing to strengthen governance and accountability	31
Children and youth in a digital world	12	Lending our voice for change:	
Trust in digital health	15	Submissions to government	32
Next-generation law enforcement	18	United we stand: National and international resolutions	34
Responsiveness:		Engage and influence: Stakeholder consultation and guidance	34
Addressing complaints and appeals in a fair, timely and meaningful manner	20	Presentations	35
Clearing the slate: Strategies to eliminate file backlogs	21	IPC outreach by the numbers in 2023	37
Procedural clarity: Updates to FIPPA/MFIPPA code of procedure	21	IPC in the courts.....	39
Interpretation Bulletins: Guidance simplified.....	22	The IPC's year at a glance	40
A review of noteworthy cases.....	22	Statistical highlights	42
Insightful analytics.....	27	Organizational chart	48
		Financial summary	49

Commissioner's message



“As we navigate our rapidly evolving digital world, the IPC’s mission is resolute – to enhance Ontarians’ trust that their privacy and access rights will be respected.”

“The future depends on what you do today.”

Mahatma Gandhi’s prophetic words remind us that our future is not predestined but is shaped instead by our present choices and actions. To me, this means being proactive, embracing change, and using our collective efforts and ingenuity to unlock new possibilities and build a better future for Ontarians.

As we navigate our rapidly evolving digital world, the IPC’s mission is resolute — to enhance Ontarians’ trust that their privacy and access rights will be respected. Our annual report offers an overview of our work over the past year to further this mission. It also describes our strategic plans and recommendations to address the access and privacy challenges that lie ahead in a future beyond imagination, where every aspect of our lives will be affected by technology in some way, shape or form.

Preparing the next generation of digital citizens

With an eye toward the future, we are preparing the younger generation to navigate the digital landscape with knowledge and confidence. In 2023, we continued to prioritize the digital literacy and privacy rights of Ontario’s children and youth. To this end, we launched educational tools like the *Privacy Pursuit!* lesson plans, established our first-ever Youth Advisory Council, and released a draft *Digital Privacy Charter for Ontario Schools*.

Recognizing that acting together is more effective than acting alone, I, alongside my federal, provincial, and territorial (FPT) counterparts, addressed the need to protect the privacy and access rights of young people across the country. During our 2023 annual FPT meeting in Québec City, we issued a unanimous **resolution** calling for legislative changes to strengthen privacy

safeguards, transparency requirements, and access to meaningful remedies for all young people in Canada. The resolution also called on both public and private sector organizations to protect the best interests of our youth and empower them to navigate digital platforms safely, with knowledge, agency, and autonomy.

Calling for guardrails around the emerging use of artificial intelligence (AI)

Without question, 2023 marked the year when AI, once a thing of a distant future, entered mainstream consciousness. As AI technology continues to explode at a breathtaking pace, the IPC recognizes the critical need for strong governance surrounding its use to earn and support public trust. This past year, we partnered with the Ontario Human Rights Commission to issue a **joint statement** that calls for much-needed guardrails that would allow Ontario to reap the benefits of AI technologies in a manner that is ethically responsible, accountable, sustainable, and human rights affirming. Together, our offices called upon the Ontario government to develop and implement binding rules governing AI technology use in the public sector, emphasizing the need to protect privacy and human rights, and uphold human dignity as a fundamental value.

We also joined our FPT counterparts to release *Principles for Responsible, Trustworthy, and Privacy-Protective Generative AI Technologies*. The principles are designed to provide practical guidance to organizations when developing, providing, or using generative AI models, tools, products, and services. The principles support transparency and accountability, emphasize the importance of accuracy, and are intended to mitigate privacy risks, particularly for vulnerable and historically disadvantaged groups who experience systemic discrimination or bias.

Our provincial and national efforts were further amplified at the international level. In 2023, the IPC co-sponsored two AI-related **resolutions** at the 45th Global Privacy Assembly that were unanimously adopted by data protection and privacy authorities worldwide. These international resolutions — one on *Generative Artificial Intelligence Systems*, the other on *Artificial Intelligence and Employment* — sounded a clarion call for governments around the world to adopt core data protection principles to govern the development, operation, and deployment of existing and emergent AI systems.

Adopting strategic foresight to prepare for our digital future

Throughout 2023, my office devoted significant efforts to deepen our understanding of emerging technologies and prepare for their potential future impacts on Ontarians through our *IPC Privacy Futures Project*. Using strategic foresight methodology, we examined investigative genetic genealogy (IGG) in the law enforcement context by engaging a diverse range of experts, including government policymakers, forensic scientists, genetic genealogists, civil society groups, academic experts, bioethicists, police services, and First Nations leaders.

By engaging a broad community through a deliberate strategic foresight approach, we are better positioned to imagine plausible scenarios and anticipate their technological implications. This helps us develop more effective strategies to address potential challenges in complex areas and help shape regulatory regimes that will lead us toward a more desirable future.

Future-proofing Ontario’s access and privacy laws

To prepare for the uncertainties of a digital future, legislators worldwide are modernizing access and privacy laws to protect their citizens from a whole new generation of risks associated with cybersecurity and artificial intelligence. Ontario must do the same.

Over the past year, my office has actively developed our policy positions and law reform recommendations in the public, health, and children, family, and youth services contexts. The future is here, and it demands heightened accountability, transparency, and oversight of public institutions to reassure Ontarians that their access and privacy rights will be protected in this rapidly changing digital world. To thrive, Ontarians need to trust that their public institutions adhere to stringent data standards and requirements to minimize risks of harm, while maximizing opportunities for a promising and prosperous future. Now more than ever, there is a critical need for reliable and trustworthy sources of information and rights protection.

Building a digitally modern and sustainable organization

Planning for a digital future also requires us, as an organization, to modernize our technological capacity and ensure the sustainability of resources in a context of ever-increasing demand for our services. Throughout 2023, we continued to advance our multi-year strategy to strengthen our information technology infrastructure, improve our digital collaboration tools and processes, and enhance online access to our services for all Ontarians.

Our commitment to plan and prepare for a sustainable future also led to significant process improvements and enhancements to our tribunal services. These efforts underscore our dedication to providing fair, timely, and meaningful resolution of appeals and complaints in a transparent, effective, and efficient manner. Ontarians expect no less of us today, and every indication is that their demand for our services will exponentially increase in the future — particularly as cybersecurity and ransomware threats continue to escalate — and the need for truth and transparency becomes more important than ever in an age of generative AI.

A year in review, with an eye on the future

While this annual report summarizes the past year’s activities, it focuses particularly on the deliberate steps we have taken to prepare for, and help shape, Ontario’s digital future. The initiatives outlined in this report are not just one-off accomplishments; they are the roadmap to our multi-year journey towards a secure digital future for all Ontarians, ensuring that privacy and access rights remain at the forefront.

I want to extend my deepest gratitude to the IPC’s **Strategic Advisory Council** and **Youth Advisory Council** for their invaluable guidance and support throughout the year.

Last but not least, the dedication and commitment of my staff have been instrumental to our success, and I cannot thank them enough for their tireless efforts.

Patricia Kosseim
Commissioner

Innovation meets accountability

VISION

To be a modern and effective regulator with real-world impact

MISSION

Enhance Ontarians' trust that their privacy and access rights will be respected by:

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.



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.

CROSS-CUTTING STRATEGIES

1.

We will consider accessibility and equity issues to help reduce disparate outcomes for marginalized communities.

2.

We will strive to be consultative and collaborative with relevant partners and stakeholders.

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.

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.



ADVOCACY:

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

PRIVACY AND TRANSPARENCY IN A MODERN GOVERNMENT



Our goal in this priority area 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.

Navigating the AI landscape: Joint IPC-OHRC statement on responsible use of AI

In 2023, the IPC and the Ontario Human Rights Commission (OHRC) jointly issued a **statement** urging the Ontario government to develop effective safeguards governing the use of AI technologies within the public sector. The statement emphasized the pressing need for a robust, binding set of rules to harness AI benefits responsibly and sustainably. Without adequate governance protocols, the potential societal advancements offered by AI in health care, education, and public safety may be put at risk and public trust may falter.

Together with the OHRC, we called upon the Ontario government to establish clear and binding guardrails around the public sector's use of AI technologies that effectively address safety, privacy, accountability, transparency, and human rights. Our organizations also committed to working together to identify and promote guiding principles and leading practices associated with building a responsible, safe, and trustworthy AI framework that upholds human dignity as a fundamental value.



We urge the government to continue showing leadership by pressing forward with a robust, granular, and binding framework for the responsible use of artificial intelligence technologies by public sector organizations. Clear and effective guardrails are needed to ensure the benefits of AI don't come at the cost of Ontarians' privacy and other fundamental human rights. Ontarians may want their public sector institutions to deploy AI technologies for the public good, but only if it is safe, transparent, accountable, and ethically responsible. Ultimately, innovative uses of AI must be supported and sustained by public trust. ”

A national perspective on responsible innovation: Principles for generative AI

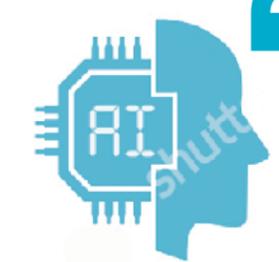
Our call for responsible AI governance was escalated at the national level, as we, along with our FPT counterparts, released comprehensive principles to guide the responsible and trustworthy deployment of generative AI technologies in Canada. The principles offer clear guidance on ethical, transparent, and accountable adoption and implementation of AI technologies, with particular focus on the unique challenges posed by generative AI. They are intended to help organizations build privacy protection into the design of generative AI tools and throughout their development, provision, adoption, and downstream use. The principles are devised to mitigate risk and promote the safe creation of AI technologies. Particular consideration is given to protecting vulnerable and historically marginalized groups, and ensuring generative content that could significantly impact individuals is transparently identified as having been created by a generative AI tool.

This FPT initiative, among several others throughout 2023, reflects our proactive and collaborative approach to harmonizing privacy protection nationwide. This joint effort also reflects our collective commitment to ensuring that rapidly evolving technologies are harnessed to respect and protect the privacy of individuals and groups while still enabling innovation.

Addressing AI on the global stage

AI governance was a topic of universal concern internationally as well. At the **45th Global Privacy Assembly** in October, Commissioner Koseim led a panel discussion about how AI technologies can, and sometimes do, inflict harm on individuals and communities and what we need to do about it. The panel was comprised of a diverse group, including an investigative journalist, privacy experts, civil society members, and data protection regulators across three continents. The discussion delved into pivotal questions about individual and community harms associated with AI and the critical role data protection regulators must play as the front line of defence while collaborating with other relevant regulators.

The IPC also proudly co-sponsored an international **resolution** focused specifically on the unique aspects of generative AI. Consistent with the principles laid out in our FPT resolution on generative AI, the international signatories unanimously recalled the fundamental importance of our democratic values, emphasizing the need for accuracy of information having potential impact on individuals and calling for transparency of AI-generated content.

“Artificial intelligence technologies, and generative AI in particular, have the potential to generate damaging content that can sustain unfair biases and discriminatory practices, putting privacy and other fundamental human rights at risk. Strong legal and ethical safeguards are needed to ensure that AI technologies are used in an accountable, transparent, and ethically responsible manner that fosters public trust.”



Federal, provincial, and territorial commissioners and ombuds, together with their staff, at the 2023 annual conference in Québec City.

New guidance on third party contracting

More and more, governments and public sector organizations rely on third party data processors in the private sector to leverage their capacity and expertise and gain efficiencies through economies of scale. Throughout 2023, the IPC worked on developing guidance for third party contracting practices [link](#) that addresses the privacy and access concerns associated with outsourcing. We drew inspiration from past findings and decisions of our tribunal and consulted various organizations to get their practical input from the ground.

Organizations can use this guidance, released in 2024, to better understand the privacy and access obligations that continue to rest with them, even when they contract out certain data processing functions to third party service providers. The guidance is intended to help organizations exercise due diligence and demonstrate the measures they have taken to ensure privacy and access issues are addressed throughout the procurement process from planning, tendering, vendor selection, negotiation and agreement management.

Privacy of Ontario workers

Throughout 2023, Commissioner Koseim continued to call on the government to address the serious gaps in statutory privacy protection for millions of Ontario workers. With the shift towards increased remote work arrangements, many employers have accelerated the use of monitoring technologies and AI as they seek new ways of tracking and evaluating employee performance. As a result, employees have never been under such intensive surveillance, creating undue stress and putting at risk their privacy in ways that may harm their productivity, creativity, autonomy, and mental well-being.

Given the power imbalance in the workplace, employees often have little bargaining strength and cannot speak up against the adoption of overly invasive technologies. They may have little to no recourse against unfair employment decisions made about them based on inaccurate inferences about their conduct, attitude, or behaviour, particularly in non-unionized environments. Those who suffer most disproportionately tend to



Advocacy

“ Digital technologies offer employees new ways of working. Through technology, we are able to engage in ways that were previously unimaginable. The future is here and it’s critical that governments and organizations act now to protect the privacy of workers, particularly in Ontario, where statutory gaps leave them vulnerable to the risks of digital surveillance. ”



“ Government-held information is a valuable source of accurate and truthful facts about present and historical events. It’s an antidote to the increasing spread of toxic misinformation, and disinformation, that erodes trust in our democratic institutions. This joint resolution urges our respective governments to strengthen access to information legislation, promote stronger information management practices and summon the courage it takes to build a culture of openness and transparency through proactive disclosure. ”

be individuals from marginalized and historically disadvantaged groups. For these important reasons, the IPC, in concert with our FPT colleagues, issued a joint resolution urging our respective governments to address any statutory gaps in their jurisdictions. The **resolution** also calls on all employers across the country to respect and protect employee rights to privacy and transparency and ensure the fair and appropriate use of electronic monitoring tools and AI technologies in the modern workplace. This call was reinforced by an international resolution on **artificial intelligence and employment**, co-sponsored by the IPC and unanimously adopted by the Global Privacy Assembly.

