

From Vision to Impact

FIVE YEARS OF
PRIVACY AND
TRANSPARENCY IN A
DIGITAL ONTARIO



Information and Privacy
Commissioner of Ontario

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

2024
ANNUAL REPORT

Cover: Original artwork by Shelby Gagnon, an Anishinaabe and Mushkegowuk artist from Aroland First Nation, who has lived in Thunder Bay for most of her life, Commissioned for the IPC [Transparency Showcase](#).



June 12, 2025

The Honourable Donna Skelly
Speaker of the Legislative Assembly of Ontario

Dear Madam Speaker,

I am honoured to present the 2024 Annual Report of the Office of the Information and Privacy Commissioner of Ontario, *From Vision to Impact: Five Years of Privacy and Transparency in a Digital Ontario*. This report highlights our achievements between January 1 and December 31, 2024, as we work towards enhancing privacy, transparency, and trust in our increasingly digital world.

As we reflect more generally on the past five years, we have made notable strides in advancing areas such as the responsible use of artificial intelligence by public institutions, privacy protection in the health care sector, adoption of next generation technologies by law enforcement, and the digital rights of children and youth in Ontario.

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

Patricia Kosseim
Information and Privacy Commissioner of Ontario



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

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

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

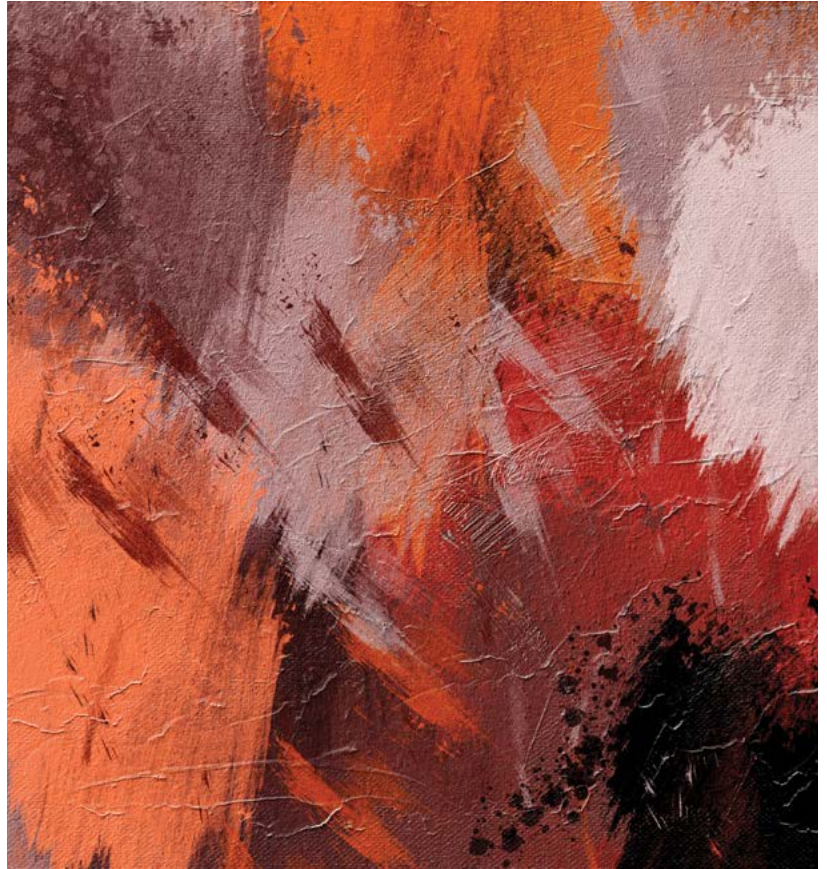
Contents

- 4 Commissioner's Message
- 10 The IPC's Vision, Mission, and Goals

12

Advocacy

- 14 Privacy and Transparency in a Modern Government
- 17 Children and Youth in a Digital World
- 20 Trust in Digital Health
- 23 Next-Generation Law Enforcement



26

Responsiveness

- 28 Enhancements to Tribunal Efficiency and Responsiveness
- 30 A Review of Noteworthy Cases
- 34 IPC in the Courts
- 37 FOI, Privacy and Performance in 2024

38

Accountability

- 40 Modernization and Digitization
- 41 Employer of Choice
- 43 Strategic Priorities and Planning



44

Engagement and Outreach

- 47 Informing the Future of Access and Privacy in Ontario
- 50 What's New in 2024
- 52 IPC Outreach by the Numbers 2024

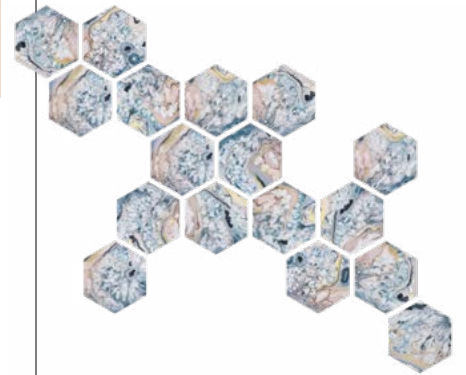


54

Spotlight on Real World Impacts 2024

56

Statistical Highlights



- 66 Organizational Chart
- 67 Financial Summary

special report

68

Ontario's Greenbelt

Access to information and government transparency

Commissioner's Message



As I reflect on my first term as Ontario's Information and Privacy Commissioner, I am reminded of the challenging start to my mandate. Five years ago, the world was in a highly precarious situation. We were just at the beginning of a global pandemic that brought with it unprecedented challenges. Ontarians turned to us for guidance on navigating the heightened privacy risks associated with the new virtual world they were thrust into from one day to the next. We saw increased citizen demand for access to trustworthy information they could rely on in an otherwise dizzying world of misinformation.

The pandemic also forced us, as an organization, to change how we think and work as we adapted to a new social reality that was shifting beneath our feet. To help build resiliency through times of uncertainty, I set out a vision of a modern and effective regulator with real-world impact. Since then, our work has focused on achieving positive outcomes from the perspective of Ontarians to ensure that privacy protection and access to information are not abstract ideals but tangible rights that strengthen the public's trust in their institutions.

Building a foundation of trust

Our mission over the past five years has been to help strengthen a foundation of public trust by enhancing Ontarians' confidence that their privacy and access rights will be respected. We achieve this through 1) proactive advocacy, by championing privacy and access rights in key strategic areas that affect Ontarians' daily lives; 2) responsiveness, by addressing complaints and appeals in a fair, timely, and meaningful way; and 3) accountability, by demonstrating the IPC's commitment to organizational excellence and responsible stewardship of public resources.



OUR MISSION OVER THE PAST FIVE YEARS HAS BEEN TO HELP STRENGTHEN A FOUNDATION OF PUBLIC TRUST BY ENHANCING ONTARIANS' CONFIDENCE THAT THEIR PRIVACY AND ACCESS RIGHTS WILL BE RESPECTED."

This foundation of public trust has never been more important as our world faces yet another existential threat. With an economic war looming over us and our very sovereignty at stake, Ontario — and Canada — are bracing for strong crosswinds to come. There will be stresses on the integrity of our public institutions, and our democracy will be put to the test as never before. Ontarians will expect to be kept well-informed by a government committed to upholding values of truth, access, and transparency in a way that distinguishes us from others. Ontarians will also expect to have their privacy protected in the face of increased border surveillance and the growing influence of a big tech oligopoly beyond our borders whose commercial interests don't always align with the public good.

Readying for the future

In times of crises like these, Ontarians turn to their governments for support and steady leadership. They expect to live in a healthy democracy where their rights and values will be respected, and they can have confidence in the checks and balances that exist to uphold the integrity of their public institutions and the rule of law.

The IPC is a critical part of those checks and balances, and we are well prepared to embrace that responsibility. Our organization today is stronger and more resilient. The foundation we have built to help us navigate through the last crisis will also help us weather the next one. We've strengthened the framework and reinforced the pillars that support public trust. Ontarians' rights and values remain the blueprint that guides our work, and public trust is the cornerstone of everything we do.

Taking a collaborative approach

But to be sure, we are not alone on this journey. Throughout this report,

we will focus on the impact we have had through our many collaborative relationships working with other regulators, consulting with regulated entities, and reaching out to Ontarians, including children and youth, First Nations groups, and marginalized communities.

Through our collaborative approach, we gain a better understanding of different realities and perspectives on the ground and use these to inform our work. It helps us better gauge risks and respond proportionately so we remain agile, relevant and effective as regulators in a fast-changing digital environment. Our collaborative approach also fosters a culture of compliance where institutions respect privacy and access rights not only because they must but also because they know it's the right thing to do; they understand the "why" and feel supported in their efforts.

Strengthening relationships for a stronger Canada

A highlight of this year was the opportunity I had to chair the monthly meetings of Canada's federal, provincial, and territorial (FPT) information and privacy commissioners and ombuds. These meetings culminated in the privilege of hosting the [2024 annual meeting](#) in Toronto. I, along with my FPT counterparts, addressed critical privacy and access to information topics such as the potential of artificial intelligence (AI) to enhance freedom of information processes, understanding Indigenous

concepts of privacy and data sovereignty, and engaging with youth on unique privacy issues they face growing up in the digital age. We also explored emerging technologies, like neurotechnology, and discussed Canada's evolving access and privacy regime.

Out of our discussions also came several important resolutions, including [Identifying and mitigating harms from privacy-related deceptive design patterns](#), [Responsible information-sharing in situations involving intimate partner violence](#), and [Transparency by default — a new standard in government service](#). These resolutions represent a collective commitment by the FPT community to protect the privacy and access rights of all Canadians proving that, together, we are more effective and impactful than any one of us can possibly be alone.

Moving the needle on key strategic priorities in 2024

Our office's work is guided by four strategic priorities: [Privacy and Transparency in a Modern Government](#), [Children and Youth in a Digital World](#), [Trust in Digital Health](#), and [Next-Generation Law Enforcement](#). Each priority was carefully selected at the beginning of my term in consultation with interested parties, institutions, and the public to ensure our efforts focus on areas of greatest concern to Ontarians and where we can have the most positive impact.

Throughout the past five years, including 2024, we have used these

strategic priorities to guide our proactive initiatives and allocate our resources where they count the most. From our advocacy and advisory work to our public education and outreach efforts, we have remained laser-focused on these four strategic priorities. And we are seeing the results. As this annual report will show, our office has developed extensive knowledge and capacity in these areas and is increasingly regarded as a thought leader — locally, nationally, and even internationally — solicited for our views and having influence in these spaces. We have contributed extensively to policy development, helped shape best practices, and raised public awareness, particularly on key issues of artificial intelligence, children's privacy, digital health, and police surveillance technologies.

Advocating for a modern privacy regime

One of the defining features of my term has been championing a modernized access and privacy regime to keep pace with rapid technological change across multiple sectors.

This past year saw the adoption of Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act*. Schedule 1 created a new law, now in force, called the *Enhancing Digital Security and Trust Act, 2024* (EDSTA), which gives the government broad discretion to create rules concerning cybersecurity, artificial intelligence (AI), and digital technologies affecting children and youth. While we fully agree with the need to legislate in these high-risk areas, we remain concerned with the lack of substantive rules in the statute itself. We have consistently recommended and called for a more principled approach, stronger transparency and accountability measures, and more effective and independent oversight.

For example, we recommended that the statute codify binding guardrails requiring AI systems to be safe and reliable, privacy-protective, accountable, transparent, and human rights affirming. This is consistent with our joint statement with the Ontario Human Rights Commission and the ethical AI principles we developed with our FPT partners. We also emphasized the need to clearly delineate no-go zones in statute and provide for independent oversight over the use of AI by public institutions rather than leave such societally important matters entirely for the government to decide on its own and to oversee itself. While we were disappointed not to see our recommended principles codified in statute, we were pleased to see them at least partly taken up in Ontario's *Responsible Use of AI Directive*.

On the issue of minors' digital information, we recommended that Bill 194 deem children's personal information as being sensitive to ensure it receives a higher level of protection. We also recommended that EDSTA explicitly recognize children's rights to personal autonomy, dignity, and self-determination. We expressed serious concern with the minister's new authority to introduce regulations governing the collection, use, and disclosure of children's digital information which overlaps squarely with my office's similar jurisdiction

“
PRIVACY PROTECTION
AND ACCESS TO
INFORMATION ARE
NOT ABSTRACT IDEALS,
BUT TANGIBLE RIGHTS
THAT STRENGTHEN
THE PUBLIC'S TRUST IN
THEIR INSTITUTIONS.”

over these same matters. The potential for duplication, or worse, divergence between the IPC and the ministry risks creating inconsistency and confusion among public institutions at a time when the rules for protecting children's privacy should be certain, predictable and crystal clear.