In early 2023, Commissioner Kosseim **wrote** to the ministers of Public and Business Service Delivery and Labour, Immigration, Training and Skills Development,

expressing serious concern with the lack of statutory privacy protections for the vast majority of Ontario workers and calling for urgent attention if Ontario is to become a leading digital jurisdiction in which to live and work.

In an age of electronic monitoring tools and artificial intelligence technologies, the privacy rights of employees, and indeed all Ontarians, must be more firmly entrenched in a comprehensive and coherent privacy regime, similar to what was proposed in the government’s 2021 white paper on **Modernizing Privacy in Ontario**. The IPC urges the government to resume its bold and ambitious efforts to address glaring gaps in statutory privacy protections in Ontario.

Celebrating democracy: Right to Know Week highlights

For Right to Know Week (RTKW) 2023, the IPC kicked things off with a **commissioner’s blog** and a podcast episode focused on breaking down barriers to access to information for women, ***A woman’s right to know: Closing the gender gap with access to information.*** Also, as part of RTKW celebrations, we launched a new suite of **Interpretation Bulletins**. These new resources are intended to codify our past interpretations of key provisions under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and its municipal counterpart, MFIPPA, to promote a greater understanding of Ontario’s access and privacy laws and help prospective parties in an appeal better anticipate what to expect.

On September 28, we endorsed a **statement** from the 14th **International Conference of Information Commissioners** (ICIC), emphasizing the importance of access rights as a fundamental pillar of social, economic, and democratic governance. Commissioner Kosseim’s endorsement highlighted how integral access to

“ Access to government-held information empowers individuals with knowledge and information to participate more fully in our democratic processes. The statement from the ICIC highlights the collective strength of its members working together to elevate access rights to the international agenda, acknowledging the importance of safeguarding these rights and encouraging the public to exercise them. ”

government-held information is for upholding democratic values. The ICIC statement commits to championing transparency and access to information, enhancing information disclosure practices, and encouraging public engagement to safeguard access rights.

During the 2023 annual gathering in Québec City, the IPC joined Canada’s information commissioners and ombuds in signing a joint **resolution** calling for comprehensive updates to access to information laws in dire need of modernization. The resolution emphasized the need for governments to update their respective access protocols and procedures, make significant investments in freedom of information resources, and embrace proactive disclosure as part of a broader culture of openness and transparency. These changes are particularly important now, with respect to historical records, to counter misinformation and advance our collective commitment to reconciliation.



Shining a light on excellence: Transparency Challenge

In 2023, the IPC let the sunshine in by showcasing the benefits of openness and transparency.

We called upon Ontario’s provincial and municipal governments and other public sector organizations to show us innovative examples of projects or initiatives that enhance government transparency or use open data to improve the lives of Ontarians. We were pleased to see institutions respond in such impressive numbers! Curated and displayed in a 3D virtual gallery, the **Transparency Showcase** celebrates the best of these examples. This novel online exhibit is intended to increase public awareness of the value of open government practices and encourage other public institutions to do the same through positive reinforcement.

“ Government transparency is essential to democracy and the healthy functioning of our society, fostering civic engagement, trust, and helping to counter misinformation. Through our Transparency Showcase we’re putting a spotlight on some compelling examples of open government initiatives to remind everyone of the benefits of transparency and open data and inspire government institutions to be more proactive in releasing information to the public. ”



INFO MATTERS

Info Matters episodes related to Privacy and Transparency in Modern Government

S3-Episode 2: Trust and truth: Navigating the age of misinformation

S3-Episode 3: A casual conversation between two Canadian privacy commissioners

S3-Episode 6: A woman’s right to know: Closing the gender gap with access to information

S3-Episode 7: Unmasking digital threats: How to guard against cyber crime



CHILDREN AND YOUTH IN A DIGITAL WORLD

Our goal in this priority area 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.



“Educators play an important role in equipping Ontario's children and youth with the knowledge and skills to navigate the digital world safely. By integrating privacy education into classrooms, we can empower students to protect their personal information, make informed choices, and become responsible digital citizens. Together, we can build a generation that values privacy and embraces the power of informed decision-making in the digital age.”

Reflecting on five years of the *Child, Youth and Family Services Act*

In July 2023, as part of the legislated five-year review of the *Child, Youth and Family Services Act* (CYFSA), the IPC provided **comments and recommendations** on ways to strengthen the access and privacy protections under the CYFSA and its regulations. Our submission called for the Ministry of Children, Community and Social Services to be subject to the act's requirements when acting as service provider and to ensure greater accountability when collecting, using, and disclosing the personal information of vulnerable children, youth, and families in Ontario.

October 27 marked Dress Purple Day, when children's aid societies across Ontario raise awareness about the important role that individuals and communities play in supporting vulnerable children, youth, and families. On this occasion, the IPC released new resources for individuals seeking to avail themselves of their privacy and access rights under Part X of the CYFSA. Based on our experience in interpreting and applying Part X, we updated our **frequently asked questions** to further elaborate on issues around consent and capacity, and clarified questions related to the custody and control of records held by child and family service providers.

FPT resolution on youth privacy

At our 2023 annual conference in Québec City, the IPC, together with our FPT counterparts, issued a joint resolution, **Putting best interests of young people at the forefront of privacy and access to personal information**.

Young people are increasingly susceptible to the unauthorized use and commercial exploitation of their personal information in ways that can negatively influence their behaviour and cause them harm. Yet, there are also wonderful opportunities for children to actively participate, grow, and flourish in the digital space. Recognizing this, the FPT privacy commissioners and ombuds discussed how to better protect youth's privacy while also empowering them to navigate through the online world with greater confidence and autonomy. The resulting FPT resolution urges our respective governments to

reform their laws to ensure stronger protections for the privacy rights of children and youth, more transparent data handling practices, and enhanced access to effective remedies for young people. The resolution also highlights the pressing need for proactive measures by both public and private sector organizations to adopt privacy best practices that prioritize the protection and empowerment of our youth in this digital age, including being transparent about what is done with children's personal information, building in privacy by design and by default, rejecting deceptive practices that can adversely nudge kids' behaviour in harmful ways, and allowing for the deletion or deindexing of their personal information.

Educate to protect and empower: *Privacy Pursuit!* lesson plans

Throughout 2023, the IPC continued to focus on the power of education to advance the privacy rights and digital literacy skills of Ontario's youth. We were proud to introduce educational tools designed to inform and empower students in grades two to eight, just in time for the 2023-24 school year.

Developed in collaboration with MediaSmarts, Canada's Centre for Digital Media Literacy, and building on concepts in our *Privacy Pursuit!* activity booklet, these classroom-ready **lesson plans** offer timely resources for educators. The lesson plans cover topics such as the core concept of privacy and why it is important to uphold privacy as a fundamental value. By integrating these plans into classroom activities, teachers can help ensure that the future generation of digital citizens can make informed choices about how to protect their data online, identify and mitigate privacy risks, and show empathy and respect for the privacy rights of others.

We were proud to see the IPC's *Privacy Pursuit!* lesson plans chosen as one of three finalists out of nearly 75 entries for 2023's IAPP **Privacy Innovation Awards** for North America and Latin America. The IAPP Privacy Innovation Awards' goal is to celebrate ideas and programs promoting privacy and ensure the global privacy community hears about them.



Digital Privacy Charter for Ontario Schools

Students rely upon and trust educators, as guardians, to make important decisions for them. This is why Ontario schools have such an essential role in protecting young people's safety online, preparing them to become responsible digital citizens and empowering them to exercise their privacy rights. In 2023, the IPC released a draft **Digital Privacy Charter for Ontario Schools** for public consultation. This charter consists of twelve high-level commitments that codify privacy best practices for schools to consider and adopt, consistent with Ontario's privacy laws.

“ I encourage educators to adopt the Digital Privacy Charter for Ontario Schools and to demonstrate – to their students, parents, and communities – a true commitment to safeguarding the privacy and future of young Ontarians in a digital world. ”

The commitments are intended as a concrete way for schools and school boards to demonstrate their leadership, become models for others to follow, and earn the enduring trust of their students, parents, and communities. By adopting the digital charter, schools and school boards can show support for their students and help prepare them for an increasingly digital future. The commitments are also intended to promote strong privacy protections in the digital education tools and services used by schools, encourage ongoing learning about privacy in the digital world, and empower students to understand and exercise their privacy and access rights.

“ Today’s youth have grown up online, and no one knows or understands their needs, desires, fears, and challenges better than they do. Their fresh perspectives are an invaluable resource for supporting the IPC’s efforts to promote digital literacy and expand digital privacy and access rights for youth in a way that is relevant and meaningful to them. ”

Empowering voices: The IPC’s Youth Advisory Council

In January 2023, the IPC gave Ontario’s youth a seat at the table by assembling a [Youth Advisory Council](#). Young people from different communities across the province between the ages of 15 and 25, with diverse backgrounds, experiences, and outlooks, came together to express their perspectives on the challenges and risks of the digital world.

In April 2023, the IPC hosted a Youth Advisory Council retreat, marking the first in-person meeting of this dynamic group of young Ontarians. Council members were asked for feedback on a range of IPC programs, including our draft [Digital Privacy Charter for Ontario Schools](#) and [Privacy Pursuit!](#) lesson plans. They provided valuable advice on our outreach methods, including through IPC’s new [Instagram](#) account intended to educate children and youth on how to protect their privacy online. Through regular online meetings, members of the Youth Advisory Council continue to provide us with a window into the privacy, identity, and reputational struggles young people face online and help us better focus our efforts where it counts the most.



IPC’s Youth Advisory Council



INFO MATTERS

Info Matters episodes related to Children and Youth in a Digital World

S3-Episode 9: Empowering young women and girls in the digital world

Advocacy



TRUST IN DIGITAL HEALTH

Our goal in this priority area 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.

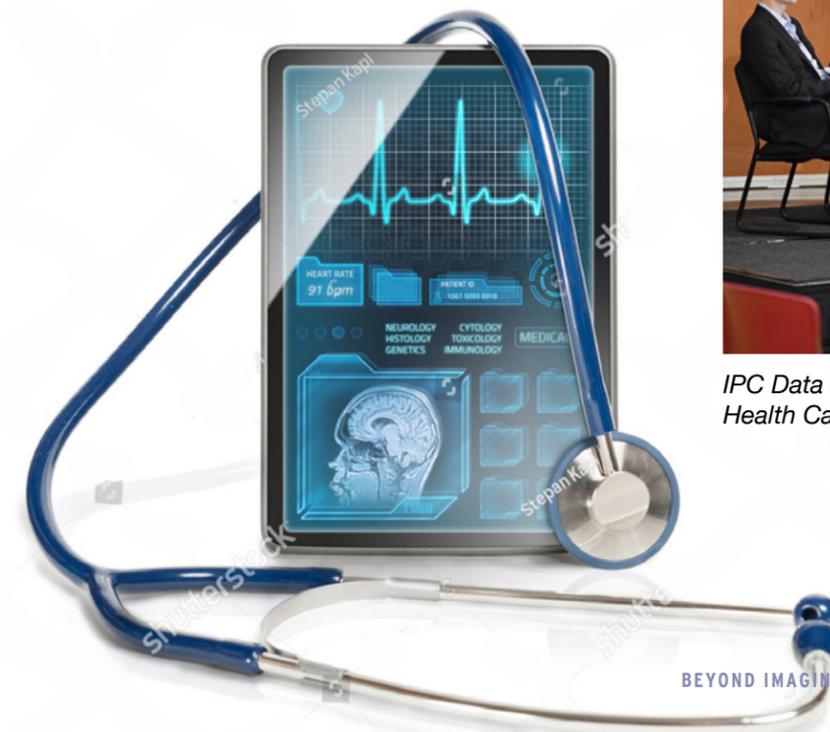
Privacy Day spotlight: Fostering trust in digital health care

The IPC’s 2023 Privacy Day event, [Building Trust in Digital Health Care](#), explored pressing concerns and opportunities within the health care sector and how to earn the public’s confidence in new digital health tools and innovations. A dialogue with a [panel of experts](#) fueled spirited discussions on a range of topics, including transitioning from faxes to secure digital communication channels, ushering in administrative monetary penalties under Ontario’s health privacy law, building resiliency against breaches and cyberattacks, and fostering a culture that prioritizes privacy and security across the entirety of the organization.

Shortly after IPC’s 2023 Privacy Day event, we were pleased to read the government’s announcement that it would finally [axe the fax](#). In a statement by the Minister of Health, the Ontario government committed to “replacing antiquated fax machines with digital communication alternatives at all Ontario health care providers within the next five years.” We were also pleased to see regulations for administrative penalties finally get introduced and adopted a few months later.



IPC Data Privacy Day event, [Building Trust in Digital Health Care](#), January 27, 2023



Advocacy

Navigating administrative monetary penalties with IPC guidance

On January 1, 2024, a new regulation under Ontario's *Personal Health Information Protection Act* (PHIPA) came into force, enabling the IPC to impose administrative monetary penalties (AMPs) directly against individuals and organizations who contravene Ontario's health privacy law. The new regulation is intended to give Ontarians confidence that there are effective mechanisms to encourage compliance with PHIPA and deter against threats to their personal health information.