Schedule 2 of Bill 194 amends the *Freedom of Information and Protection of Privacy Act* (FIPPA). It introduces new privacy obligations for provincial institutions, such as mandatory breach reporting and an express requirement to conduct privacy impact assessments (PIAs). It also expands the IPC's oversight powers, including its authority to issue orders and share information with our federal, provincial, and territorial counterparts. We supported the bill's overall objectives, although here, too, we identified important gaps and made several recommendations for improvement.

One significant recommendation we continue to advocate for strongly is the urgent need to bring equivalent amendments to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). For decades, FIPPA and MFIPPA have operated as twin statutes, with similar jurisprudence, interpretations and guidance. Amending one and not the other risks unravelling years of education and compliance efforts, resulting in confusion and lack of clarity among provincial and municipal institutions. Worse yet, this divergence risks frustrating Ontarians who have rightly come to expect a similar level of rights protection no matter which level of government they interact with.

Although the government did not adopt our recommendations, we see Bill 194 as the beginning — not the end — of a conversation about regulating cybersecurity, AI, children's digital information, and privacy protections more broadly. My office will continue to constructively engage with the



Her Honour the Honourable Edith Dumont, Lieutenant Governor of Ontario (left) hosted Commissioner Kosseim and access and privacy authorities from across Canada as part of the 2024 Annual Meeting of Federal, Provincial, and Territorial Information and Privacy Commissioners and Ombuds.

government and other interested parties in shaping the regulations and guidance that will follow. We will continue to advocate for a coherent regulatory framework with robust protections and accountability measures, coupled with strong and independent oversight, to ensure that innovative technologies are used responsibly to serve the public interest without sacrificing Ontarians' privacy.

Ensuring transparency in government decision-making: The Greenbelt

Access to government records is a fundamental pillar of a healthy democracy. Trustworthy and transparent information allows Ontarians to actively engage as citizens and hold governments to account for their decisions and actions. A prime example of this has

been the significant public interest and scrutiny surrounding decisions about Ontario's Greenbelt.

Over the past year, the IPC has resolved several appeals of access to information requests for records relating to the government's decisions about the removal of land from the Greenbelt. These appeals revealed several systemic themes, including the use of personal devices and email accounts for government business, the use of code words that have the effect of frustrating FOI searches, the lack of proper documentation of key government decisions, and poor retention practices. Such issues, if left unaddressed, risk undermining government accountability and eroding public trust. The IPC's findings, lessons learned, and recommendations for upholding access to information rights in Ontario are detailed in an appendix to this annual report.

Enhancing service to Ontarians

Over the past five years, demand for the IPC's services has grown to an all-time high, with nearly 1,000 more incoming files in 2024 compared to 2020, representing a 30 per cent increase in volumes. At the same time, we have successfully closed a record number of cases and reduced the average time to resolve cases overall, ensuring that Ontarians receive faster and more efficient services. We also managed to reduce our backlog of files by more than 17 per cent. We've achieved these results by streamlining our tribunal operations and adopting more modern and flexible approaches to resolution.

For example, we recently launched an expedited process that fast-tracks straightforward access appeals and complaints, significantly reducing



TOGETHER, WE'VE BUILT A SOLID FOUNDATION, AND WITH THE PRIVILEGE OF A RENEWED MANDATE, I LOOK FORWARD TO CONTINUING TO BUILD ON THIS TO SHAPE A BRIGHTER, MORE TRANSPARENT AND PRIVACY-PROTECTIVE FUTURE FOR ALL THOSE WHO ARE PROUD AND FORTUNATE TO CALL ONTARIO — AND CANADA — HOME."

wait times for many Ontarians. In 2024, our expedited team successfully resolved nearly 15 per cent of all closed files in just its first nine months of operation. We also updated our *Code of Procedure, practice directions, and policies* to improve the timeliness of the general appeals process and make the most efficient use of public resources while still providing fair and just consideration of appeals and being transparent about our procedures.

Faster, smarter operations

As a modern and effective regulator, we've been working hard to enhance our own digital capabilities. By migrating our servers to the cloud and leveraging new digital collaboration tools, we've adopted more modern ways of working and seamlessly connecting with others, while also enhancing the overall cyber security and resiliency of our network. Through better internal communications and knowledge management functions, we've been able to respond more efficiently to increasing demands for our services and provide more timely and accessible answers to public inquiries and requests for consultations.

Our new and improved [website](#) also provides features for improved accessibility and search functions, making it easier for the public to find the information they need quickly and for institutions to have direct access to up-to-date resources and guidance in real time.

Acknowledging our people and our partners

As I look back on the past year, and indeed the past five years, I am proud of what we've accomplished together. By *together*, I mean the many highly dedicated people who have contributed to supporting and advancing the IPC's vision of becoming a modern and effective regulator with real-world impact.

I want to begin by thanking the members of the Legislative Assembly, and particularly, the members of the Board of Internal Economy, for the trust and confidence they have placed in me and my office throughout my first term. I would be remiss if I did not acknowledge their continuing support and how instrumental it has been in helping us fulfil our mandate with the resources and independence we need to be effective. I also want to thank my fellow Officers of the Legislative Assembly and my fellow federal, provincial, and territorial commissioners, both past and present, for their guidance, support and collegiality.

Thanks to the members of our [Strategic Advisory Council](#), who have generously given their time and collective wisdom to the IPC. Through their valuable input and guidance, we have gained a better understanding of the practical access and privacy issues that Ontario institutions face, and the multiple perspectives they bring to the table. SAC members have helped

make us more strategic, effective, and impactful in advancing our strategic goals and have supported us in building bridges and collaborations across various groups and communities of interest.

I am particularly grateful to our [Youth Advisory Council](#), which consists of ten very bright, engaged, and inspiring youth who genuinely care about the state of their digital future and constantly remind us that we should too. By providing us with their feedback, YAC members help make us more relevant and effective in our public education efforts aimed at reaching younger audiences. They help raise awareness about online privacy by serving as privacy leaders and ambassadors among their peers. I was especially proud of their presentation at this year's FPT meeting, where they made an impassioned plea to all Canadian commissioners to remain strategically focused on protecting children's privacy.

Last, but certainly not least, I want to thank the IPC team for the unwavering dedication and passion they bring to their work every day in the service of Ontarians. I am humbled by their hard work and commitment to excellence, their deep knowledge and expertise, and the impressive capacity they have shown for change and innovation. How fortunate I've been to work with such a collegial and professional team that has energized and inspired me every day throughout my term to continue striving for better.

Together, we've built a solid foundation. With the privilege of a new mandate, I look forward to continuing to build on this to shape a brighter, more transparent and privacy-protective future for all those who are proud and fortunate to call Ontario — and Canada — home.

– Patricia

IPC Vision, Mission, and Goals

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

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



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



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



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



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

Cross-Cutting Strategies

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

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

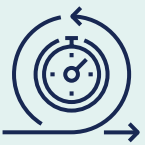
Values

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

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

Mission

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



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



Maintaining their confidence in the organizational excellence of the IPC



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.



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.

3

We will develop the knowledge, skills, and capacity needed, both internally and externally, to advance IPC's goals.

4

We will be bold and aspirational in our vision, but also stay grounded in pragmatism.

FAIRNESS

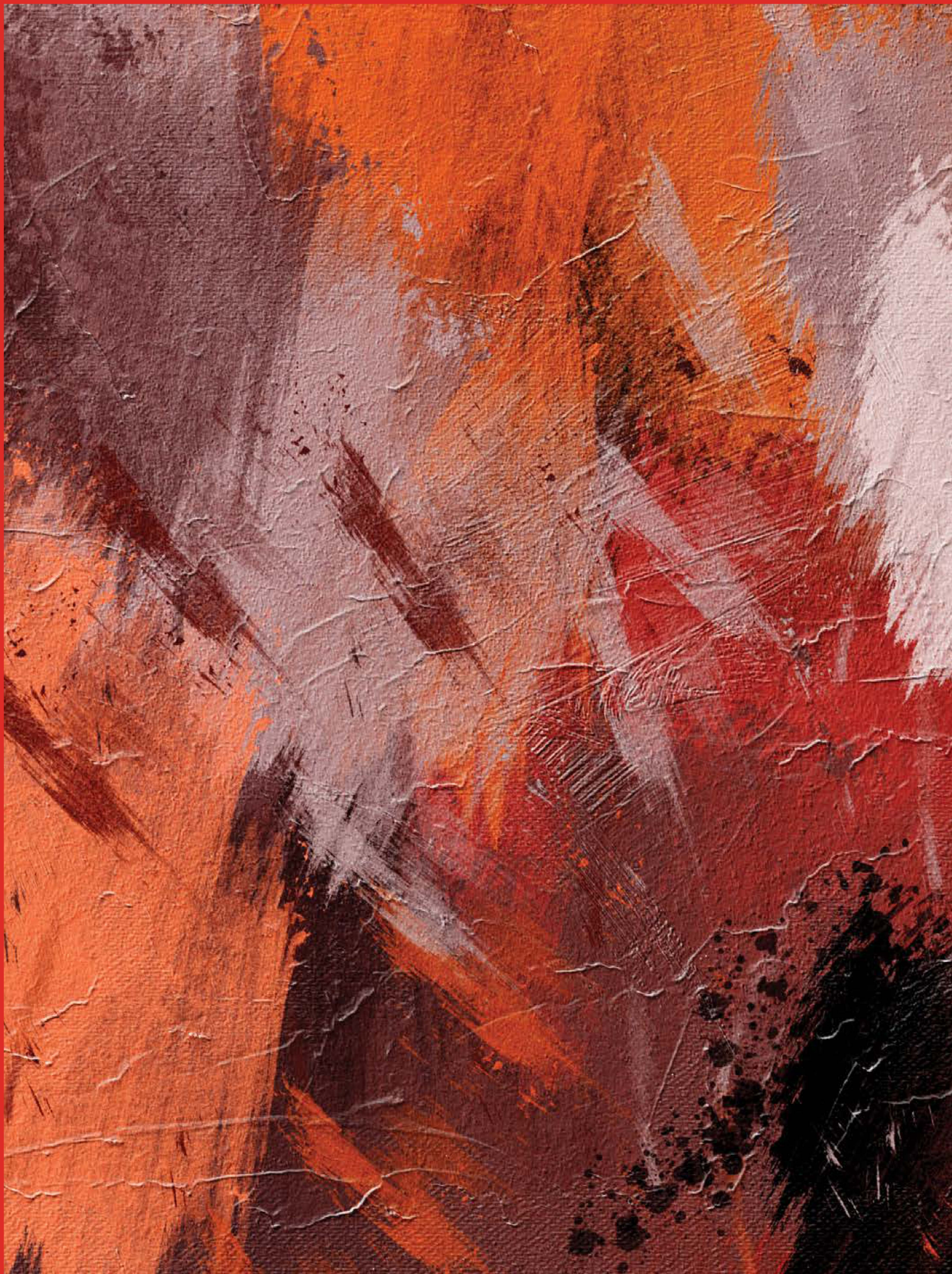
We make decisions that are impartial and independent, based on the law, using fair and transparent procedures.

COLLABORATION

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

EXCELLENCE

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



Advocacy

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



Original artwork by Aedán
Crooke of Surface Impression,
commissioned for the IPC's
[Transparency Showcase](#).

Privacy and Transparency in a Modern Government



IPC goal: 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.

Privacy Day spotlight: Use of AI in a modern government

On January 24, 2024, the IPC had the pleasure of hosting a special event in celebration of Data Privacy Day. *Modern Government: Artificial Intelligence in the Public Sector* presented an opportunity to discuss the benefits and risks of AI use in the public sector with a [panel of experts](#) from different perspectives including government, academia, research, private sector and civil society. The webinar was attended by over 2,200 people in person and online on the day of the event and has since been viewed at least another 2,100 times on our YouTube channel.

Combined, the panelists' contributions were rich, insightful,

and engaging, helping to advance the dialogue around responsible use of AI in the public sector. Panelists discussed the tremendous opportunities for AI to improve public services, such as fast-tracking the processing and delivery

2,200

people attended our Privacy Day event in person and online

2,100

Privacy Day webinar views on the IPC's YouTube channel

of government benefits, informing decision-making by policymakers, and enhancing communications and engagement with residents.

Panelists also discussed the risks involved, including the potential for flawed algorithms that can perpetuate biases, and the reliance on large volumes of personal information that heighten the risks of cyberattacks and breaches. The lack of transparency and potential for misinformation through generative AI tools raise further issues, highlighting the need for responsible AI governance to protect public trust.

As Ontario continues to lead in AI investments and innovation, gaining public trust through effective governance remains crucial for the successful adoption of AI tools by public institutions.

Third party contracting: Essential guidance for public institutions

In 2024, we released guidance on [Privacy and Access in Public Sector Contracting with Third Party Service Providers](#), to help public institutions fulfil their privacy and access obligations when using external service providers to process Ontarians' personal information. The guidance reminds institutions of their continuing obligation to take accountability for personal information within their control, even when it is processed by private sector organizations on their behalf.

The guidance emphasizes the importance of institutions to build in privacy and access requirements through all stages of the procurement process, including, planning, tendering, vendor selection, contracting, agreement management and termination. Throughout, institutions must protect the personal information for which they are responsible, regardless of the mode of service delivery they choose.

“

“No matter the arrangement with a third-party vendor, public institutions must ensure full compliance with Ontario’s access and privacy laws. While public sector organizations may decide to outsource services, they cannot outsource their accountability.”

Updated de-identification guidelines for a new era

In 2024, the IPC began updating its award-winning De-identification Guidelines for Structured Data, originally released in 2016. These guidelines, which earned the International Conference of Data Protection and Privacy Commissioners’ (ICDPPC) award for excellence in research, are a critical resource for institutions.

Throughout 2024, the IPC worked with our Scholar-in-residence, [Dr. Khaled El Emam](#), and consulted with many stakeholders to inform key updates to our guidance in light

THE SUCCESSFUL ADOPTION OF AI TOOLS BY PUBLIC INSTITUTIONS CAN ONLY BE ACHIEVED WITH THE PUBLIC’S TRUST THAT THESE TOOLS ARE BEING EFFECTIVELY GOVERNED. TO GAIN THAT TRUST, WE MUST ENSURE THEY ARE BEING USED IN A SAFE, PRIVACY-PROTECTIVE, AND ETHICALLY RESPONSIBLE MANNER, WITH FAIR OUTCOMES AND BENEFITS FOR ALL ONTARIANS.”

of rapid advances in information technology and evolving risks. The updates are intended to better support public institutions with practical techniques they can use to effectively deidentify data while minimizing the risks of reidentification. The aim of this initiative is to help equip Ontario institutions with the technical guidance they need to manage the increasingly complex nature of

data and make responsible use of it — in *deidentified* form — to advance the public good.



The Beauty and the Benefits: Transparency Showcase 2.0

During Right to Know Week 2024, the IPC proudly launched its Transparency Showcase 2.0, *The Beauty and Benefits of Transparency*. This initiative aims to encourage greater openness and transparency by highlighting exemplary projects from Ontario’s public institutions and the positive impacts that open data and open government initiatives can have on the daily lives of Ontarians.

This past year, we placed particular emphasis on model and creative ways public institutions are being transparent about how they collect, use, and disclose personal information and for what purposes. Criteria for the challenge included creativity, effectiveness, inclusivity, civic engagement, and the transparent use of data for the common good.

This second [Transparency Showcase](#) featured 14 projects, some of which were highlighted in a special episode of our award-winning *Info Matters*



Panelists (from left to right) Dr. Teresa Scassa, Colin McKay, Dr. Christopher Parsons, Stephen Toope, Dr. Jeni Tennison, and Assistant Commissioner Michael Maddock discuss the use of AI by the public sector at IPC’s 2024 Privacy Day event

podcast, as well as feature articles in [Municipal World](#), the [IAPP Digest](#), and [The National Observer](#), among other publications. The showcase offers visitors a chance to browse the projects through captivating audio and video, graphics, and descriptions that bring the initiatives to life. Each project was represented by a unique and original [piece](#) of artwork, including a specially commissioned piece by artist Shelby Gagnon from Aroland First Nation.

“Transparency and access to government-held information is about empowerment. It equips people with the information they need to participate meaningfully in the democratic process, engage in constructive discourse, and hold their governments accountable. It’s the bedrock that democracy is built on, inspiring public trust in evidence-based information that shapes policies, programs, and services to improve Ontarians’ lives.”

A good news story

For more than 25 years, the Ministry of the Environment, Conservation, and Parks (MECP) has processed more freedom of information (FOI) requests than any other institution in Ontario, with the majority coming from businesses looking for records about the environmental history of a property. During the COVID-19 pandemic, MECP’s reliance on paper-based records severely affected its ability to process requests. In 2021, its reported compliance rate for responding to FOI requests within 30 days dropped below 1.5 per cent. This matter was detailed in the IPC’s [2022 annual report](#). Since then, MECP has worked proactively to modernize its recordkeeping, offer alternative service options, and build a robust staffing and FOI program management plan.

In 2024, as a result of these activities, MECP achieved a major

milestone by virtually eliminating its pandemic backlog and climbing to an annual 30-day response rate of 77 per cent, with an expectation of continued improvements in 2025. A key factor in this success has been the [Environmental Property Information Program](#), an alternative service delivery channel which has streamlined access to environmental records and reduced the volume of requests that need to go through the FOI process. Throughout this effort, the ministry has engaged constructively with the IPC, providing regular updates and seeking our feedback. The IPC looks forward to continuing its engagements with MECP as it actively pursues its FOI modernization initiatives. ●



INFO MATTERS PODCAST

Episodes related to Privacy and Transparency in Modern Government in 2024

› S4 EPISODE 3

No government ID: Navigating homelessness, identity, and privacy

› S4 EPISODE 6

Why mediation matters: Improving outcomes in FOI appeals

› S4 EPISODE 7

The beauty and benefits of transparency: Ontario’s public institutions rise to the challenge with innovative projects

› S4 EPISODE 8

Indigenous led innovation: Aligning technology with community values



Digital painting of Frank Lloyd Wright’s Fallingwater by Aedán Crooke of Surface Impression, commissioned for the IPC’s [Transparency Showcase](#).

Children and Youth in a Digital World



IPC goal: 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.

Digital Privacy Charter for Ontario Schools

On [Digital Citizen Day](#), the IPC released the [Digital Privacy Charter for Ontario Schools](#), inviting schools and school boards to pledge their commitment to protecting students' personal information while also empowering students to make informed privacy choices. The charter consists of twelve high-level commitments reflecting a "smart mix" of existing legal obligations, best practices, and common sense, for educators to earn the confidence of the students, parents, and communities they serve.

The commitments are intended to promote strong privacy protections in the digital education tools and services used by schools and support ongoing learning by empowering students to understand and exercise their privacy and access rights in an



Original artwork by Aedán Crooke of Surface Impression, commissioned for the IPC's [Transparency Showcase](#).

increasingly digital world. By signing on to the charter, school boards can show exemplary leadership. They can also demonstrate their level of preparedness to meet the anticipated requirements of EDSTA, which are designed to protect student privacy

and regulate digital technologies used by school boards.

"As schools continue to integrate education technologies into their classrooms, it's now more important than ever for school boards to have security, transparency, and accountability measures in place to strengthen privacy protections for students. Schools and school boards are essential partners in preparing young people to be safe and responsible digital citizens. By signing on to the charter, educators can demonstrate their commitment to making student privacy a top priority."

Advancing digital literacy: Ontario's new curriculum promotes privacy skills

For years, the IPC has [advocated](#) for stronger privacy education for children. In 2024, we were delighted to see Ontario launch its revised [Elementary Language Curriculum](#) (grades 1-8), which prominently features the promotion of privacy skills. The curriculum introduces a new focus on digital literacy, digital citizenship, and online safety. These learning objectives directly align with the IPC's [Privacy Pursuit! lesson plans](#) for grades 2-8 we launched last year, as well as our [Digital Privacy Charter for Ontario Schools](#). They are also entirely consistent with the Global Privacy Assembly's [Personal Data Competency Framework for Students](#), co-sponsored by the IPC in 2016.

We were very pleased to see that [MediaSmarts](#), Canada's centre for digital media literacy, has integrated content from the IPC's [Privacy Pursuit!](#) lesson plans into digital textbooks, released in early 2025, to support Ontario's new curriculum. These digital textbooks will provide students with valuable, practical insights on privacy and online safety, helping them develop critical privacy skills to navigate the digital world confidently.



Building future privacy leaders: IPC Youth Advisory Council

This year, the IPC's [Youth Advisory Council](#) (YAC) helped develop our first-ever [Youth Ambassador Program](#), aimed at empowering young people to champion online privacy awareness by spreading the word about digital literacy and privacy rights among their peers. The YAC provided advice on a [Youth Ambassador Toolkit](#), including a slide deck, speaking notes, handouts, a presenter's guide, a train-the-trainer tip sheet, as well as social media resources — everything

“

EMPOWERING CHILDREN WITH THE KNOWLEDGE AND SKILLS THEY NEED TO UNDERSTAND AND NAVIGATE THE ONLINE WORLD HELPS THEM EXERCISE THEIR PRIVACY RIGHTS AND MAKE INFORMED, THOUGHTFUL DECISIONS ABOUT WHAT PERSONAL INFORMATION THEY WISH TO SHARE, AND WITH WHOM. BUT WE CANNOT DOWNLOAD ALL RESPONSIBILITY ON THEIR SMALL SHOULDERS ALONE. IT IS INCUMBENT ON US, AS GOVERNMENTS, REGULATORS, SCHOOLS, AND EDUCATORS, TO PROTECT THEM AND THEIR PERSONAL INFORMATION ONLINE FROM THE FORCES THEY CANNOT SEE OR CONTROL.”

young leaders need to be effective privacy ambassadors.

Throughout the year, the YAC provided the IPC with timely and valuable feedback on our public outreach efforts, including

social media, to help improve our effectiveness and impact when communicating with this younger demographic. They also helped us update our frequently asked questions on children's consent in the area of child and family services.

At the annual FPT meeting, hosted by the IPC this year, a panel of YAC members engaged directly with Canada's information and privacy commissioners and ombuds to discuss the need to protect the rights of Canada's children and youth in the digital age. Moderated by [Jane Bailey](#), Professor at the University of Ottawa, the panel provided firsthand insights into the challenges youth face in a digitally networked environment. They emphasized the importance of policies and educational programs to equip young people with the knowledge and tools they need to fully and safely participate in the digital world.

Youth privacy: A global matter

At the Global Privacy Assembly in October, Commissioner Kosseim was invited to chair a panel on youth privacy, *Education from the Ground Up*:

IPC's Youth Advisory Council





Commissioner Kosseim discusses the importance of empowering young people at the 46th Global Privacy Assembly



INFO MATTERS PODCAST

Episodes related to Children and Youth in a Digital World in 2024

› S3 EPISODE 9

Empowering young women and girls in the digital world

› S4 EPISODE 1

In their own words: Students from Westboro Academy speak out about privacy

› S4 EPISODE 9

Technology in the classroom: Digital education, privacy, and student well being

The Societal Impact of Privacy Education. The Commissioner led an engaging discussion on the role of privacy education in empowering children to navigate the digital world safely. The panel featured esteemed experts, including Baroness Beeban Kidron, Founder of [5Rights Foundation](#),

who spoke about the importance of balancing protection with empowerment; Bertrand du Marais, Commissioner at France's [Commission Informatique & Libertés \(CNIL\)](#), who provided insights on international commitments to privacy education; Amy Lam, Deputy Privacy Commissioner at Hong Kong's [Office of the Privacy Commissioner for Personal Data \(PCPD\)](#), who shared local efforts to advance digital education; and Matthew Johnson, Director of Education at MediaSmarts, Canada's Centre for Digital Media Literacy, who highlighted Canadian research and the integration of digital literacy in the school curriculum.

Law reform for youth privacy

In May, the IPC made [recommendations](#) to the Standing Committee on Social Policy on Bill 188, the *Supporting Children's Futures Act*. The proposed amendments to the *Child, Youth*

and Family Services Act (CYFSA) were aimed at modernizing and standardizing important safeguards throughout the child and youth services sector.