To prepare for the coming into force of the regulation, the IPC released [guidance](#) setting out a comprehensive roadmap for how the IPC intends to exercise these new powers. The guidance explains when we might consider when issuing AMPs, and the factors that would inform the amount imposed on a case-by-case basis. We aim to take an approach similar to a just culture approach

(commonly used in the health sector to deal with medical errors) by emphasizing the value of reporting and learning from mistakes that occur in complex systems, and reserving more severe consequences for cases where stronger responses are necessary.

The IPC's fair, measured, and proportionate approach is intended to meaningfully address privacy violations while promoting and encouraging accountability and continuous improvement. AMPs are but one option among a number of escalating actions and interventions available to the IPC, ranging progressively from providing educational guidance and advice, recommending corrective measures, issuing orders, imposing administrative penalties, and referring matters to the Attorney General of Ontario for prosecution in the most egregious cases.



“ I continue to strongly urge the government to ensure that any new data governance framework or changes to PHIPA intended to increase the sharing of personal health information be met with a commensurate increase in accountability and transparency measures to protect Ontarians' privacy and support public trust. ”



Three-year reviews of prescribed persons and entities: The PHIPA manual

Every three years, the IPC thoroughly **reviews** the practices and procedures of prescribed entities and persons who handle vast amounts of personal health information. These reviews are a cornerstone of PHIPA, ensuring that those specific organizations entrusted with greater legal flexibility to process this sensitive information for the public good without individual consent are held to the highest standards of privacy and confidentiality.

The IPC conducts these reviews against the standards set out in the *Manual for The Review and Approval of Prescribed Persons and Prescribed Entities*. The IPC spent much of 2023 reviewing the manual to take a modern, risk-based approach and updated the standards in accordance with evolving best practices, especially in respect of cybersecurity. In fall 2023, the IPC held a first-ever face to face meeting of all the prescribed entities and persons under PHIPA to discuss and finalize the changes that were eventually released in November. The meeting was the culmination of a two-year consultation process focused on soliciting their views and comments to ensure that the IPC's updates to the manual are feasible to apply in practice and can stand the test of time. This modern and effective regulatory approach allows us to consider the perspectives of the regulated entities, establish a relationship of trust, and ultimately achieve a more cooperative form of compliance.

Ontario Health Data Council

Throughout 2023, the commissioner continued to serve as ex officio, non-voting member of the Ontario Health Data Council (OHDC). The OHDC was convened by the Minister of Health to provide advice on enhancing the management and use of health data to benefit the people of Ontario. In 2022, the OHDC published an ambitious report, *A Vision for Ontario's Health Data Ecosystem*, with “data driving better and more equitable health, leading to healthier Ontarians.” The report contained recommendations to “enable ethical, timely, and responsible access to and use of health data for people, communities, and populations in Ontario.”

The OHDC spent most of 2023 looking at how to achieve that vision by modernizing Ontario's health data governance regime for a digital age, including its privacy laws, culture, and practice of data access and sharing. The commissioner and her staff provided relevant background and recommendations to the OHDC.



INFO MATTERS

Info Matters episodes related to Trust in Digital Health

S3-Episode 4: Ethical Uses of Genetic Data: A Conversation with Dr. Bartha Knoppers

S3-Episode 5: Co-designing digital health systems with patients and families

NEXT-GENERATION LAW ENFORCEMENT



Our goal in this priority area 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.



Breaking barriers: Intimate partner violence information sharing guide

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 due to intimate partner violence (IPV). Recommendation 78 called on the IPC to work with IPV professionals to develop a plain language guide to empower practitioners to make informed decisions about privacy, confidentiality, and public safety. We readily agreed to carry out this critically important work, in consultation with partners across the IPV ecosystem, including the justice sector, the child and family services sector, the health care sector, and IPV service providers. Released in 2024, the guide <link> sets out an approach for considering when to share relevant information with those who need it in a timely manner and clarify that Ontario's privacy laws are not a barrier to the lawful sharing of information where an individual is at risk of serious harm.

Privacy Futures Project: Strategic foresight into investigative genetic genealogy

In 2023, the IPC held its first Privacy Futures Project on investigative genetic genealogy (IGG). We devoted significant effort to deepen our understanding of IGG tools, recognizing the potential privacy implications for individuals and their biological family members. Adopting a strategic foresight methodology, we envisioned multiple plausible futures to anticipate how IGG tools might evolve and be used in different ways, particularly in conjunction with other emerging surveillance technologies. This approach is helping us prepare for various scenarios, develop strategies to tackle potential challenges, and craft future regulatory pathways that could lead us towards a more desirable future. A future where Ontarians could reap the benefits of this technology to enhance public safety while also maintaining confidence that their privacy and other human rights will be respected.

This proactive approach involved hosting strategic foresight events, bringing together a broad range of perspectives from government policymakers, regulators, law enforcement, forensic scientists, genetic genealogists, academics, civil society, bioethicists, and First Nations groups.

Strategic foresight enables us to anticipate and respond to technological shifts by actively shaping and guiding their evolution to ensure both innovation and privacy are carefully considered before deployment. Working in this way upstream helps build public trust downstream.



Until a clear and comprehensive legal framework for police use of facial recognition technology exists in Canada, I urge Ontario police services and police service boards that are currently operating or considering setting up a facial recognition mugshot database program to review their programs against our guidance as soon as possible, to ensure their program meets legal requirements and includes rigorous privacy safeguards and controls.



Practical guidance on facial recognition with police mugshot databases

Following our 2022 joint FPT statement and privacy guidance on facial recognition for police, and in response to requests by interested parties, the IPC developed more specific Ontario-based guidance for police use of facial recognition technology in connection with mugshot databases. Facial recognition is an artificial intelligence technology that uses software to analyze sensitive biometric information to identify or verify a person's identity. Despite the intended benefits, the technology presents legal, privacy, and ethical challenges, including risks of bias and inaccuracy and impacts on privacy and other fundamental rights, leading to ongoing regulatory debates about its use in Canada and worldwide.

Building on our FPT work, the IPC's *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* provides more granular guidance to help police reduce the privacy risks associated with these specific types of programs in Ontario before, during, and after implementation. Our guidance is intended to contribute to discussion and decision-making about whether and how police may responsibly use facial recognition in connection with mugshot databases to enhance public safety while respecting the rights of persons and diverse groups in Ontario. Like other advanced AI technologies, public sector use of facial recognition in Ontario needs to be built within clear and binding guardrails that effectively address safety, privacy, accountability, transparency, and human rights.

Advancing privacy and oversight in modern policing

In 2023, the IPC responded to the evolving legal framework for policing and community safety in Ontario, focusing on the *Community Safety and Policing Act* (CSPA). Our February and September submissions to the Ministry of the Solicitor General commented on the privacy and transparency implications of various

regulatory proposals under the CSPA. We made several detailed recommendations to the government on how it can achieve its goal of modernizing policing legislation in a manner that balances public safety with individual privacy and access rights.

We also made submissions on Schedule 1 and Schedule 2 of Bill 102, the *Strengthening Safety and Modernizing Justice Act*. In our submission on Schedule 1, we expressed concern about proposed amendments that would remove the IPC's oversight role under the CSPA. Our submission recommended the use of existing data integration authorities under FIPPA and called for maintaining robust privacy safeguards and independent oversight.

In our submission on Schedule 2 of Bill 102, we expressed concerns about the expanded regulation-making authority for the collection of materials for post-mortem analyses, including genetic analysis. We recommended clear purpose limitations and safeguards in the legislative language to prevent potential privacy risks and misuse, such as the use in criminal investigations, without adequate statutory protections.



INFO MATTERS

Info Matters episodes related to Next-generation Law Enforcement

S3-Episode 1: Predicting crimes before they occur: Not so sci-fi anymore

S3-Episode 8: What's on your mind? Neurotechnology and mental privacy

RESPONSIVENESS:

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



To resolve Ontarians' appeals and complaints in a fair, timely and meaningful manner, our office has made significant efforts to improve our tribunal processes and procedures and demonstrate greater transparency with parties about the IPC appeals process. Some of these efforts are highlighted below.



Clearing the slate: Strategies to eliminate file backlogs

Over the past year, our tribunal has made significant strides in improving the efficiency and responsiveness of our services through enhancements to our internal processes and our Case Resolution Information System. In 2023, we embarked on several key initiatives, directly addressing our file backlog and enhancing our operational effectiveness while navigating a record volume of over 3,100 incoming cases.

In July 2023, we began planning to create an expedited appeals process in 2024. The pilot project aims to streamline and resolve straightforward cases through a single-person processing model from beginning to end, significantly reducing processing times.

These and other dedicated efforts have been crucial in managing and reducing our case backlog. Our team closed more than 2900 files in 2023, just shy of repeating our 2021 record for number of file closures. More than 85 per cent of files were successfully resolved to the parties' satisfaction or dismissed through early resolution or mediation, avoiding the need for a more formal and lengthy adjudication

process. The IPC's tribunal was also successful in reducing the average time taken to resolve a file by a notable 18 per cent compared to last year.

Procedural clarity: Updates to FIPPA/MFIPPA code of procedure

The IPC dedicated the past year and a half to reviewing and updating its **FIPPA/MFIPPA code of procedure** to reflect new processes and procedures adopted since it was last reviewed in 2004. These changes aim to enhance process efficiencies and accommodate for modern e-appeals. In September 2023, the updated code was released for public review and comment. The final code was published and implemented in 2024.

The new code:

- reflects the IPC's current procedures for processing e-appeals under FIPPA and MFIPPA
- improves timeliness for the processing of appeals
- maintains the fair and just consideration of appeals
- provides greater transparency and understanding of the IPC's procedures when considering appeals

Responsiveness



Interpretation Bulletins: Guidance simplified

In fall 2023, the IPC developed Interpretation Bulletins to promote a greater understanding of Ontario's access and privacy laws, increase the transparency of our adjudication process, and help people involved in an appeal better understand what to expect.

The Interpretation Bulletins provide insight into how the IPC and the courts have interpreted different sections of FIPPA and MFIPPA when reviewing appeals. By codifying these interpretations and making them readily available on the IPC's website, these bulletins can provide early and concrete guidance to institutions, so they are better positioned to know how to respond to information requests right from the outset.

Interpretation Bulletins cover the following topics:

- Custody or Control
- Fees and Fee Waivers
- Frivolous or Vexatious Requests
- Personal Information
- Reasonable Search

Additional interpretation bulletins on other frequently cited topics are slated to be published in 2024.

A review of noteworthy cases



Conflict to consensus: The power of early resolution

The early resolution team is dedicated to addressing appeals, complaints, and self-reported breaches promptly and effectively. Their central aim is to take early action to resolve matters as early as they can. If an early resolution isn't an option, they decide whether the matter should be dismissed or moved to mediation, investigation, or adjudication. In 2023, more than 50 per cent of all IPC files were successfully completed at early resolution, which is a testament to the significant benefits of early intervention and taking a practical and streamlined approach.



Cyberattack at an Eastern Ontario hospital: Lessons in cybersecurity and data management

Threat actors were able to access the hospital's electronic network via a compromised VPN account, resulting in ransomware lockout and the encryption and corruption of legacy health information databases. The hospital was unable to contain the breach or identify the specific individuals impacted. Approximately 180,000 individuals' personal health information may have been impacted. The early resolution analyst worked with the hospital to ensure it took adequate steps to notify potentially affected individuals through postings on their website and public service announcements. The hospital also took preventative measures to mitigate the risk of such an incident recurring, including by implementing multi-factor authentication.

This incident highlights the need for appropriate disposal of redundant data and ensuring that legacy data, if it needs to be kept, has the same protections as other personal health information. It also highlights the importance of ensuring backup data is not connected to the main networks to safeguard against future breaches.

Cyberattack of a third party vendor, Aetonix, affects 32 health information custodians

In a significant incident, a cyberattack on Aetonix, a vendor providing virtual care platforms, compromised the personal health information (PHI) of over 100,000 patients across 32 health care providers. The breach, rooted in the vulnerabilities of the third-party service, exposed the crucial need for stringent data protection measures, including strong contractual safeguards between the client health care institutions and Aetonix.



This review, conducted with Aetonix's full cooperation, led to strengthened contractual arrangements and an enhanced understanding of PHI security responsibilities for which health care institutions remain accountable, even when they use third party service providers.

With over half of the year's cybersecurity incidents involving third party attacks, the Aetonix breach is a stark reminder to the health care sector of the importance of ensuring strong data protection strategies and cybersecurity measures are in place, especially when entrusting PHI to external service providers.

Enhanced privacy measures implemented following CPIN breach by CAS employee

An employee of a Southwestern children's aid society (CAS) accessed the Child Protection Information Network (CPIN) without authorization, affecting 24 individuals. The privacy breach was discovered during an audit following a high-profile investigation. The IPC's early resolution team swiftly intervened, focusing on ensuring victim notification, containment of the breach, and the implementation of measures to prevent similar future incidents.

Responding quickly, the CAS made significant improvements to its privacy protocols, including enhanced compliance with annual privacy training, regular signing of oaths of confidentiality, introduction of privacy warnings on CAS network logins, and a formal auditing program. The CAS also updated its privacy policy to explicitly include disciplinary actions for unauthorized access to personal information. Working cooperatively with the IPC's early resolution analyst, the CAS implemented these steps to strengthen its responses to future privacy breaches, reflecting the importance of proactive measures in safeguarding sensitive information.



Mediation: A collaborative path to resolution

When cases cannot be quickly resolved at an early stage, our skilled mediation team takes over to assist parties in discussing and resolving the issues. The objective is to reach a consensus that satisfies all parties involved. These professional mediators establish an environment where individuals can voice their interests, perspectives, and concerns. When appropriate, mediators also provide guidance to the parties to help manage expectations. Resolving appeals via mediation dramatically reduces the number of cases that proceed to the more formal adjudication process.

Collaborative approach unlocks information for human trafficking research

A group of researchers filed a request for information relating to a human trafficking operation. The police denied access to some of the information based on several exemptions, namely law enforcement, advice or recommendations and personal privacy.

The police agreed to take part in a mediated teleconference where the researchers pinpointed the specific type of information they were looking for. The police informally consulted with another police service and then revised its decision, disclosing additional information. The researchers further inquired about statistical data, which the police provided, effectively resolving the appeal.

Transparency and access to information are key to shedding light on societal issues that matter to Ontarians. The mediation process proved instrumental in expediting the exchange of information, highlighting the benefits of collaborative and efficient resolution methods.

Responsiveness

Disclosure of historical records opens up dialogue about reconciliation

An Indigenous individual requested historical information related to a police morality squad active between 1945 and 1955. Some of the information requested was withheld under the law enforcement exemption.

A constructive teleconference, followed by a further search by the police, led to the discovery and disclosure of all responsive records at no extra cost. The appellant was also provided with explanations for non-responsive information during mediation, leading to the successful closure of the appeal to the appellant's satisfaction. This case was significant not only for the disclosure of historical records important to the Indigenous appellant, but also for the trust-building and insightful discussions that took place during the teleconference, where topics like reconciliation and the Sixties Scoop were explored and discussed.

Innovative problem-solving in mediation unearths missing township records

An individual appealed a decision by a township to withhold a lot grading plan due to a third party objection. The mediator provided the township with previous IPC orders where lot grading plans did not meet the test for withholding confidential commercial information of third parties. After providing notice to the third party, the township issued a revised decision to release the lot grading plan. It also conducted further searches but did not find additional records. The individual

advised the mediator that she had information about the engineering firm that created the additional record she believed existed. The mediator facilitated contact between the engineering firm and the township, and the engineering firm provided a copy of the missing record to the township. Following third party notice, the township released the additional record to the appellant, and the appeal was resolved.

This successful appeal resolution reflects the effectiveness of interest-based mediation, showing how openness and creative problem-solving can lead to satisfying solutions for all.

Collaborative mediation leads to satisfaction in bylaw complaint records case

In a case involving a request for records related to a bylaw complaint, the municipality initially denied full access. The IPC mediator educated both parties about the appeal process and suggested the municipality provide a detailed index of records, which helped the appellant refine their request. Consequently, the municipality granted partial access to the records, after notifying affected individuals, and issued a revised decision. The appellant was satisfied with the disclosure, and the appeal was resolved. The detailed index of records played a crucial role in facilitating negotiation, leading to an efficient resolution and mutual appreciation from both parties involved in the mediation process.



Adjudication: Efficiency and fairness in focus

If a resolution cannot be achieved through early resolution, mediation or investigation, the file is then referred to an adjudicator. The adjudicator determines whether to proceed with a formal inquiry or review. They receive submissions, assess evidence and arguments presented by the parties, and generally issue a conclusive decision, which may include a binding order.

Key records in inmate death ordered released \\ PO-4428

The appellant in this case was the father of the deceased inmate, who sought access to information about the circumstances of his son's death following an altercation with correctional officers at the Central East Correctional Centre. The Ministry of Solicitor General denied access to the records, citing employment, law enforcement, and personal privacy exemptions.

The IPC's adjudicator ordered the disclosure of several records, including use of force reports and surveillance footage, which detailed the actions of the correctional officers. The adjudicator ruled that while some of the information in these records was subject to the mandatory personal privacy exemption, other information should be disclosed, given the public interest in understanding the details of the inmate's death.

This order highlights that government institutions must interpret the labour relations and employment exclusion in a way that aligns with the transparency purposes of FIPPA. It also emphasizes that government officials should not use privacy exemptions as a shield from public scrutiny.

Transparency in tragic circumstances: Order to release records in murder-suicide case \\ PO-4446

A requester sought access to records relating to the granting and renewal of a firearm license to an individual who was on probation for a violent offence and who used a firearm to kill his girlfriend and himself. The Ministry of the Solicitor General refused access to the relevant records, citing law enforcement exemptions related to the potential of the records to reveal investigative methods, endanger security systems, and facilitate unlawful acts, along with mandatory personal privacy concerns.

The IPC adjudicator ordered the disclosure of certain information relating to the deceased individual and his girlfriend on the basis that disclosure was required to subject the Chief Firearms Office's decision to grant the license to public scrutiny.

This case illustrates how, in certain circumstances, the disclosure of personal information can help the public better understand government decisions affecting the safety and lives of Ontarians.

Transparency in policing \\ MO-4403

An individual requested high-level information about homicides involving intimate partners cleared by the Kingston Police Services Board between 2015 and 2020. The IPC's adjudicator considered the balance between individual privacy rights and the desirability of subjecting the police to public scrutiny, and decided that the transparency of police operations, especially concerning intimate partner violence, outweighs the privacy concerns in this context. The adjudicator found that even if a privacy exemption applied, the compelling public interest in understanding how these sensitive cases are handled by law enforcement would have overridden such exemptions.

Intimate partner violence is a major public health problem, and the public needs to know how these cases are being handled and investigated by the police. Personal information may be disclosed where its disclosure would serve the purpose of subjecting government institutions to public scrutiny.

The Greenbelt Plan: defending the public's right to know \\ PO-4505-F

The Ministry of Municipal Affairs and Housing received a request for access to records relating to the withdrawals of land from the Greenbelt.

In her Special Report on the Changes to the Greenbelt, the Auditor General made observations regarding the use of personal email accounts by political staff and their record retention practices. These gave rise to reasonable grounds to believe that records responsive to the appellant's request may be irretrievably lost or destroyed. On the IPC's own initiative, the adjudicator issued an interim order for the ministry to take steps to secure the preservation and recovery of records responsive to the appellant's request.

The adjudicator accepted the ministry's evidence of the steps taken to recover the records and acknowledged the limitations to retrieving data that may have been permanently deleted prior to such measures being taken. In this order, the IPC recommended the ministry develop and implement comprehensive policies and procedures to train staff in records management and retention, emphasizing the importance of compliance with Ontario's access laws, and assign a senior individual to oversee these practices.

This case reflects the ongoing struggle for transparency in governmental decisions, particularly those with far-reaching environmental impacts, and highlights the essential role that record-keeping plays in maintaining governmental accountability and the public's right to know. Further appeals related to the Greenbelt matter are ongoing and will be publicly released once completed.

Responsiveness



Insights from recent privacy investigations

IPC investigators handle privacy complaints and review privacy breach incidents that cannot be resolved at early resolution. After completing an investigation, they offer findings and recommendations to the respective institution or organization. In some cases, the matter may proceed to a formal review and a binding order.

Protecting student privacy from online exam proctoring powered by AI \\[PI21-00001](#)

Following a complaint by a student who wished to remain anonymous, the IPC opened a commissioner-initiated complaint under FIPPA to investigate McMaster University's use of Respondus exam proctoring software. This software locks down certain functions of a student's computer during online exams so they can't conduct an internet search, access other files on their computer, use the copy/paste function, message, or screen share with others. It also collects sensitive biometric information and monitors students' movements and behaviours through audio/video recordings, using AI to detect instances of potential cheating.

The investigation found that the university is lawfully authorized to conduct and proctor exams to ensure their academic integrity and that nothing legally prevented them from doing so online, both during and post pandemic. This is a legitimate aim in a context moving

towards remote learning and given heightened risks of cheating associated with modern digital tools.

The investigation also found that the university's collection of students' personal information was technically necessary for this exam proctoring software to function properly. However, the sensitive nature of the personal information being collected and the consequential inferences about students' movements and behavioural conduct through AI, raised significant privacy concerns.

The university's notice to students about the purposes for this data collection was found to be inadequate, and the university's safeguards to protect student's personal information through its contractual arrangements with the company, were not sufficient. Most concerning was the company's non-consensual use of students' audio and video recordings, including via third party researchers, to improve system performance and enhance its services.

The commissioner recommended that McMaster University introduce stronger measures to protect students' personal information in the context of online exam proctoring and ensure an approach that balances academic integrity and student privacy rights. She also went on to make additional recommendations to address the broader privacy and ethical risks associated with the use of AI and asked the university to report back within six months on the implementation of these recommendations.

Uncovering and addressing unauthorized access to personal health information \\[PHIPA Decision 202](#)

In this investigation, a health centre experienced 28 incidents of unauthorized access to patient records by employees, which were found to be breaches under PHIPA. Initially discovered during an audit for a separate privacy breach, these additional breach incidents revealed systemic issues, including inconsistencies in staff confidentiality agreements, inadequate privacy notices on the electronic medical record (EMR) system, and the absence of a formal privacy breach policy.

The health centre responded by implementing stronger privacy breach policies, enhancing EMR system privacy notices, and reinforcing staff agreement protocols. Despite these improvements, the IPC investigator noted the health centre failed to ensure reasonable safeguards were in place to protect personal health information and provide notice to those affected by the breach at the first reasonable opportunity, as required by the act. The centre has since taken steps to rectify these issues, ensuring better compliance with privacy protection standards and more timely notification to patients in case of future breaches.

Cybersecurity in health care: lessons learned from a major data breach \\[PHIPA Decision 210](#)

A cyberattack at a hospital affected the personal health information of over a million patients. The hacker used a password spraying attack to gain access to over a dozen hospital accounts, including a legacy account with significant privileges, which the hacker used to access servers and transfer out data. The hacker was able to do this because a temporary change to a firewall was mistakenly left in place, leaving the server connected to the internet and vulnerable to the hacker.

The hospital was unable to specify exactly which data was compromised and estimated that over a million patients were potentially affected. The hospital issued a public notice and committed to two years of dark web monitoring to track any misuse of the data. After reviewing its security protocols, the hospital revised

its information security policies, focusing on password strength, account privileges, and firewall security. The IPC found that the hospital's measures and policy revisions provided adequate response and the case did not need to go on to formal review.

This incident serves as a reminder of the ever-evolving nature of cybersecurity threats and the importance of strong data protection measures. Health care institutions must continually review and enhance their security protocols, particularly in areas of password management, access controls, and firewall security.

Insightful analytics

In 2023, Ontarians submitted 66,422 freedom of information requests, more than a 14 per cent per cent increase over the previous year.

Response rates, indicated by the number of access requests fulfilled within a 30-day timeframe, varied across sectors. For provincial institutions subject to FIPPA, over 67 per cent of access requests were successfully addressed within 30 days, signifying an improvement compared to 2022, when just 51.2 per cent of requests were completed within 30 days.

Municipal institutions covered by MFIPPA completed 80.2 per cent of requests within 30 days, consistent with the previous year's rate.

Ontarians submitted 105,163 requests for access to personal health information under PHIPA in 2023, up five per cent over the previous year. Health information custodians successfully maintained a commendable 30-day response rate in 97.4 per cent of cases.

Under the CYFSA, child and family service providers fulfilled 10,952 access requests for personal information, up ten percent over the previous year, with 72.6 per cent of those completed within 30 days.

A comprehensive overview of 2023 tribunal statistics can be located on page 42 of this report, while a full breakdown of all submitted statistics is accessible in the [IPC's 2023 Statistical Report](#).

“ The government must amend both FIPPA and MFIPPA to establish a comprehensive privacy protection framework that positions Ontario well for an evolving digital world that is resilient to rapid change and provides the next generation with optimism about their future. This amended framework should include mandatory privacy breach reporting and more explicit accountability and transparency requirements for government institutions to respond to breaches and mitigate against the risk of breach in the first place. It should also include provisions for initiating privacy complaints, including commissioner-initiated complaints, and more explicit powers of investigation for the IPC, including the power to compel the production of evidence and to issue binding orders. Such reforms are crucial for ensuring consistent privacy protections, enhancing institutional accountability, and maintaining public trust and confidence across Ontario's public and broader public sectors. ”

ACCOUNTABILITY:

Maintaining Ontarians' confidence
in the organizational
excellence of the IPC



A cornerstone of the IPC's mission is our commitment to meeting the high standards of organizational excellence and accountability that the people of Ontario expect from us. This past year was marked by significant advancements in our digital capabilities and improvements to our internal governance and management.