The IPC's submission urged that proposed exceptions to the existing statutory publication ban protecting the privacy interests of children and youth be set out in legislation rather than regulation, to ensure transparency and proper balancing of privacy interests of all affected individuals.

We also questioned a new provision that would permit the Ministry of Children, Community and Social Services to keep retaining personal information of individuals who are no longer in care, for purposes of research, compliance, planning and delivery of services. The IPC continued its call for the government to repeal the excessively broad personal information collection scheme under sections 283 and 284 of the CYFSA. ●

Trust in Digital Health



IPC goal: to promote confidence in the 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 accountability program to build patient trust

Throughout 2024, the IPC worked to develop privacy guidance specifically customized for small health information custodians (HICs) under the *Personal Health Information Protection Act* (PHIPA). The IPC's *Privacy Management Handbook for Small Health Care Organizations* provides the basic elements they need to build an effective privacy management and accountability program their patients can trust.

Health care providers, both large and small, must comply with their legal responsibilities to protect patients' personal health information. However, we recognize that one size does not fit all. Small providers are often strapped for time, capacity, and resources, and this guidance is intended to help make it easier for them to understand and comply with their basic privacy obligations under the law.

The guidance outlines best practices for developing a privacy management



Privacy Management Handbook for Small Health Care Organizations offers practical guidance to help smaller organizations meet their obligations under Ontario's health privacy law.

program tailored to the needs of small health information custodians, considering their size and specific circumstances. A well-implemented privacy management program helps HICs uphold good practices and identify areas in need of strengthening, so they can continually strive to improve by developing greater privacy maturity and sophistication over time.

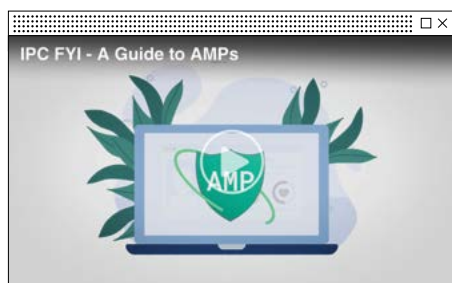
AI in health

AI has the potential to vastly improve medical diagnostics, accelerating access to early interventions and treatments that could save lives. AI can also reduce administrative burdens on health providers by automating many routine tasks. Some say this could free up their time so they could take on more patients, helping to resolve the shortage of health providers in Ontario, or at least, enhance the quality of their interactions with existing patients. Introducing AI in health, however, also ushers in new privacy, safety, and ethical considerations that must be factored in and addressed as part of responsible innovation.

Throughout 2024, the IPC has conducted extensive research on the use of AI in Ontario's health care sector, with a particular focus on AI scribe technology. The IPC's guidance, set for release in 2025, will provide health care providers with key considerations for using AI in a way that complies with PHIPA, particularly around patient consent, transparency, security, and data protection.

IPC FYI: The Trust in Digital Health series

To demystify what are often complex concepts in PHIPA, both for individuals and providers, the IPC released a special IPC FYI Health Privacy series. These short, animated, and easy-to-access videos highlight some of the



obligations of health information custodians under PHIPA, and let individuals know about their rights in simple, plain language.

The three short videos we released as part of the IPC FYI Health Privacy series include:

› [IPC FYI: A Guide to AMPs](#).

This short video aimed at health providers describes the purpose of AMPs, the circumstances under which AMPs might be issued, and the factors influencing the penalty amounts on a case-by-case basis.

› [IPC FYI: Sharing Health Data](#)

describes the situations in which health information custodians can engage in responsible sharing of personal health information under PHIPA, including for research, health system planning and public health.

› [IPC FYI: Understanding PHIPA](#)

raises awareness among Ontarians about their right to access their health record. This video also describes basic rules health providers must follow when collecting, using, and disclosing personal health information, as well as their obligations to keep it safe and secure, particularly in the digital health context.

In addition to the IPC FYI Health Privacy video series, we launched a [patient privacy hub](#) on our website to help Ontarians better understand and exercise their rights under PHIPA. Many patients are unaware of what they can expect from their health provider in terms of privacy protection.

They may not know about their right to access their own health records or how to navigate the process effectively.

In response, the IPC developed a user-friendly portal that brings together essential guidance, resources, and other key tools specially tailored for patients. By consolidating high-value resources in a one-stop shop, the IPC is helping individuals take control of their personal health information and make more informed decisions about how it is managed.

Advocacy for protecting health privacy and access rights

In 2024, the IPC continued its advocacy to protect Ontarians' privacy and access rights in the evolving digital health landscape. Central to these efforts was [our critique](#) of Schedule 6 in the *More Convenient Care Act*, which proposed significant changes to PHIPA. The IPC raised concerns about the diminished rights to access personal health records, the risks posed by an overly complex and inconsistent privacy framework, and the extensive reliance on vague rulemaking for implementing Digital Health IDs. These amendments,

4,300

downloads of Info Matters podcast episodes on Trust in Digital Health since its release

designed to enable patient access to their electronic health records (EHRs), lack sufficient safeguards, clarity on their use, and transparency about the roles of Ontario Health and third parties involved in the system.

The IPC emphasized the need for a simpler, more streamlined and coherent legislative approach. We called for stronger privacy protections, clear limits on data use, and stronger oversight mechanisms. Recommendations included retaining individuals' full access rights to their health records, embedding privacy-enhancing principles such as data minimization, and ensuring transparency in the governance of digital health tools.

“

PUTTING PATIENTS AT THE CENTRE OF CARE MEANS SAFEGUARDING THEIR PRIVACY, ENSURING THEIR ACCESS RIGHTS, AND FUNDAMENTALLY RESPECTING THEIR DIGNITY. THE IPC'S PATIENT PRIVACY HUB IS DESIGNED TO HELP ONTARIANS FEEL CONFIDENT IN NAVIGATING THEIR PERSONAL HEALTH INFORMATION SO THEY CAN SEEK CARE WHEN THEY NEED IT MOST, KNOWING THEIR RIGHTS ARE PROTECTED.”

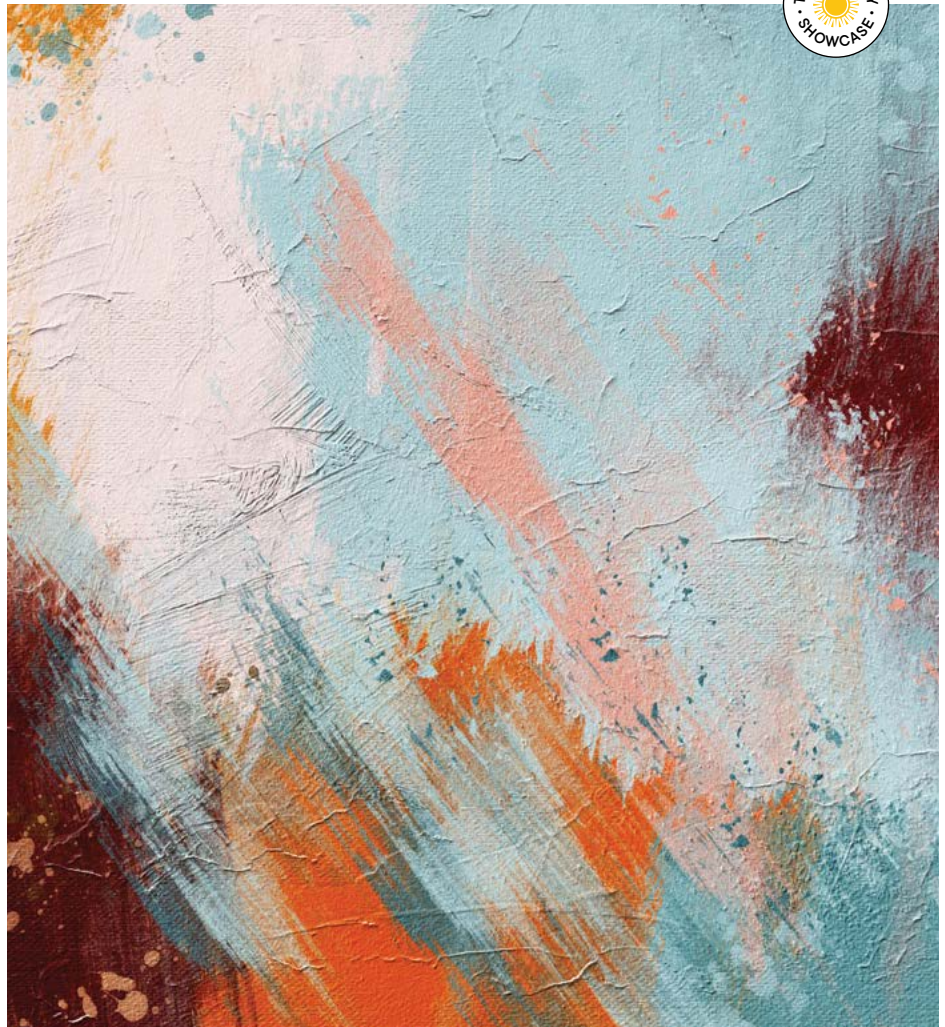
Data Integration under FIPPA

Part III.1: IPC orders

Under Part III.1 of FIPPA, interministerial data integration units (IMDIUs) are government teams that are conferred special authority to link together different sets of personal information to be used and analyzed for purposes of planning, managing and evaluating government programs and services. Given this unique authority, IMDIUs are held to defined transparency, privacy, and security standards, and are subject to review of their practices and procedures by the IPC, both initially, before linking any personal information, and then at least every three years thereafter.

At the end of 2024, the IPC launched the first three-year review of the Ministry of Health's IMDIU, following its initial review in 2022. The initial review found areas of significant risk. As a result, the IPC issued several orders to bring the ministry into compliance with the required data integration standards established by the Minister of Public and Business Service Delivery and Procurement and approved by the IPC. In particular, we ordered the ministry to update its privacy impact assessments and threat/risk assessments to identify and address privacy and security risks arising from using legacy and shared technical infrastructure in the new data integration context. Also, we ordered the ministry to implement a business continuity and disaster recovery plan in accordance with the required standards. The deadline to comply with these orders was September 30, 2022.

The IPC is highly concerned that these and other orders remain outstanding to this day, despite having given several extensions and made numerous attempts to support the ministry in their efforts. The failure of the ministry to comply with IPC's orders seriously undermines the very purpose and integrity of the data



Original artwork by Aedán Crooke of Surface Impression, commissioned for the IPC's [Transparency Showcase](#).

integration regime established by government itself. The IPC strongly recommends that government allocate the necessary funding and expertise in privacy and data governance to bring the ministry into compliance with the required data integration standards as soon as possible. The IPC will take into account this state of continuing non-compliance as we conduct our three-year review of the Ministry of Health's IMDIU and will expect a swift resolution of these outstanding issues and any new issues that are identified. ●



INFO MATTERS PODCAST

Episodes related to Trust in Digital Health in 2024

› S4 EPISODE 4

Artificial intelligence in health care: Balancing innovation with privacy

› S4 EPISODE 10

Lessons in health privacy: Key takeaways from 2024

Next-Generation Law Enforcement



IPC goal: 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.

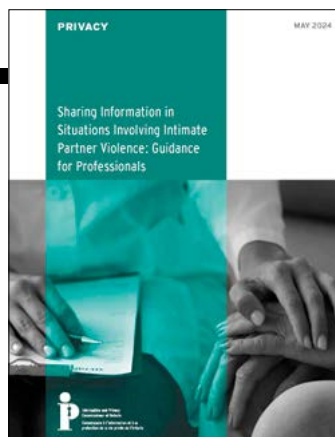
violence-informed approach to information-sharing that increases the security, control, and resilience of victims, survivors, and their families. The guidance specially calls for a culturally sensitive approach that considers historical, cultural, and internal biases to prevent further victimization of historically marginalized communities. The IPC has been heartened by the uniformly positive response to the guidance, and its widespread adoption by organizations across the sector. The guidance is currently featured on the Association of Municipalities of Ontario's [Gender-based Violence Resources for Municipal Elected Officials](#) and the Ministry of the Solicitor General's [Guidance on information sharing in multi-sectoral risk intervention models](#).

Further to this work, the IPC, together with our FPT counterparts, issued a joint resolution on November 27, 2024, during Woman Abuse Prevention Month, to support responsible information-sharing in contexts involving IPV. The resolution affirms that Canada's privacy laws generally permit the disclosure of personal information to prevent injury or loss of life in IPV situations and calls on governments and organizations to develop privacy compliant governance frameworks around disclosure practices. It also highlights the need for training, transparency in disclosure

Sharing information in situations involving intimate partner violence

In May 2024, the IPC released new guidance on [Sharing Information in Situations Involving Intimate Partner Violence \(IPV\)](#). This guidance was developed in response to recommendation 78 from a 2022 Ontario coroner's inquest into the tragic deaths of three women at the hands of their former partner. The resulting guidance provides a clear, practical approach, specifically tailored for professionals, to support responsible information-sharing in situations where there's a risk of serious harm to a person's health or safety.

Based on consultations across the justice, health, and social services sectors, as well as those with lived experience of IPV, the guidance advocates for a trauma and



“

INTIMATE PARTNER VIOLENCE IS A DEVASTATING AND PERVERSIVE REALITY IN OUR SOCIETY. WE KNOW AND RESPECT HOW SERIOUSLY PROFESSIONALS TAKE THEIR OBLIGATION OF CONFIDENTIALITY, BUT INJURY OR LOSS OF LIFE SHOULD NEVER HAPPEN BECAUSE OF A HESITANCY TO SHARE VITAL INFORMATION BASED ON A MISUNDERSTANDING OF PRIVACY LAWS.”



Experts gathered at the IPC's IGG workshop to discuss proposed guardrails for the responsible use of investigative genetic genealogy.

practices, and a culturally sensitive approach when serving marginalized and vulnerable groups. By supporting a better understanding of the conditions under which personal information may be disclosed, this resolution helps alleviate the 'privacy paralysis' that inhibits information sharing and support timely interventions to prevent injury or loss of life.

Shaping the future of investigative genetic genealogy

In 2024, the IPC furthered its research and policy work on an emerging investigative tool called Investigative Genetic Genealogy (IGG). IGG involves collecting a DNA sample from a crime scene and comparing it against profiles in private sector DNA databases to search for partial family matches, using new, sophisticated

“
THE IPC STRONGLY
RECOMMENDS THAT
POLICE SERVICES ADOPT
THESE GUARDRAILS IF
USING, OR CONSIDERING
USING IGG AS AN
INVESTIGATIVE
TECHNIQUE IN ADVANCE
OF ANY EXPLICIT LEGAL
AUTHORITY AND
PROPER STATUTORY
CONTROLS IN THIS
NOVEL AREA.”

genetic sequencing techniques. Then, using genealogical research and tactical surveillance methods, police begin to narrow down investigative leads in their search for possible suspects. Police are increasingly using IGG to solve serious crimes, but it also raises significant legal, privacy and ethical considerations. Building on insights from the IPC's [Privacy Futures Project](#) in 2023, we engaged directly with interested parties to develop meaningful guidance that balances public safety with fundamental privacy and human rights.

A major step in this effort was a half-day workshop in January 2025 where we convened experts from across Ontario and the US, including forensic scientists, privacy and human rights experts, bioethicists, civil society, victims' rights advocates, academics, police services, government representatives, and First Nations technology leaders. Participants expressed broad consensus on the need for clear, enforceable standards to ensure IGG is used responsibly. Discussions centred on twelve guardrails we proposed to guide whether IGG should be used and if so, in what circumstances and how. We sought participants' input on these proposed guardrails, based on established privacy principles and best practices, and their technical feasibility, policy implications, and operational impact.

Based on this feedback, we finalized our guidance, [Guardrails for Police Use of IGG in Ontario](#). The guardrails include the need to ensure lawful authority, necessity, accountability and transparency of IGG investigative tools, together with data security safeguards and procurement guidance to uphold privacy rights of Ontarians. Other guardrails include controls on surreptitious DNA collection, limits on retention of DNA or DNA-derived information, and guidelines for ethical disclosure.

ALPR: Evolving tech, greater risks

In 2024, the IPC released updated guidance on the [Use of Automated Licence Plate Recognition Systems by Police Services](#) to reflect evolving technologies and their expanded uses in law enforcement. ALPR systems, both fixed and mobile, capture and compare large volumes of licence plate data against databases, supporting police services in identifying vehicles with stolen or expired plates and those registered to suspended drivers.

Police services now use this technology for a wider range of law enforcement tasks, including tracking vehicles tied to criminal investigations, monitoring the movements of known offenders, and identifying

vehicles involved in serious crimes such as human trafficking and drug smuggling. This broadened use brings risks to both privacy and fundamental human rights.

The IPC collaborated with law enforcement agencies, privacy experts, and civil society to develop best practices for ALPR policies, procedures, and technical controls. The updated guidance highlights key obligations under Ontario’s privacy laws and offers practical advice for using ALPR systems in a way that protects privacy and human rights. Some of the key recommendations include conducting a thorough privacy impact assessment prior to deploying an ALPR pilot or program, regularly reviewing hotlist databases to ensure they are kept accurate and up to date, immediately

destroying non-hit data, notifying the public about the location of cameras, engaging and consulting with affected communities, and building in the necessary privacy and transparency requirements in contracts with third party vendors. ●



INFO MATTERS PODCAST

Episodes related to Next Generation Law Enforcement in 2024

› S4 EPISODE 2

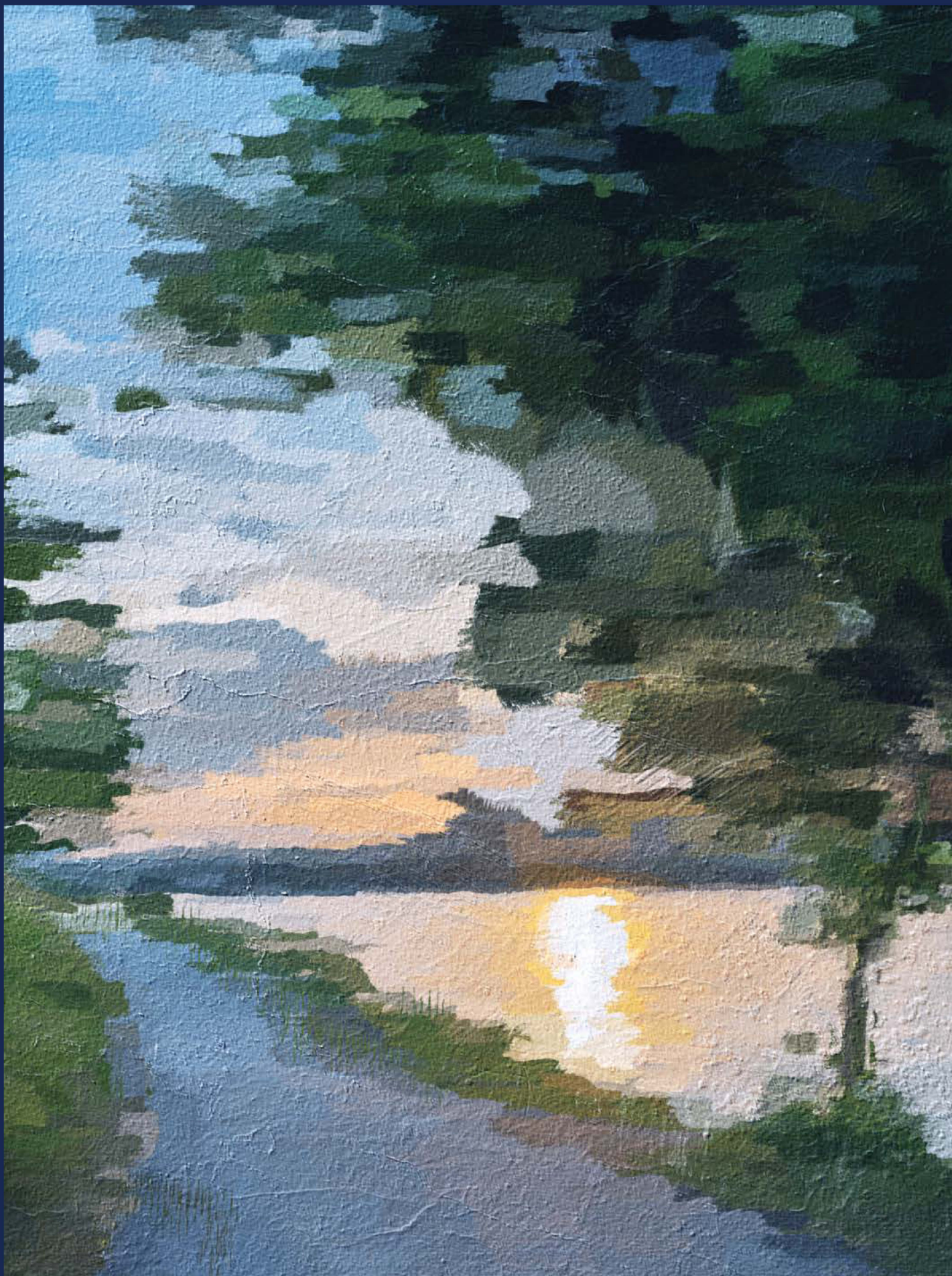
At face value: Facial recognition technologies and privacy

› S4 EPISODE 5

Addressing intimate partner violence: Information sharing, trust, and privacy

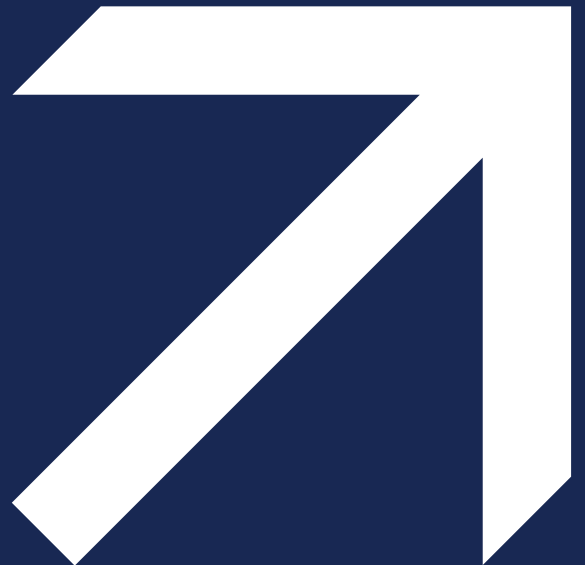


Original artwork by Aedán Crooke of Surface Impression. Artwork commissioned for the IPC’s [Transparency Showcase](#).



Responsiveness

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



Original artwork by Aedán
Crooke of Surface Impressions,
commissioned for the IPC's
[Transparency Showcase](#).

Enhancements to Tribunal Efficiency and Responsiveness



The IPC helps Ontarians exercise their access and privacy rights by striving to resolve appeals and complaints in a timely way and issuing decisions that are fair, plain language, and practical. We support understanding of the law by publishing actionable guidance based on trends and lessons learned from individual cases.

Over the past five years, the IPC has seen a 30 per cent increase in incoming files, rising from 2,768 in 2020 to a record high of 3,613 in 2024. Despite this significant growth in caseload, we have made substantial improvements in efficiency, ensuring that Ontarians receive timely resolutions to their privacy and access concerns.

In 2024, the IPC closed 3,084 files, marking the highest number of closures in IPC history. Of those, 2,719, or 88 per cent, were successfully resolved or dismissed through early resolution, expedited process or mediation, avoiding the need for lengthy adjudication. At the same time, we reduced the average time to resolve access appeals by 8 per cent, from

3,084

closed files in 2024

88%

were successfully resolved or dismissed through early resolution, expedited process or mediation.

10.7 months in 2023 to 9.9 months in 2024. Average time to resolve privacy complaints saw an even greater drop in average processing time of 9 per cent,

from 5.9 months to 5.4 months. We managed to reduce the backlog by more than 17 per cent from the beginning to the end of 2024.