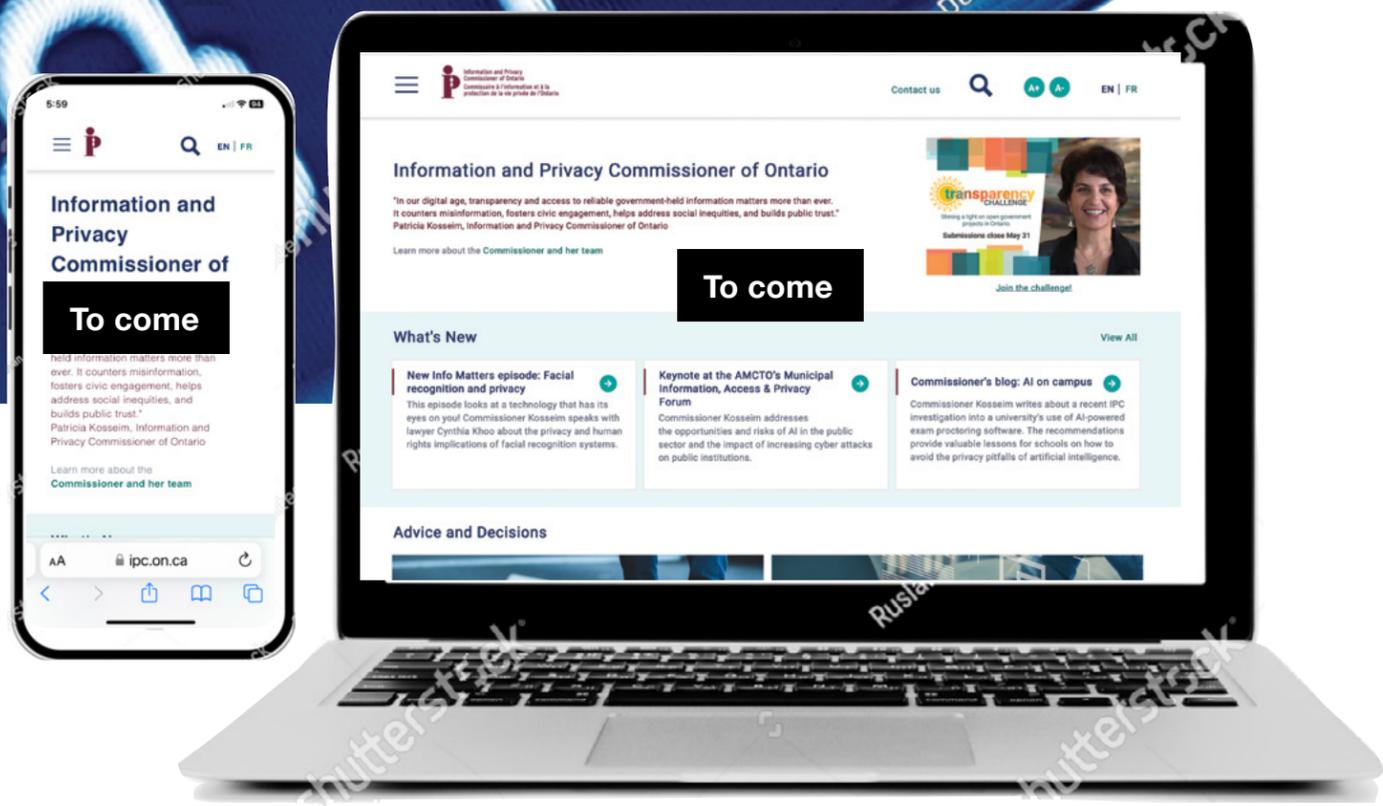


The IPC's digital transformation in action

Ascending to the cloud with Microsoft 365

In 2023, the IPC continued to intensify its efforts to enhance our digital services building on our successful Microsoft 365 collaboration pilot. We took a transformative step by implementing new hardware management tools and moving email online as part of our multi-year plan to migrate our IT operations to the cloud, heralding a new chapter in our operational capabilities. This transition equips our workforce with robust, flexible tools for seamless remote

collaboration and secure data access, reflecting our dedication to modernization and responsiveness. The move not only enhances our productivity and data analytics potential but also strengthens our commitment to privacy and information stewardship. Embracing this digital evolution, the IPC is now better poised to address the complex challenges of today's information landscape with agility and forward-thinking resolve.



The new IPC: A website for the modern age

In the spirit of innovation and accessibility, the IPC intensified its efforts throughout 2023 to enhance our digital services by developing a new IPC website built on modern technologies, featuring greater potential for interactivity and an improved user experience. Launched in April 2024, this initiative involved rigorous analysis and user-centred design, ensuring every page of our website reflects our commitment to provide clear

information on privacy and access rights in a format accessible to all Ontarians. Our new online home is optimized for all devices, offering intuitive navigation and enhanced features that allow users to find guidance, resources, and services with ease. Moving forward, our new website reflects our dedication to transparency and public engagement, empowering every visitor with the knowledge to safeguard their privacy and access rights in an increasingly digital world.



The IPC was deeply honoured to be shortlisted as one of Canada's Top Employers for 2024.

Cultivating the best: The IPC's journey as an employer of choice

At the IPC, our pursuit of excellence is deeply reliant on the valuable contributions of our professional staff. As part of our commitment to foster an outstanding workplace and retain top talent, we pursued our formal and informal staff recognition program with great pride and enthusiasm. In addition to informally recognizing significant achievements and excellent contributions of staff every quarter, we held our second annual IPC Exemplary Awards ceremony — celebrating those who best exemplify our core values and dedication to public service.

We further demonstrated our commitment to excellence through stepped-up investments in learning and professional development, particularly in cybersecurity and artificial intelligence. With the introduction of a new senior talent management and training advisor, we significantly expanded our management training curriculum and continue to develop and strengthen the IPC's integrated corporate training program and leadership competencies.

These investments will continue to nurture the IPC's culture of continuous learning and better position us to address the complex digital and data challenges that lie ahead. These initiatives are the cornerstones of our journey towards becoming an employer of choice — a journey marked by a steadfast focus on employee engagement and empowerment, ensuring that as we grow and evolve, we do so together, with every team member feeling valued, supported, and primed to thrive.

These efforts and initiatives have not gone unnoticed. The IPC was deeply honoured to be shortlisted as one of Canada's Top Employers for 2024.

Continuing to strengthen governance and accountability

In 2023, the IPC launched its Strategic Plan, the result of two years of work to establish strategic priorities and goals, and a concrete implementation and measurement plan for the organization. This work expanded our vision and mandate by confirming our three mission pillars and putting ten key operational goals in place.

The multi-year plan comprises detailed activities, expected outputs, desired outcomes, and specific data collection methods. As part of the IPC's new strategic planning and evaluation program, an ongoing reporting process has been put in place to facilitate the regular review and effective monitoring of progress to achieve our goals along our planned trajectory. More than just a bureaucratic exercise, this framework is intended to measure and report on resulting benefits for Ontarians and support IPC's vision of becoming a modern and effective regulator with real world impact.

IPC's work in this area was recognized as leading-edge internationally in the global review of data protection authority strategies. The report, *Data Protection Authority Strategies: A Global Review of Current Practices*, points to our effective consultation and stakeholder engagement approach in developing our strategic priorities and describes our leadership in setting a clear vision and mission to guide our work. The IPC's approach, as featured, is a rewarding acknowledgement of our commitment to upholding privacy rights and fostering trust through accountability and innovation in privacy and information management practices.

ADVOCACY AND INFLUENCE

Lending our voice for change:

Submissions to government and stakeholder relations

Through our advocacy work, the IPC submits comments, open letters, and recommendations on various proposed laws and regulations having access and privacy implications.

The IPC's submissions to the government in 2023 included:

January 19

Letter to Ontario government on the need to amend legislation to protect employee privacy

February 8

Letter to Dr. Cameron, Ontario Regional Supervising Coroner, Operations, on inquest jury recommendation to develop plain-language tool to empower intimate partner violence professionals to share information

February 3

Letter to the Ministry of the Solicitor General on the need to ensure strong access and privacy considerations in four regulatory proposals under the *Community Safety and Policing Act*

March 23

Comments on privacy implications of Bill 60, *Your Health Act*, and recommendations to ensure privacy protection in respect to Integrated Community Health Services Centres and regulated health professions.

April 18

Letter to government recommending withdrawal of schedules 4, 6 and 7 of Bill 79 to better protect Ontarians' privacy in the context of employment services transformation.

May 17

Comments on Schedule 1 of Bill 102, *Strengthening Safety and Modernizing Justice Act*, on the need for clear legal authority and effective privacy safeguards in the data practices proposed under the *Community Safety and Policing Act*.

May 17

Comments on Schedule 2 of Bill 102, *Strengthening Safety and Modernizing Justice Act*, and the need for clear purpose limitations and safeguards to protect privacy rights in Ontario.

July 5

Comments on a regulatory proposal to establish administrative monetary penalties under PHIPA and their role in ensuring compliance and protecting public trust in Ontario's digital health care system.

July 13

Submission for review of the *Child, Youth and Family Services Act*, calling for enhanced transparency and privacy and access protections for vulnerable Ontarians receiving services under the act.

August 25

Submission for proposed Regulatory Changes to Ontario Regulation 155/18 and 156/18, calling for any amendments to expand the collection, use or disclosure of personal information to be matched by a proportionate level of robust privacy protection.

September 1

Letter to the Ministry of the Solicitor General on three regulatory proposals under the *Community Safety and Policing Act*, emphasizing the need for modernized policing standards that uphold privacy, transparency, and accountability, particularly in intelligence activities and responses to major incidents.

September 11

Submission for the five-year review of the *Police Record Checks Reform Act*, recommending measures to ensure public safety while protecting privacy and fundamental rights.

September 26

Letter to the Ministry of the Solicitor General on three regulatory proposals under the *Community Safety and Policing Act*, calling for enhanced transparency and proper governance of personal information in policing.

October 13

Comments on PHIPA administrative monetary penalties and the IPC's proportionate approach to their administration

November 15

Submission for Bill 135, *Convenient Care at Home Act*

United we stand: National and international resolutions

The IPC regularly collaborates with fellow regulators both domestically and on the global stage, to harmonize our policy positions and expand our public awareness initiatives. Throughout 2023, the IPC led, co-led, sponsored, and supported a range of national and international resolutions and joint statements.

National

- [Facilitating Canadians' access to government records to help restore trust in our institutions](#) (October 2)
- [Putting best interests of young people at the forefront of privacy and access to personal information](#) (October 6)
- [Protecting Employee Privacy in the Modern Workplace](#) (October 6)

International

- IPC endorsement of International Conference of Information Commissioners' statement highlighting the importance of access rights (September 28)
- IPC co-sponsors Global Privacy Assembly international [resolution](#) on AI and employment (October 31)
- IPC co-sponsors Global Privacy Assembly international [resolution](#) on Generative Artificial Intelligence (October 31)

Engage and influence: Stakeholder consultation and guidance

As part of our statutory power to offer comments on the privacy protection implications of proposed legislative schemes, programs and information practices, we invite organizations to [consult](#) the IPC on precedent-setting initiatives that significantly impact data privacy or access. For a full list of informal consultations completed in 2023, visit our [consultations webpage](#).

Educate and empower: The IPC's public education initiatives

Under our enabling laws, the IPC may conduct public education programs and provide information concerning Ontario's access and privacy laws and the office's role and activities.

In 2023, the IPC developed several multimedia guidance materials and documents, delivered 57 [presentations](#) to various audiences, posted eight blogs and released 10 *Info Matters* podcast episodes on access and privacy issues that matter to Ontarians. We are also active on social media, and over the last year, we increased our LinkedIn followers by 28 per cent and YouTube viewers by 22 per cent. Our new Instagram account attracted a 164 per cent increase in followers in just one year.

Guidance

- [Privacy Pursuit! Lesson Plan – What is Privacy? \(Grades 2-3\)](#)
- [Privacy Pursuit! Lesson Plan – Protecting Your Privacy \(Grades 4-5\)](#)
- [Privacy Pursuit! Lesson Plan – The Value of Privacy \(Grades 6-7\)](#)
- [Privacy Pursuit! Lesson Plan – My Privacy, Your Privacy \(Grades 7 – 8\)](#)
- Updates to Part X of CYFSA guidance
- Administrative Monetary Penalties: [Guidance for the Health Care Sector](#)



Interpretation Bulletins

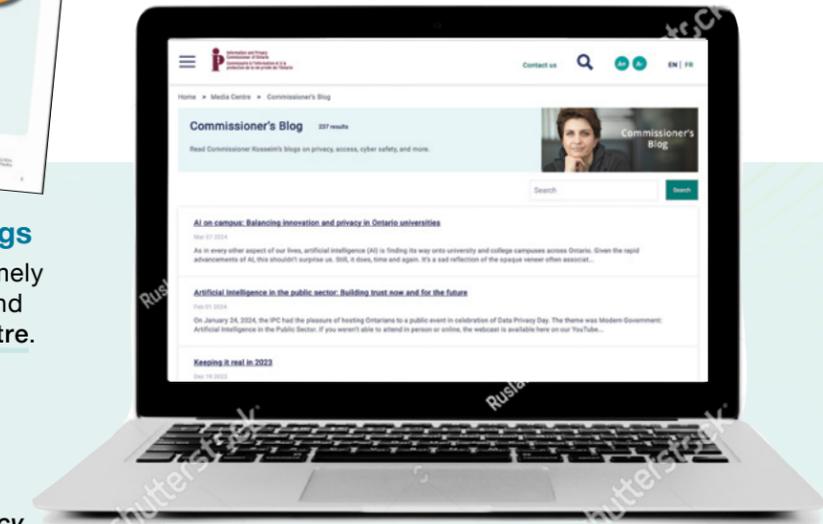
- [Custody or Control](#)
- [Fees and Fee Waivers](#)
- [Frivolous or Vexatious Requests](#)
- [Personal Information](#)
- [Reasonable Search](#)

Learning in the digital era: IPC webcasts and videos

- Privacy Day 2023 event: [Building Trust in Digital Health Care](#)
- IPC FYI Episode 1, [Decisions, Decisions!](#)

Presentations

In keeping with our focus on outreach, engagement, and collaboration, the IPC actively participated in events and conferences during 2023 across a broad range of stakeholder groups. The commissioner, assistant commissioners, and legal, policy, communications, and tribunal staff delivered 57 speeches and presentations. For a list of presentations, visit our [media centre](#).



From the commissioner's desk: IPC blogs

Commissioner Kosseim regularly blogs about timely issues relating to privacy, access, technology, and more. For a full list of blogs, visit our [media centre](#).