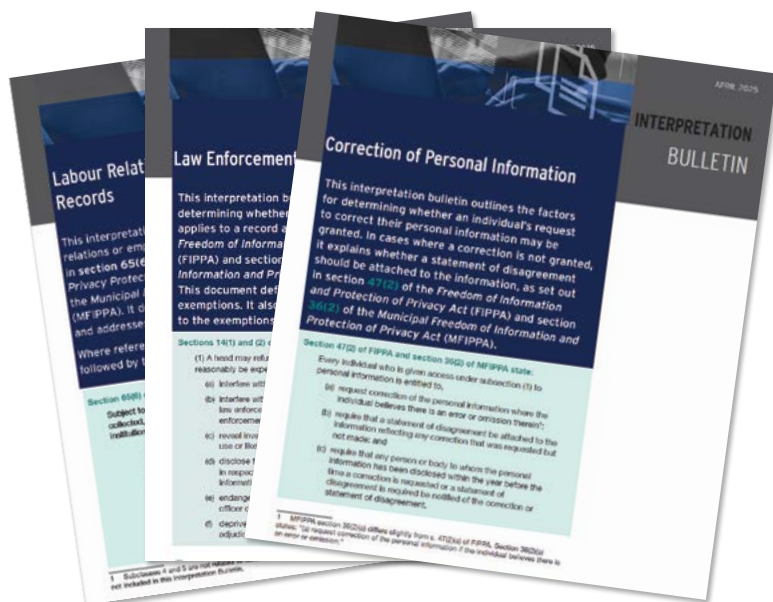
Looking ahead, we will continue to build on these efficiencies to manage growing demand while maintaining the highest standards of service.

New tribunal processes for a digital future

On September 9, 2024, we introduced a wholesale review of our [Code of Procedure](#), with related practice directions and policies, for processing appeals under FIPPA and MFIPPA. The purpose of this review was to reflect the IPC's current and planned operations for considering appeals; improve timeliness of processing of appeals; maintain the fair, just, and expeditious consideration of appeals; and provide greater transparency and understandability of our processes and procedures, including timelines, so parties know what to expect.

One key improvement in the revised code is our new [expedited process](#) for handling straightforward issues. This new process reduces resolution times by streamlining the handling of preliminary or interlocutory issues through a single-person processing model from start to end. This new process has greatly enhanced our efforts to resolve files quickly and ensure faster outcomes for Ontarians. Since it began operations in March 2024, the expedited team successfully closed 619 files. Compared to before, average time to resolve *reasonable search* files has been reduced by 117 days, *fee-related* files have been resolved up to 193 days faster, and *interim* decisions are wrapping up 161 days sooner. We've also reduced the time to resolve *failure to disclose* files by 107 days and *failure to provide access* files by 123 days.

The code, policies, and procedures were also updated to reflect our new



Interpretation bulletins help clarify how Ontario's access and privacy laws are applied, supporting better decision-making by institutions and smoother resolutions for the public.

By codifying these interpretations and making them readily available on the IPC's website, we can help institutions respond more effectively to information requests from the outset. These interpretation bulletins also allow parties to an appeal know more clearly what to expect earlier on during our informal resolution process, helping to avoid protracted disputes having to go all the way through adjudication.

To further enhance accessibility, the IPC launched a new [IPC FYI Appeal Process](#) video series to provide short, engaging explanations of key tribunal appeal processes. The four videos, released in 2025, walk Ontarians through the appeals process — intake, expedited process, mediation, and adjudication. These videos, available in English and French, are complemented by glossaries, infographics, and other online resources to support public understanding.

By combining clear, written guidance with dynamic video content, we are modernizing the way Ontarians engage with access and privacy law, making our processes more transparent, accessible, and user-friendly than ever before. ●

e-appeals process, introduced in 2022. This new, digital-friendly way for individuals to file complaints and appeals and to pay for them online is working to reduce processing times and increase efficiencies. In 2024, 73 per cent of incoming appeals came through our e-appeals process, up from 71 per cent in 2023.

Among other updates, the code introduces a new requirement for parties to disclose when they have used AI tools to prepare their submissions. Parties must now disclose to the IPC if AI was used, the type of AI, and how it was applied. Where AI is used to prepare submissions, parties must review the accuracy and content of any legal references or analysis and certify in writing that they have completed that review.

Tribunal orders and decisions: summaries made simpler

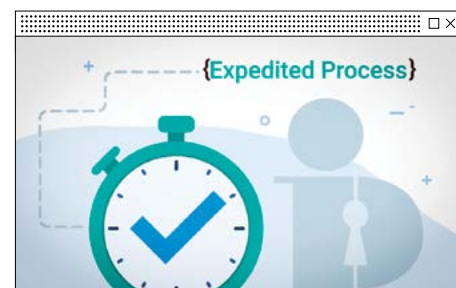
As part of our efforts to improve and modernize, we have prioritized making our [orders and decisions](#) clear and accessible for all Ontarians. Through ongoing training and quality assurance reviews, we've prioritized

plain language writing to ensure they are clearly understood by all parties.

Our efforts are bearing fruit. In 2024, we contracted third party experts in plain-language legal decision-writing to evaluate a sample of our decision summaries. The average overall score for readability and accessibility of this year's sample was the equivalent of 8.13 on a fifteen-point scale, showing a slight improvement from last year. The distribution of scores across samples was also more concentrated, suggesting greater consistency in summary writing.

Demystifying access and privacy law: IPC's interpretation bulletins and FYI video series

Throughout 2024, the IPC added to its suite of interpretation bulletins to promote a greater understanding of Ontario's access and privacy laws. These bulletins are intended to help individuals and institutions better understand how the IPC and the courts have interpreted various sections of FIPPA and MFIPPA.



A Review of Noteworthy Cases

A worrying rise in cyberattacks in the MUSH sector

Over the past several years, Ontario organizations have become increasingly vulnerable to cyberattacks. According to the [Canadian Internet Registration Authority's 2024 Cybersecurity Survey](#), the risks of cyberattacks, particularly to municipalities, universities, schools and hospitals — or the MUSH sector — are on a rise. The survey found that 55 per cent of MUSH sector organizations had experienced a cyberattack in 2024, compared to 38 per cent in 2023. Of these attacks on MUSH sector organizations in 2024, 29 per cent were successful, compared to 22 per cent in 2023.

MUSH sector organizations store vast amounts of personal information and must maintain critical operations *through thick or thin*, leaving them particularly at the mercy of cyberattacks. While some hackers focus on locking down data to disrupt services, others threaten to publish sensitive personal information on the dark web. In either case, organizations must act quickly to contain the breach, recover the data, and investigate the root cause. Organizations affected by cyberattacks must notify those affected in a timely and appropriate manner, considering factors such as

the number of people impacted, the sensitivity of the data involved, and any ongoing privacy risks. And most importantly, organizations must put in place remedial measures to minimize the risks of such breach from recurring.

Responding to cyberattacks

Throughout 2024, the IPC received a number of high-profile breach reports by institutions that had been subject of major cyberattacks. The IPC resolved several of these cases by ensuring the affected institutions contained the breach, took satisfactory steps to identify the root cause, notified affected individuals, and implemented remedial measures to prevent future attacks. Among these resolved cases are [MOVEit](#) (in relation to a prescribed person under PHIPA), [Innomar Strategies](#), [Toronto Public Library](#), and the [Toronto District School Board](#).

Other cyberattack incidents that could not be resolved early on proceeded to a fuller investigation by the IPC. An example is [PHIPA Decision 249](#). This investigation involved a ransomware attack on a medical imaging clinic, compromising over 500,000 patient records. Unfortunately, the clinic ended up having to pay the ransom to restore access to its records and resume providing health services.

The clinic responded to the attack by shutting down its servers immediately and engaging cybersecurity experts to investigate the source of the breach. By the end of our investigation, the IPC found that the clinic acted appropriately in containing the breach, notifying affected individuals, and improving cybersecurity measures on a go-forward basis, including by limiting administrative access and maintaining reliable offline backups.

Encryption: To notify or not to notify?

When personal information is locked down or encrypted by a threat actor — making it inaccessible or unavailable to authorized users — it can be considered a loss or unauthorized use of that information. This is so even if the files themselves aren't accessed or taken (exfiltrated) from the system. In a series of four decisions issued in 2024, the IPC clarified the obligation of organizations to notify affected individuals in such cases.

Three of these cases ([PHIPA Decision 253](#), [Decision 254](#) and [Decision 255](#)) involved health information custodians (HICs) subject to the *Personal Health Information Protection Act* (PHIPA), and the fourth case ([CYFSA Decision 19](#)) involved a children's aid society subject to Part X of the *Child, Youth and Family Services Act* (CYFSA). In all four cases, the organizations took the position that there was no duty to notify affected individuals because there was no evidence that personal health information or personal information was exfiltrated from their systems. The IPC disagreed, finding that the loss or unauthorized use or disclosure of personal (health) information triggered the duty to notify affected individuals, under PHIPA, even if the cyberattack did not result in the exfiltration of the information.

Two of these respondent organizations, the Hospital for Sick



Digital artwork by Amy Jiao of Surface Impression, commissioned for the IPC's [Transparency Showcase](#).

Children and the Halton Children's Aid Society, disagreed with the IPC's decisions and filed for judicial review of PHIPA [Decision 253](#) and CYFSA [Decision 19](#), respectively (see IPC in the courts).

Ensuring privacy protections on university campuses

In 2024, the IPC addressed significant privacy concerns related to the use of

personal data in university settings, reinforcing the need for transparency, consent, and compliance with privacy laws.

In PHIPA [Decision 243](#), the IPC investigated an anonymous complaint from a group of physicians regarding the UTOPIAN health research database at the University of Toronto. The physicians alleged that the personal health information used to populate the database had been

extracted without patient consent and without providing them with sufficient information about the research. The physicians also alleged that the personal health information was not adequately de-identified before being sold or otherwise provided to third parties.

The IPC's investigation found that the university had violated several research conditions of section 44 of PHIPA. Of significant concern was the fact that the university had been operating UTOPIAN for some time after the Research Ethics Board (REB) approval had lapsed and had not informed the participating physicians of this. The investigation also found that the university failed to provide copies of the research plans to the physicians and did not effectively amend these research agreements to reflect the expanded information it began collecting, using and retaining from patient records. Although patient consent was not required, the university failed to conduct the required site visits to ensure compliance with patient notice requirements in doctors' offices. The IPC found no concerns with the deidentification method being used, and no evidence of unauthorized data sale to commercial third parties.

The IPC recommended that the university update its research agreements with contributing physicians to reflect its current practice and that it comply with the terms of those agreements. The IPC also recommended that the university update its means of notifying patients about the project, conduct a reidentification study to assess the continuing effectiveness of its deidentification procedures, and improve its transparency with physicians who agreed to provide patient data to the research database.

This case highlights the importance of compliance with privacy regulations

to maintain ethical research practices and public trust in the use of health data for research.

Lessons from Waterloo: The importance of due diligence in smart tech procurement

In February 2024, media reports brought to light that intelligent vending machines equipped with face detection technology had been installed on the University of Waterloo's main campus. These machines were part of a snack vending services agreement between the university and a third-party provider.

The IPC's investigation found that the machines used cameras to capture identifiable facial images, resulting in an unauthorized collection of personal information and a privacy breach. However, there was no evidence indicating that identifiable information was further used or disclosed. The collection occurred without proper notice to individuals.

55% of MUSH sector organizations experienced a cyberattack in 2024.

Of these attacks, **29%** were successful.

The investigation further revealed that these issues resulted from flaws in the university's tendering and procurement process. Specifically, the process failed to examine the full supply chain and did not identify or assess the use of facial detection technologies in the machines.

When institutions are considering smart technologies — particularly those involving facial detection —

they need to take steps to understand what's being deployed. This includes conducting a privacy impact assessment and information risk assessment where appropriate and ensuring that any third-party providers are properly vetted.

Following the IPC's investigation, the university confirmed it has stopped using the vending machines, eliminating any ongoing risk to students and staff.

A wake-up call for physician privacy training

In PHIPA [Decision 260](#), a public hospital reported a privacy breach after one of its physicians accessed thousands of patient records without authorization. The hospital audited the physician's access and interviewed him directly. The physician, who had recently joined the hospital, told the hospital he believed he was allowed to review the records for educational purposes. While there was no evidence of targeted snooping or personal ties to the patients, the physician accessed the records of nearly 4,000 individuals who were not under his care.

The IPC investigation found that although the hospital had policies in place requiring privacy training and signed confidentiality agreements



for all staff, it wasn't enforcing these requirements for its physicians. Unlike other staff, physicians weren't receiving privacy training or re-signing confidentiality agreements each year, and their compliance wasn't being tracked. In addition, the hospital had no policy or guidance about using personal health information for education purposes, an oversight that contributed directly to this breach.