2023 blogs

[Giving Ontario's youth a seat at the table](#)

January 12

[Privacy Day 2023: A positive diagnosis for privacy](#)

February 1

[Let the sunshine in! Showcasing the benefits of government transparency](#)

May 18

[Bookending my year as the IPC's first Scholar-in-Residence](#)

June 29

[IPC's Back-to-School Lesson Plans: Helping kids learn about online privacy](#)

August 16

[RTKW 2023: Why access to information matters more than ever!](#)

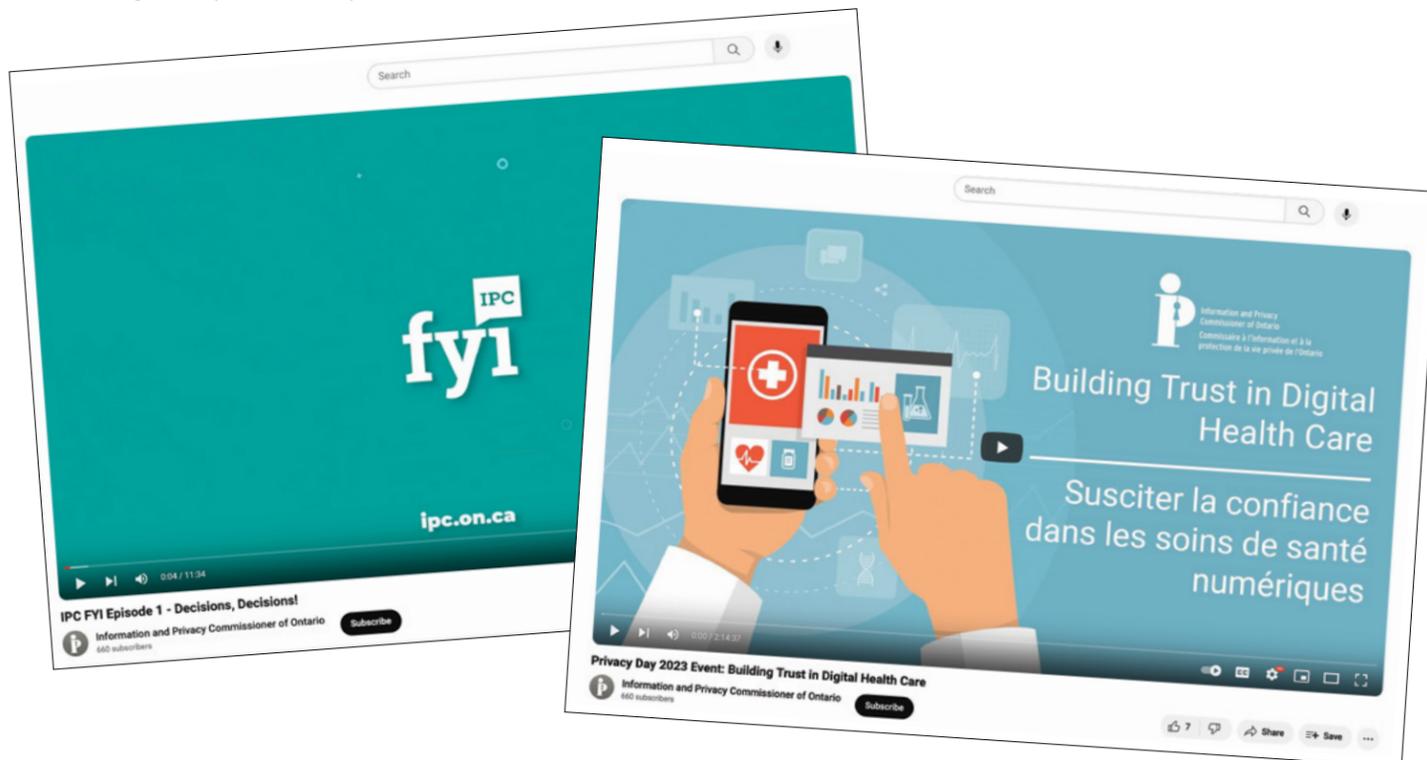
September 20

[Media Literacy Week: Protecting and empowering students in the digital age](#)

October 20

[Keeping it real in 2023](#)

December 19





In December, Info Matters received the award for Outstanding Technology Series at the 6th Annual Canadian Podcast Awards.



INFO MATTERS

The Info Matters podcast: Conversations that count

In its third season, the IPC's podcast, *Info Matters*, continued to delve into current and emerging issues in the digital age. Hosted by Commissioner Kosseim, the podcast features in-depth discussions about issues ranging from the dangers of misinformation to the design of equitable health systems and predictive policing.

In December, *Info Matters* received the award for Outstanding Technology Series at the 6th Annual Canadian Podcast Awards.

Info Matters Season Three

Episode 1: Predicting crimes before they occur: Not so sci-fi anymore

Episode 2: Trust and truth: Navigating the age of misinformation

Episode 3: A casual conversation between two Canadian privacy commissioners

Episode 4: Ethical Uses of Genetic Data: A Conversation with Dr. Bartha Knoppers

Episode 5: Co-designing digital health systems with patients and families

Episode 6: A woman's right to know: Closing the gender gap with access to information

Episode 7: Unmasking digital threats: How to guard against cyber crime

Episode 8: What's on your mind? Neurotechnology and mental privacy

Episode 9: Empowering young women and girls in the digital world

Episode 10: Best of season three

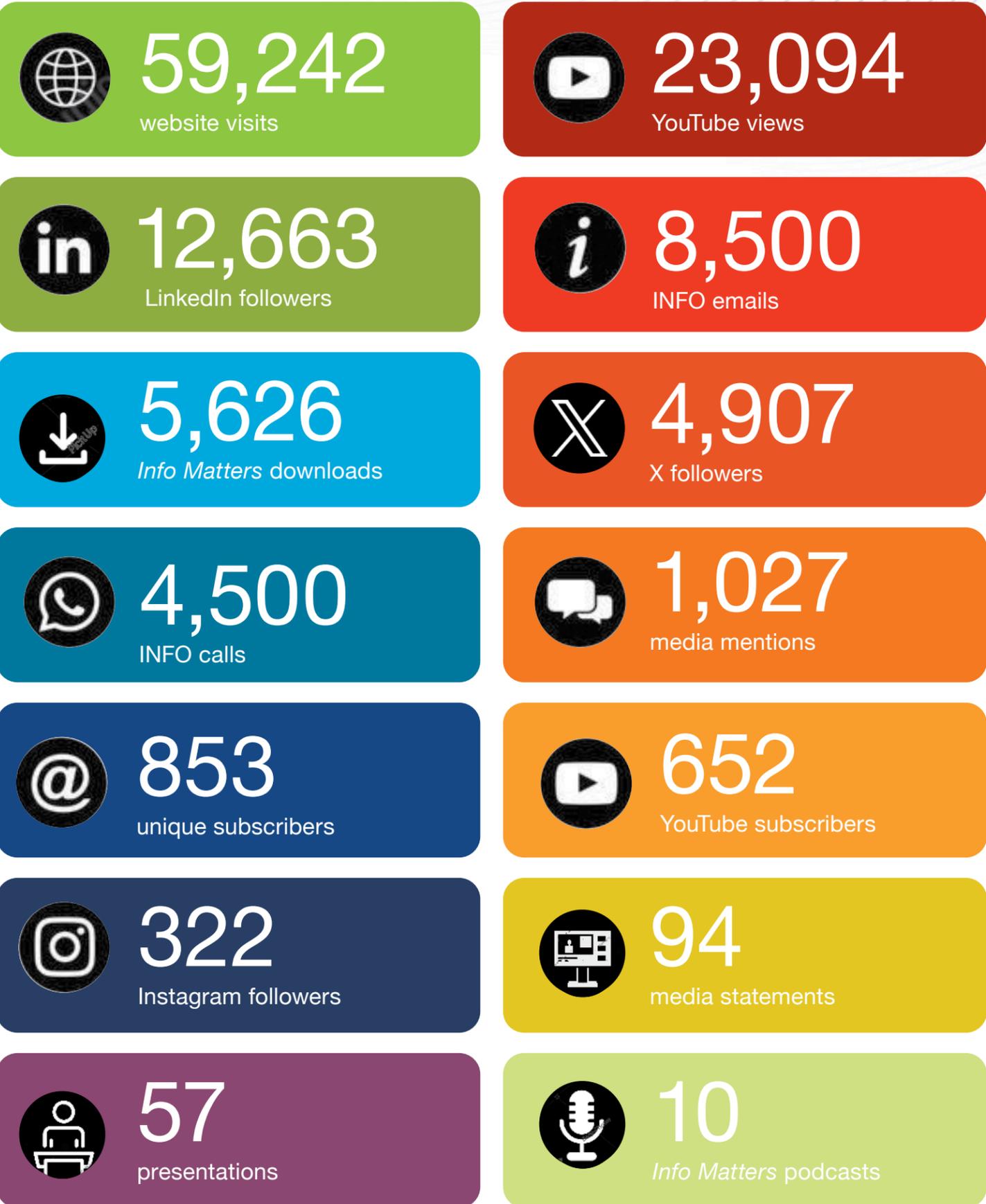


The IPC in the media

The IPC responded to 94 media requests in 2023 and was mentioned in the media more than 1,000 times. We were front and centre in several high-profile matters in 2023, including:

- Commissioner Kosseim featured in *McGill News Alumni Magazine*
- Commissioner Kosseim as a guest on *Leadership in the Digital Enterprise* podcast
- *Ontario Today*, How has DNA testing changed your story?
- The Globe and Mail, Privacy commissioner urges 'guardrails' on using forensic genealogy to catch criminals
- The Agenda with Steve Paikin, How Free is Canada's Information System?
- Reaping the benefits of keeping things real: Commissioner Kosseim on *Leadership in the Digital Enterprise* podcast
- *In Conversation with Stephen Hurley*. Commissioner Kosseim discusses the IPC's Privacy Pursuit! lesson plans
- Commissioner Kosseim welcomed as guest blogger for MediaSmarts, *Protecting and Empowering Students in the Digital Age*
- In Conversation with Stephen Hurley, Commissioner Kosseim discusses the importance of Media Literacy Week

IPC outreach by the numbers in 2023



IPC in the courts



8 Judicial Reviews



3 Legal Hearings



6 Motions

Cabinet Office // PO-3973

In January 2022, 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 majority of 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 heard the Ontario government's appeal from the decision in April 2023 and issued its **judgment**, allowing the appeal in February 2024. The Supreme Court's ruling clarified the scope of information subject to cabinet confidence under Ontario's access to information legislation and held that the government is not required to disclose the mandate letters to the public.

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 2019 cyberattack on LifeLabs' computer systems. The IPC and OIPC found that LifeLabs did not comply with its obligations under Ontario's health privacy law and British Columbia's *Personal Information Protection Act*, including through 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 and could be published. The IPC and OIPC were required to wait for the court's ruling on whether any of the information in the report is privileged or confidential before publishing the report. In April 2024, the Divisional Court heard and dismissed LifeLabs' challenge to the IPC and OIPC's procedural decision. The Divisional Court found, among other things, that health information custodians cannot defeat their responsibilities under PHIPA by placing facts about privacy breaches in privileged documents.