In the months that followed, the hospital made significant improvements. It launched an electronic system to ensure that all staff — including physicians — receive annual privacy training and sign updated confidentiality agreements. It put systems in place to monitor compliance and follow up when training isn't completed. It also revised its policies to clarify that staff may not use personal health information for education purposes unless they have specific permission.

This case highlights the importance of not just writing privacy policies but implementing them, tracking compliance, and making sure everyone — physicians included — comply with the rules and understand what is and isn't allowed when it comes to accessing patient information.

Out of sight is not out of mind: Ensuring secure disposal of health records

In PHIPA Decision 266, the IPC investigated a complaint about a health clinic that failed to securely dispose of paper records containing personal health information (PHI). Patient records were found discarded in an unsecured recycling bin. Although many documents were shredded or torn by hand, IPC investigators were able to recover sensitive details, including names, birthdates, and medical history.

The clinic admitted it had no formal privacy or disposal policies in place



and had relied on informal, verbal instructions. The investigation found the clinic was not in compliance with its legal obligations under PHIPA, including the duty to take reasonable steps to protect PHI and to securely dispose of it.

To address these issues, the clinic implemented new privacy and records policies, updated its employee handbook with PHIPA resources, and introduced mandatory staff training with written attestations, on the basis of which the case was resolved.

For health information custodians looking to get rid of old patient files at the end of their applicable retention

period, this case provides key insights. It highlights the importance of having clear, written policies on how personal health information must be securely disposed of and regularly training staff on their privacy-related responsibilities. Paper records must be properly shredded using a cross-shred or micro-cut shredder (and not just hand torn) to prevent reconstruction. If disposal is handled by a third party, there should be a formal agreement outlining how records will be securely destroyed. Further, organizations must be prepared to notify individuals promptly when their information is lost, stolen, or improperly disclosed. ●

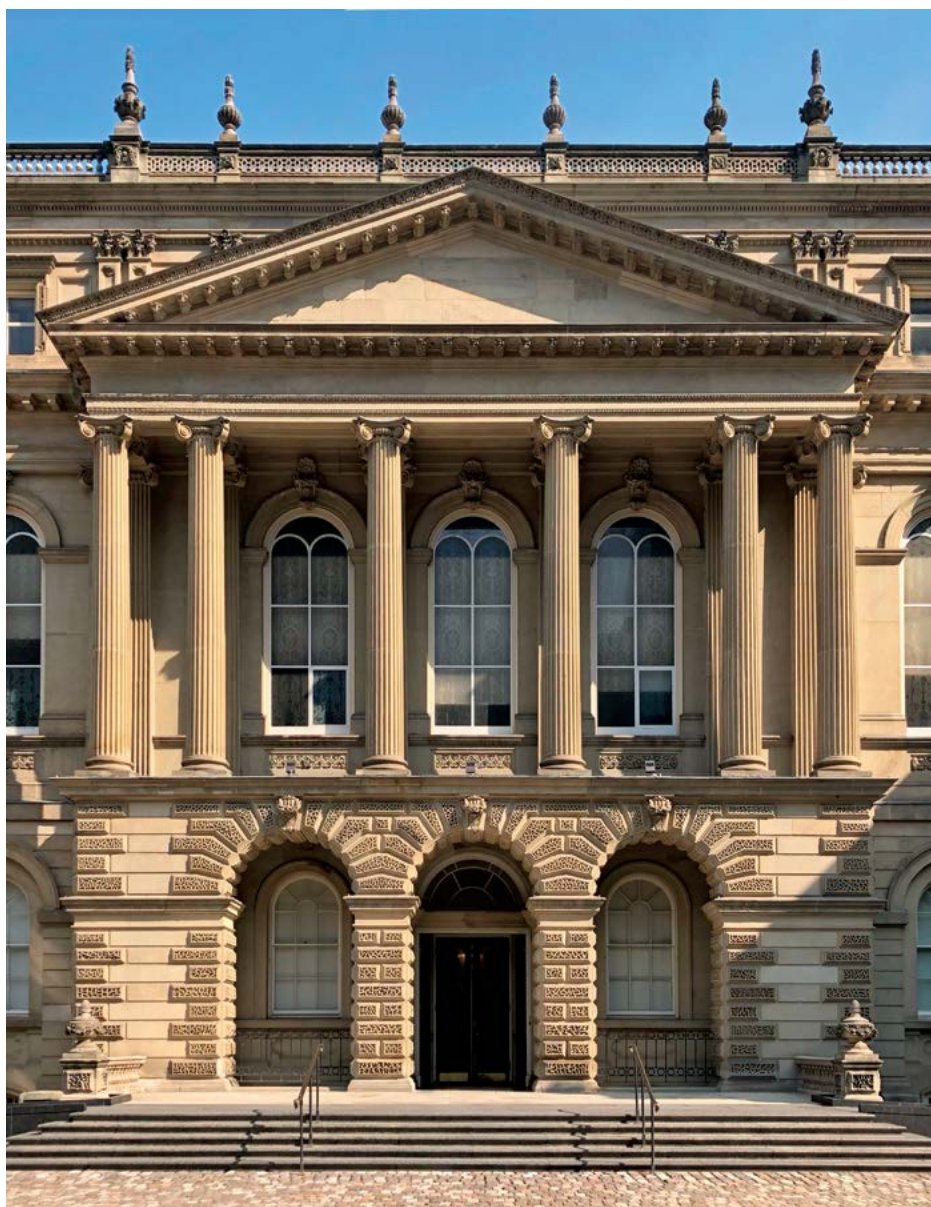
“

TIME AND AGAIN, WE SEE THAT GOOD INFORMATION GOVERNANCE MEANS NOT ONLY HAVING PRIVACY POLICIES IN PLACE, BUT ALSO TRAINING STAFF ON HOW TO IMPLEMENT THEM IN PRACTICE AND THEN DOING THE NECESSARY FOLLOW UP TO MAKE SURE THE TRAINING IS UP TO DATE AND PROVIDED ON A REGULAR BASIS.”

IPC in the Courts



Judicial reviews and rulings in 2024



Protecting the integrity of Ontario's FOI System

This year, the issue of individuals submitting multiple appeals or complaints to our tribunal led to important developments in our processes, including the adoption of a [File Processing Limitation Policy](#). A 2024 Ontario Divisional Court [ruling](#) dismissed an application for judicial review brought by an appellant who challenged the IPC's decision to limit the number of files they could actively pursue at one time. The court found that the IPC's file processing limits amount to administrative directions that allow the IPC to control its own process and manage its limited resources effectively.

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 PHIPA 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.

In April 2024, the Ontario Divisional Court heard and [dismissed](#) LifeLabs' challenge. The Divisional Court upheld the IPC and OIPC's procedural decision finding, among other things, that health information custodians cannot

defeat their responsibilities under PHIPA by placing facts about privacy breaches in privileged documents. The Divisional Court also found that the IPC and OIPC had authority to conduct a joint investigation and to issue joint decisions related to their joint investigation. The Ontario Court of Appeal's dismissal of LifeLabs' motion for leave to appeal in November 2024 concluded this lengthy legal process, allowing the IPC and OIPC to finally publish their joint investigation [report](#).

Liquor Control Board of Ontario **PO-4302**

The Ontario Court of Appeal unanimously [upheld](#) an IPC decision ordering the release of statistical records related to thefts from LCBO stores. The court restored the IPC's decision which it found it to be reasonable in all respects.

This outcome followed a legal challenge by the Liquor Control Board of Ontario (the LCBO) of an IPC decision finding statistical records of thefts from individual LCBO stores in Toronto and statistics for 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 Ontario Divisional Court [overturned](#) the IPC decision, holding 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 IPC's statutory duty not to reveal the LCBO's confidential submissions in its decision. The Ontario Court of Appeal granted the IPC leave to appeal from the majority judgment.

PO-4383 and PO-4404-R

The applicant sought judicial review of two IPC decisions concerning the adequacy of a records search conducted by Seneca College in response to a request for records related to a ridesharing service provided at the college. The applicant argued that the IPC adjudicator erred in accepting a single affidavit from the college's Privacy Officer rather than requiring affidavits from all staff involved in the search.

The Ontario Divisional Court [upheld](#) the IPC's decision that found

the Privacy Officer's detailed affidavit provided sufficient evidence to demonstrate that the college conducted a reasonable search. The court also rejected claims of procedural unfairness, affirming that the IPC has discretion under its Code of Procedure to manage its inquiry processes. This decision reinforces the IPC's established approach to assessing institutional compliance with FOI obligations.

Canadian Home Healthcare Inc. **PO-4413 and PO-4443-R**

The third party applicant sought judicial review of an IPC decision ordering disclosure of records related to a hospital contract. The applicant challenged the IPC's handling of procedural issues and its application of section 17(1) of FIPPA, which exempts certain third-party information from disclosure.

The Ontario Divisional Court [dismissed](#) the judicial review application, affirming the IPC's processes and reasoning. On procedural fairness, the court found that the IPC did not have an obligation to inform the applicant of other possible arguments that the applicant could make. In any event, the IPC had advised the applicant that it could raise additional exemptions under FIPPA, and the applicant did not do so. The court declined the applicant's request to overturn established precedents on section 17(1), emphasizing that doing so would severely undermine transparency in government contracting, contrary to FIPPA's legislative intent.

MO-4447 and MO 4461-R

The applicant sought judicial review of two IPC decisions concerning access to records held by the integrity commissioner of the Toronto District

15

Judicial
Reviews

5

Legal
Hearings

2

Motions

School Board. The applicant argued that the IPC adjudicator erred in concluding that the board did not have custody or control over records held by its integrity commissioner.

The Ontario Divisional Court upheld the IPC's decisions, finding that the IPC's "detailed and thoughtful consideration of the evidence, the submissions, and the law" was reasonable. The IPC found the integrity commissioner's independence and impartiality, important values in the context of carrying out their functions, would be eroded if the board had the ability to assert control over their records. The court also rejected the applicant's argument that it was procedurally unfair for the IPC to decline to join two of his access to information appeals, affirming that

the IPC has considerable latitude to determine the course and conduct of its own proceedings.

CYFSA Decision 19/Halton Children's Aid Society

The Halton Children's Aid Society (CAS) seeks judicial review and appeal of CYFSA Decision 19, where the IPC found that the CAS had a duty to notify individuals of a ransomware attack. In that decision, the adjudicator determined that encryption of the CAS servers by a cyber-attacker amounted to an unauthorized use and loss of personal information under the CYFSA and ordered the CAS to provide indirect public notice. This obligation arose as part of the explicit duty to notify under the CYFSA, which, unlike other privacy

statutory regimes, is not subject to any minimum risk threshold. The CAS argued that the decision was incorrect, asserting that the ransomware attack did not involve the cyber-attacker viewing, handling, copying, or exfiltrating personal information. The CAS also maintained that the encryption only affected the containers housing the information, that the data was never permanently lost, and that accessible copies remained available. The Ontario Divisional Court heard the CAS' judicial review and appeal on May 1, 2025, and reserved its decision.

PHIPA Decision 253/Hospital for Sick Children

The Hospital for Sick Children (SickKids) seeks a judicial review of PHIPA Decision 253, where the IPC found that the hospital had a duty to notify individuals of a ransomware attack. The adjudicator determined that encryption of the hospital servers by a cyber-attacker amounted to an unauthorized use and loss of personal health information under PHIPA, but did not issue an order requiring additional notification as it would serve no useful purpose. Like the CYFSA, the duty to notify individuals of a breach under PHIPA is not subject to any minimum risk threshold.

SickKids argued that the decision was unreasonable, asserting that the ransomware attack did not involve the cyber-attacker viewing, handling, copying, or exfiltrating personal health information. The hospital also asserted that the encryption only affected the containers housing the information, that the data was never permanently lost, and that accessible copies remained available. Additionally, SickKids claims the decision improperly conflates the definitions of use and loss. The Ontario Divisional Court heard Sick Kids' judicial review on May 1, 2025, and reserved its decision. ●



FOI, Privacy and Performance in 2024



What the numbers reveal about the state of freedom of information and privacy protection in Ontario.

Under Ontario's privacy laws, public institutions are required to provide annual compliance statistics to the IPC, which we collate into a yearly statistics report and use to provide insights into notable trends to the Ontario Legislative Assembly.