Liquor Control Board of Ontario // PO-4302

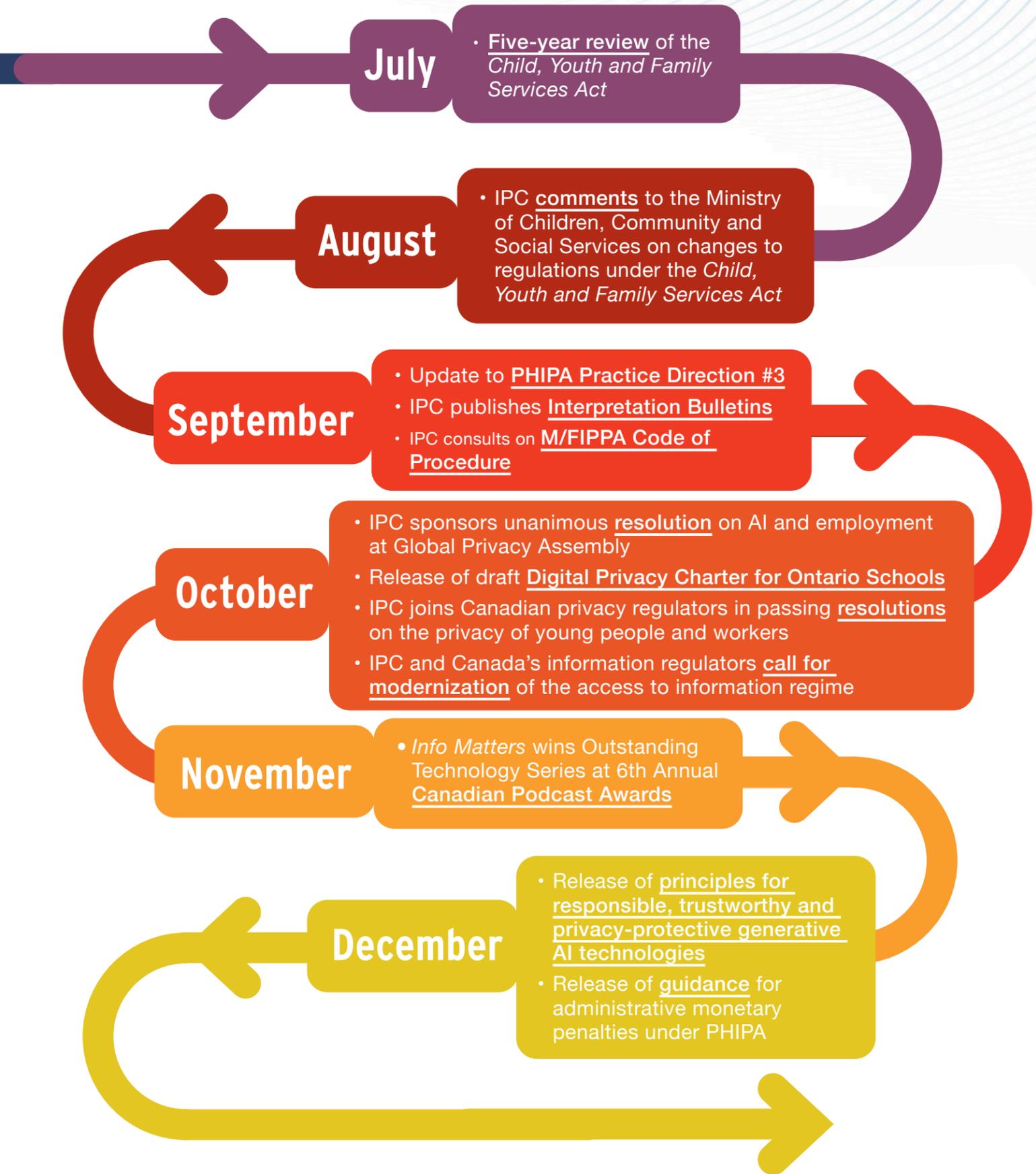
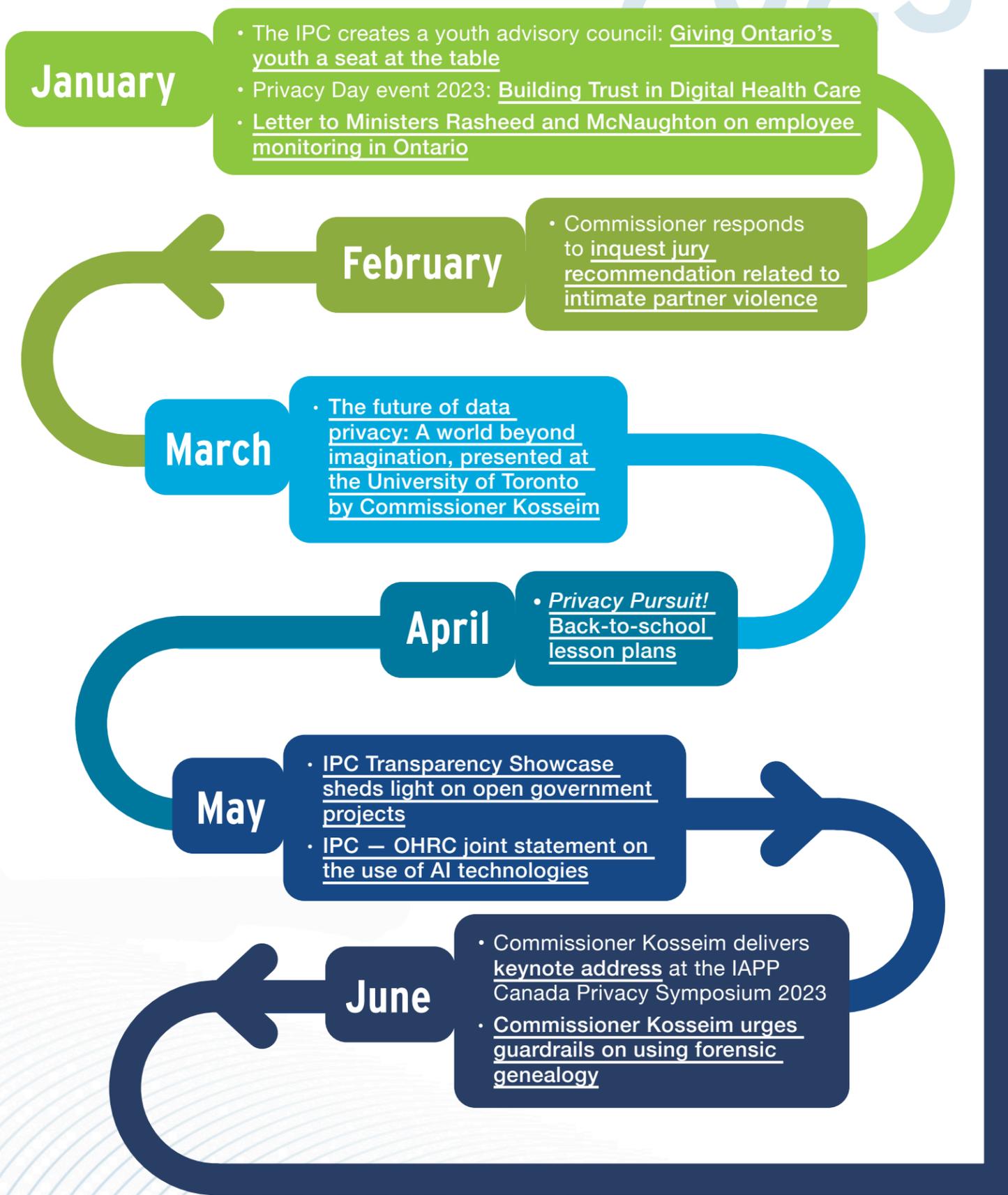
The Liquor Control Board of Ontario (the LCBO) challenged an IPC decision finding statistical records of thefts from individual LCBO stores in Toronto and global statistics all stores province-wide were not exempt from disclosure under sections 14(1)(e) and 20 (endanger physical safety), 14(1)(i) (endanger security), 14(1)(l) (facilitate unlawful act) and 18(1)(c) and (d) (prejudice economic interests) of FIPPA. A majority of the Divisional Court overturned the decision, holding the decision of the IPC was unreasonable for applying the wrong standard of proof, misapprehending the LCBO's evidence, and giving inadequate reasons. The dissenting judge found the IPC applied the correct standard of proof, made reasonable findings based on the evidence, and gave adequate reasons in light of the statutory duty imposed on the IPC not to reveal the LCBO's confidential submissions in its decision. The IPC's application for leave to appeal the majority's decision to the Court of Appeal was granted in January 2024.

Algoma Family Services PHIPA // Decision 83 and Decision 128

In January 2019, the IPC issued a decision determining that the applicant did not have a right of access, under PHIPA, to his son's records of personal health information in the custody or control of Algoma Family Services. In September 2020, the IPC issued a reconsideration decision determining that Algoma Family Services exercised its discretion properly when it did not disclose the son's personal health information to the applicant. The applicant sought to judicially review both decisions. This application for judicial review was heard in June 2023 and dismissed by the Divisional Court.

The IPC's year at a glance

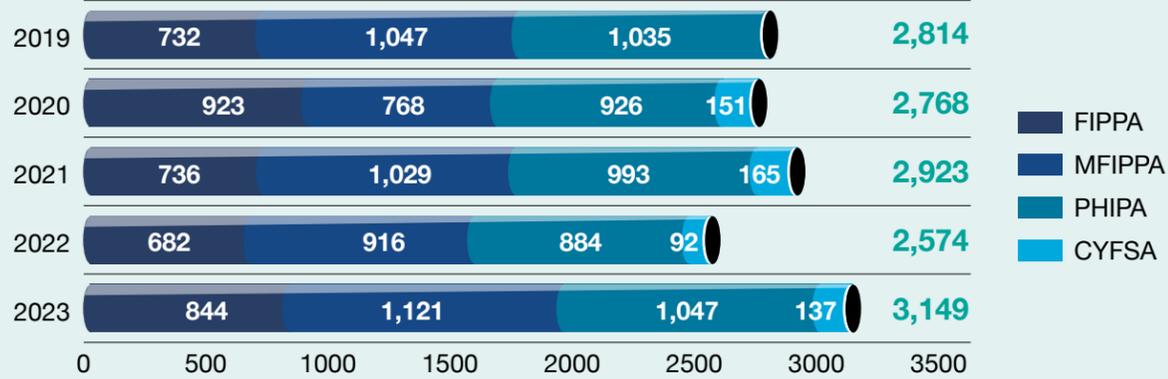
2023



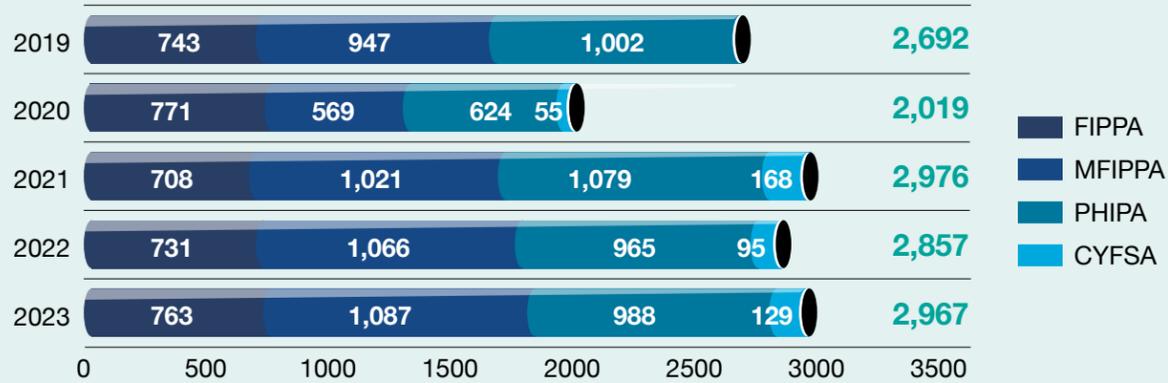
Statistical highlights

Overall

Overall opened files 2019-2023



Overall closed files 2019-2023

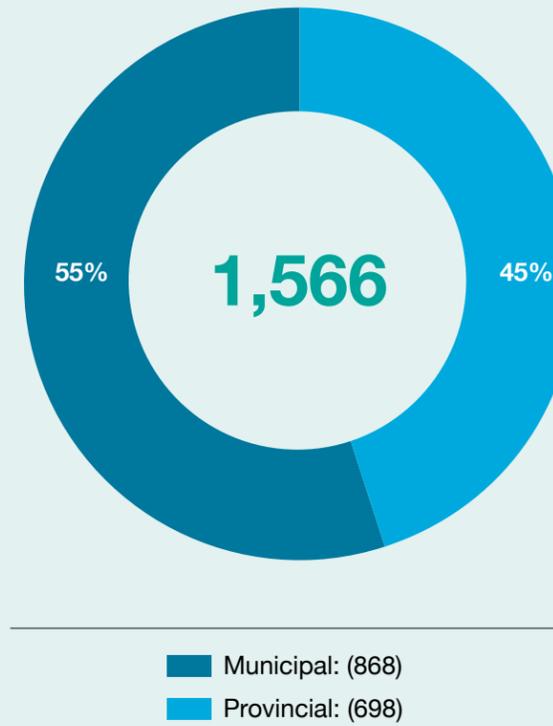


Average duration (in months) to process and close a file 2019-2023

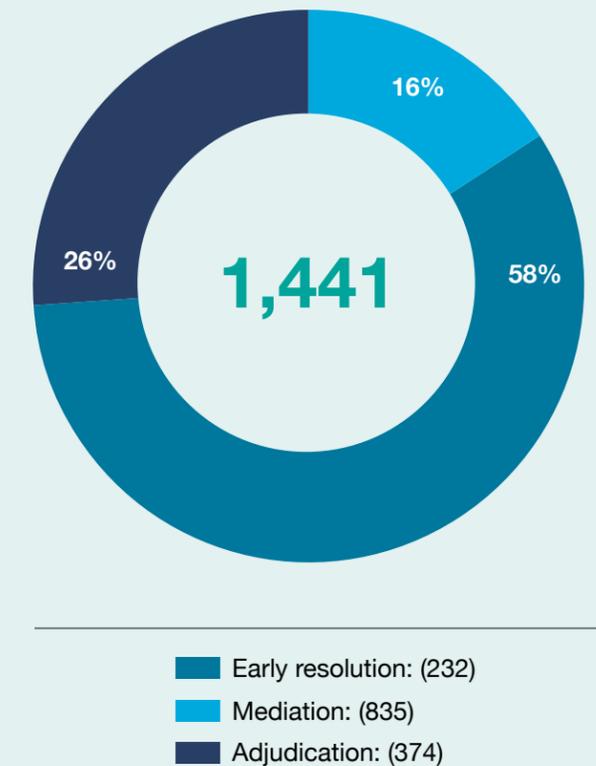


FIPPA/MFIPPA

Access appeals opened 2023



Access appeals resolved by stage 2023



Issues in access appeals opened in 2023



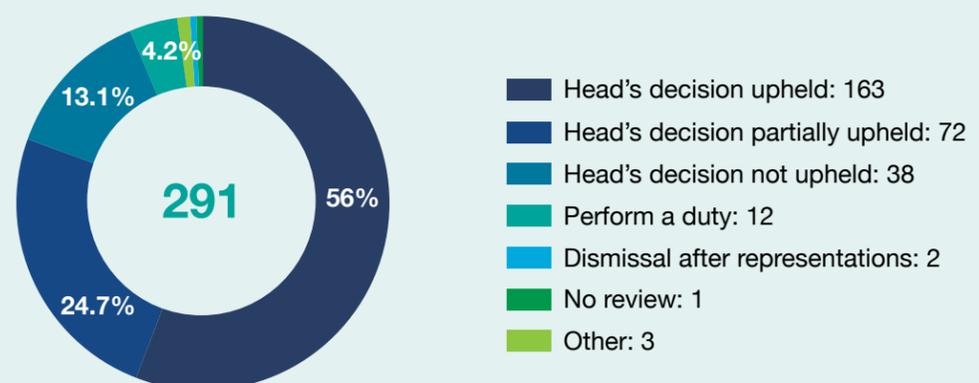
Provincial access appeals opened/closed 2019-2023



Municipal access appeals opened/closed 2019-2023



Outcome of access appeals closed by order in 2023*



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

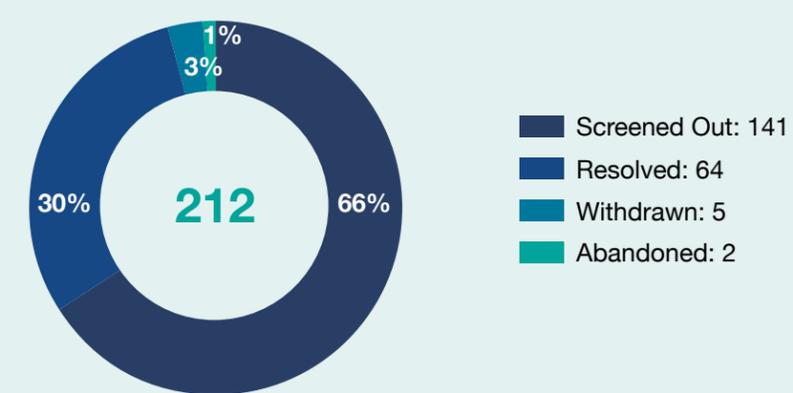
Provincial privacy complaints and self-reported breaches opened/closed 2019-2023



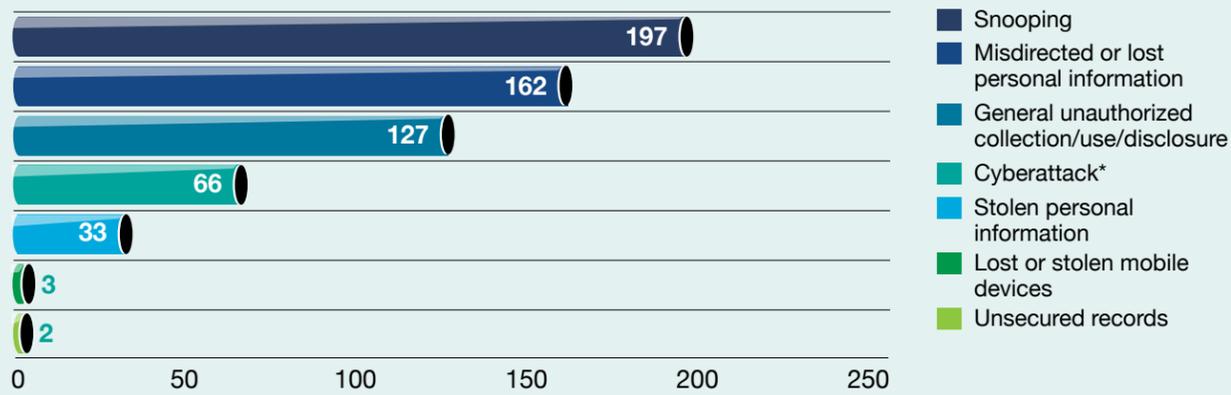
Municipal privacy complaints and self-reported breaches opened/closed 2019-2023



Privacy complaints closed by type of resolution 2023

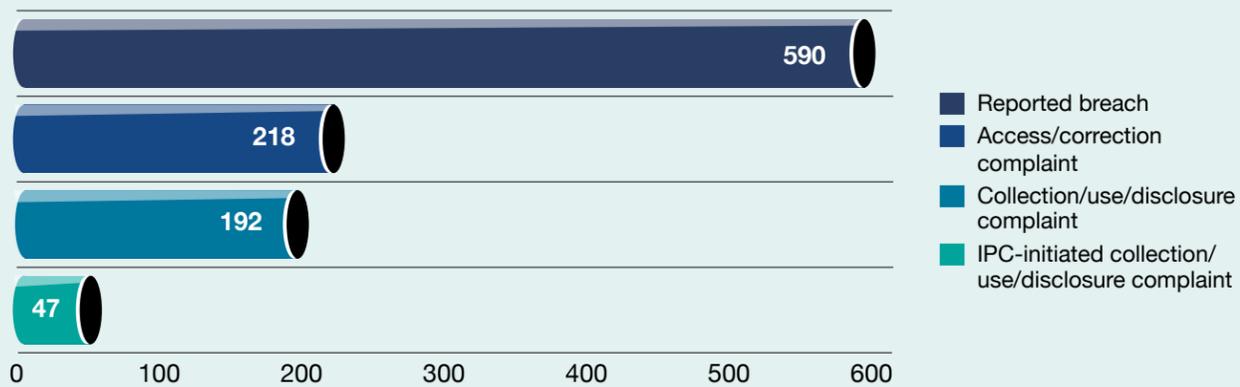


Self-reported health privacy breaches by cause 2023

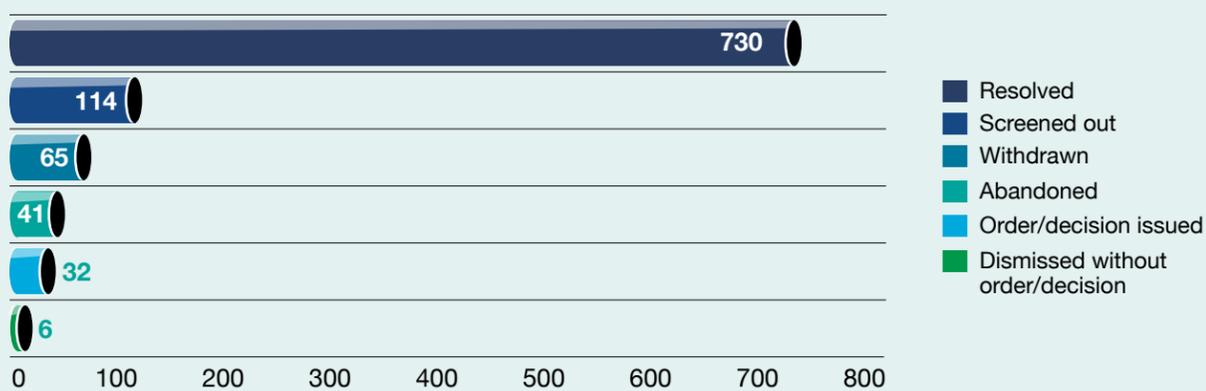


* Cyberattacks involving ransomware: 11 of 66

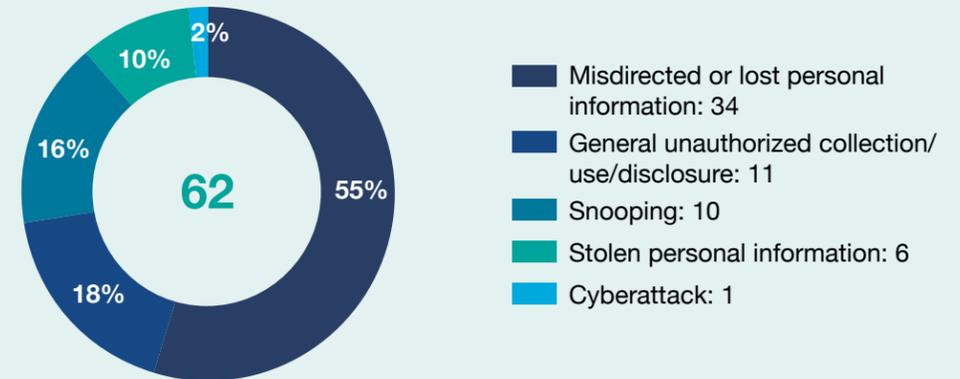
Types of health files opened 2023



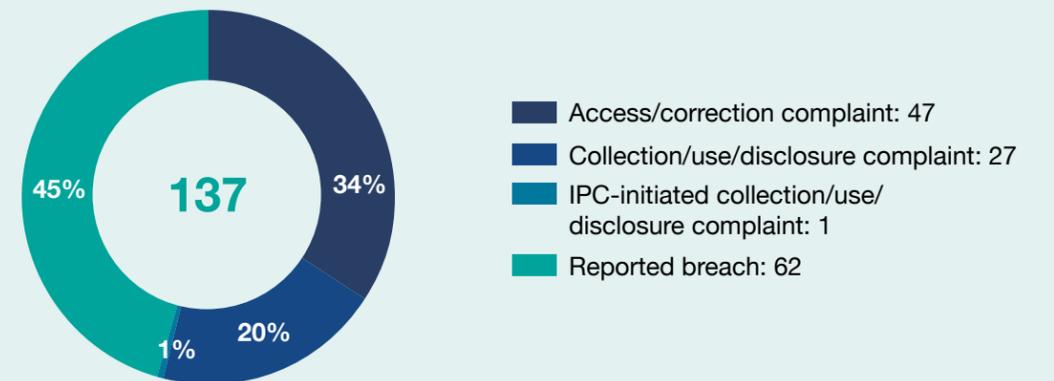
Outcome of health files closed 2023



CYFSA self-reported CYFSA privacy breaches by cause 2023



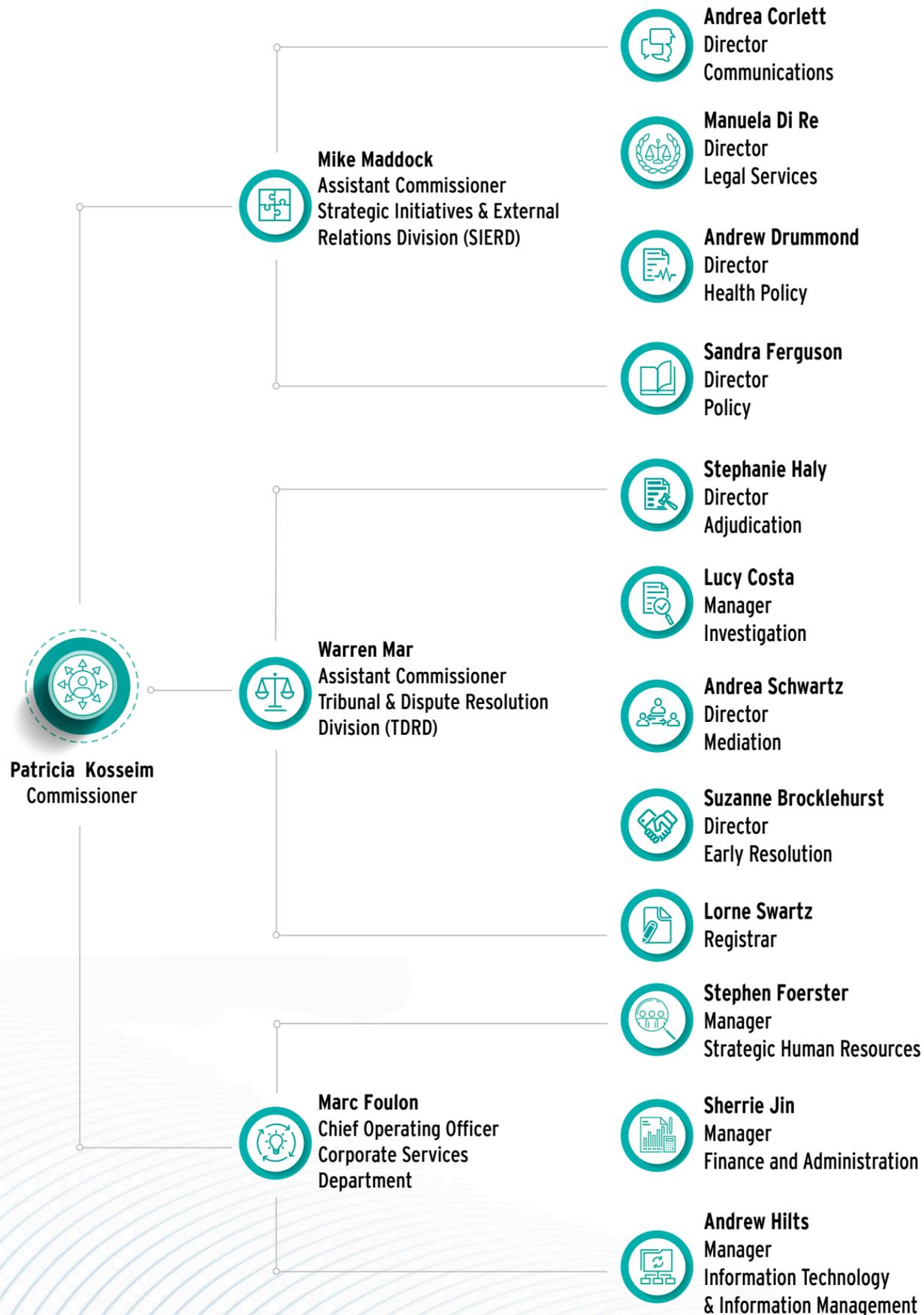
CYFSA files opened by issue 2023



Outcome of CYFSA files closed 2023



Organizational chart



Financial summary

	2023-2024 Estimate (Unaudited)	2022-2023 Estimate (Unaudited)	2022-2023 Actual (Unaudited)
Salaries and wages	\$ 17,586,000	\$ 14,900,500	\$ 15,204,322
Employee benefits	\$ 4,653,300	\$ 3,980,400	\$ 3,489,586
Transportation and communications	\$ 185,300	\$ 122,000	\$ 100,414
Services	\$ 4,612,100	\$ 3,492,400	\$ 3,568,818
Supplies and equipment	\$ 162,600	\$ 137,000	\$ 138,037
Total	\$ 27,199,300	\$ 22,632,300	\$ 22,501,177

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.

	2023 (Calendar year)
Appeals fees deposit	\$ 27,372.00

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, the 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