In 2024, Ontarians submitted 70,293 freedom of information requests, more than a 6 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 78 per cent of access requests were completed within 30 days, signifying a notable improvement compared to 2023, when just 67 per cent of requests were completed within 30 days.

Municipal institutions covered by MFIPPA completed 82 per cent of requests within 30 days, slightly higher than the previous year's rate of 80 per cent. This modest but steady improvement shows that many municipalities continue to prioritize timely access to information for their communities.



Ontarians submitted 117,595 requests for access to personal health information under PHIPA in 2024, up almost 12 per cent over the previous year. That nearly 98 per cent of requests were answered within 30 days speaks volumes about the commitment of health information custodians to upholding Ontarians' access rights, even amid a notable year-over-year increase in demand.

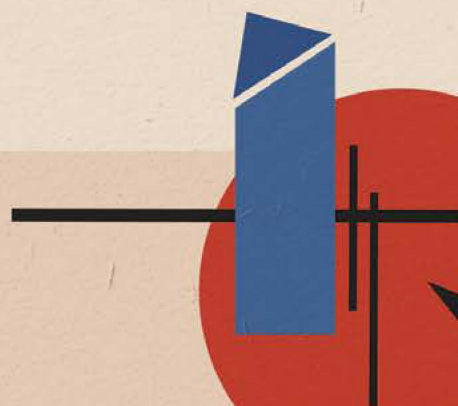
Under the CYFSA, child and family service providers received 11,169 access requests for personal information, up two per cent over the previous year. Service providers completed over 75 per cent of requests within 30 days in 2024, a slight improvement over almost 73 per cent in 2023.

In 2024, health information custodians reported 11,970 breaches of personal health information, compared to 10,770 in 2023, representing an increase of seven per cent across the sector. Misdirected faxes account for 5,047 of these. Despite repeatedly urging health information custodians to replace antiquated fax machines, misdirected faxes remain a persistent problem in the health care sector, representing almost 50 per cent of breaches. We look forward to seeing the fulfillment of [government's promise](#) to finally "axe the fax" by 2028.

Service providers subject to the CYFSA reported 437 breaches of personal information, compared to 374 in 2023. The leading cause of breaches in the child and family services sector was unauthorized disclosure, with the majority — 194 out of 351 — caused by misdirected emails.

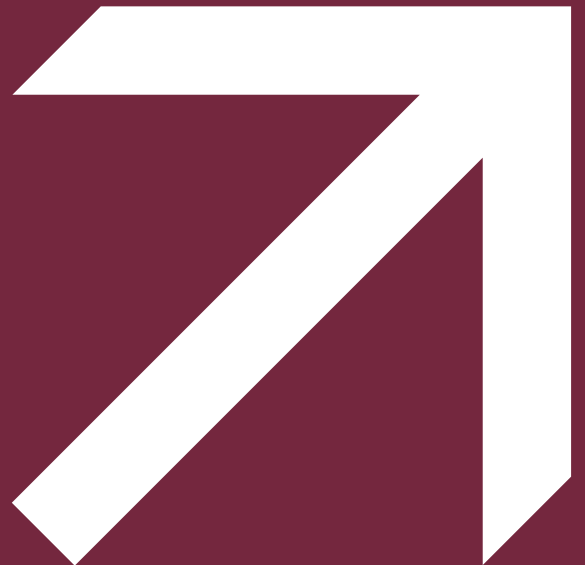
While Ontario's public sector institutions were not subject to mandatory requirements to report privacy breaches to the IPC during the last reporting period, that will soon change — in part. As of July 1, 2025, new FIPPA amendments under Bill 194 will introduce a mandatory breach reporting obligation for provincial institutions. Although MFIPPA institutions do not have a similar mandatory requirement, the IPC strongly encourages and expects MFIPPA institutions to continue the practice of reporting significant breaches to our office.

An overview of 2024 tribunal statistics can be located on page 56 of this report, while a full breakdown of all submitted statistics can be found in the IPC's 2024 Statistical Report. ●



Accountability

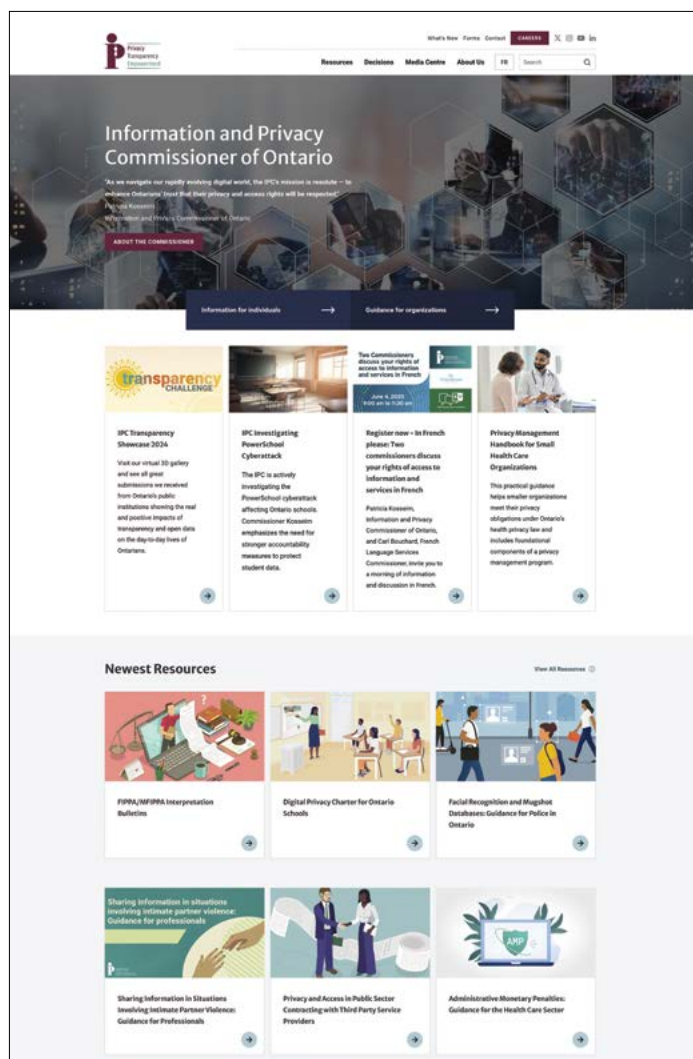
Maintaining Ontarians'
confidence in the organizational
excellence of the IPC



Original artwork by Aedán
Crooke of Surface Impression,
commissioned for the IPC's
[Transparency Showcase](#).

Modernization and Digitization

 In 2024, the IPC modernized its digital tools, systems, and services to work smarter, respond faster, and serve Ontarians more effectively.



In May 2024, the IPC launched its new and improved website, offering an enhanced, user-friendly experience designed to make accessing our information more straightforward than ever. The new site prioritizes speed, ease of use, and search functionality, featuring faster loading times and an intuitive design.

Throughout 2024, the IPC continued to modernize its operations to improve efficiency and enhance how it delivers services. As part of this effort, we've successfully moved to Microsoft 365 to help teams work more effectively, collaboratively, and securely.

We also introduced IRIS, our new intranet site, giving staff easier access to key resources, guidance, and tools. In parallel, we have begun a multi-year project to replace our internal case management system, to better support our day-to-day operations and casework. These modernization efforts, supported by an enterprise-wide staff training program, will enable the IPC to provide more responsive, transparent, and secure services.

Throughout 2024, we also stepped up our information security and cyber-resiliency. We made great strides in maturing our cloud computing incident prevention and detection capabilities to increase alignment with industry standards. We updated our incident response plan and conducted a table-top exercise to test it out in practice and improve our emergency readiness. ●

“

AS TECHNOLOGY EVOLVES, PRIVACY OVERSIGHT MUST BE JUST AS FLEXIBLE AND DYNAMIC. DIGITAL INNOVATION MUST BE MET WITH REGULATORY INNOVATION.”

Employer of Choice



Through continuous learning, collaboration, and staff engagement, the IPC is cultivating a workplace culture focused on inclusion and impact.



Recognizing excellence

The IPC's employee recognition program celebrates outstanding contributions, teamwork, and dedication to our mission. At the heart of the program are the IPC's Annual Exemplary Awards, which recognize individuals and teams, nominated by their peers, who embody the organization's core values of respect, integrity, fairness, collaboration, and excellence.

In addition to the Exemplary Awards, exceptional work is highlighted throughout the year through a variety of means, ensuring that employee achievements are acknowledged and celebrated in real-time, and in a way that is meaningful to IPC staff. This

includes regular recognition employee emails on behalf of the Commissioner and Senior Management Committee. By fostering a culture of appreciation, the program encourages and reinforces the IPC's commitment to excellence in service and leadership.

Adding "innovation" to our taxonomy

At the IPC, we recognize the value of innovation in helping us respond to new challenges and opportunities so we can put our strategic plan into action. Whether it's finding more efficient ways to serve the public, using technology to support our mandate, or rethinking how we engage with stakeholders, innovation plays an increasingly important role in how we operate. By staying curious, open to change, and willing to try new approaches, we're better equipped to make a meaningful impact in a world that doesn't stand still.

As part of this renewed focus, we launched the IPC Innovation Champions, a cross-functional group of staff and management from across the organization, working together to promote innovation. Guided by a clear

purpose and objectives, the Innovation Champions act as an advisory group to senior leadership and colleagues across the IPC. Their role is to encourage new ways of working, surface and celebrate innovative practices, and offer practical advice on navigating emerging challenges through innovative approaches.

IPC champions and committees

Meanwhile, the IPC's other champions and committees continue their tireless efforts to make the IPC an even better place to work and to help us grow as responsible and engaged corporate citizens. These groups play an important role in shaping our workplace culture, building connections, and advancing shared values across the organization.

From the *Champions for Community Giving* who organize charitable campaigns, to the *Bilingual Champions* who support our commitment to providing high-quality services in both official languages, each team brings energy and purpose to their work. Our *Champions for Health and Wellness* promote mental and physical well-being, while the *Social Committee* creates opportunities for staff to connect and celebrate, and the *Learning Committee* fosters a culture of continuous learning and professional development.

The *Inclusion, Diversity, Equity and Accessibility (IDEA) Champions* lead important conversations and initiatives to make the IPC a more inclusive and equitable place to work. And through the *Green Committee*, staff help champion environmentally sustainable practices in our day-to-day operations.

Together, these committees and champions bring our values to life in practical, meaningful ways, helping to build a workplace that is supportive, dynamic, and aligned with the world we want to live in.

Shaping future leaders: The IPC summer student program

The IPC's enhanced summer student program provides university and college students with valuable hands-on experience in privacy, access to information, and public sector work. Over the course of four months, students gain real-world skills, mentorship, and leadership development while contributing fresh ideas and perspectives to IPC initiatives.

This year, we received a record-breaking 5,960 applications, reflecting the growing interest in privacy and access to information careers. Students work in various teams across the organization, gaining exposure to different aspects of our work. To enrich their experience, the program includes group orientations, leadership touchpoints, and a buddy program, which pairs students with IPC team members to foster mentorship and coaching opportunities. Lunch and learn sessions led by subject matter experts from across the organization

“

AT THE IPC, WE CREATE A CULTURE OF SUPPORT, RECOGNITION, AND LEARNING THAT EMPOWERS PEOPLE TO LEAD AND INNOVATE.”

give students insight into areas of the IPC's work beyond their specific focus.

Our summer student program not only equips students with practical skills but also aims to develop the next generation of access and privacy leaders, fostering a deep understanding of the critical role privacy and transparency play in the public sector.

Investing in continuous learning and growth

In 2024, the IPC continued to refine and expand its Strategic Training Program to further support staff development. All management completed workshops in strategic

change leadership and performance management. Organization-wide training was rolled out for all staff, focusing on important topics like cybersecurity, Indigenous cultural awareness, mental health first aid, data de-identification methods, clear writing/plain language, and communication skills training. Employees work with their managers to develop tailored learning objectives as part of their performance plans to not only help them excel in their current role but prepare them for future opportunities as well.

In addition, our HR team continually monitors training needs, provides tailored learning support to our various departments, and hosts orientation sessions for new staff and summer students. Learning at the IPC is not just encouraged — it's deeply embedded in our culture. And in the fast-moving data and digital environment in which we work, it has to be. The IPC's Strategic Training Program empowers employees to deepen their expertise, strengthen their skills to navigate challenges effectively, and contribute to the organization's mission with confidence.

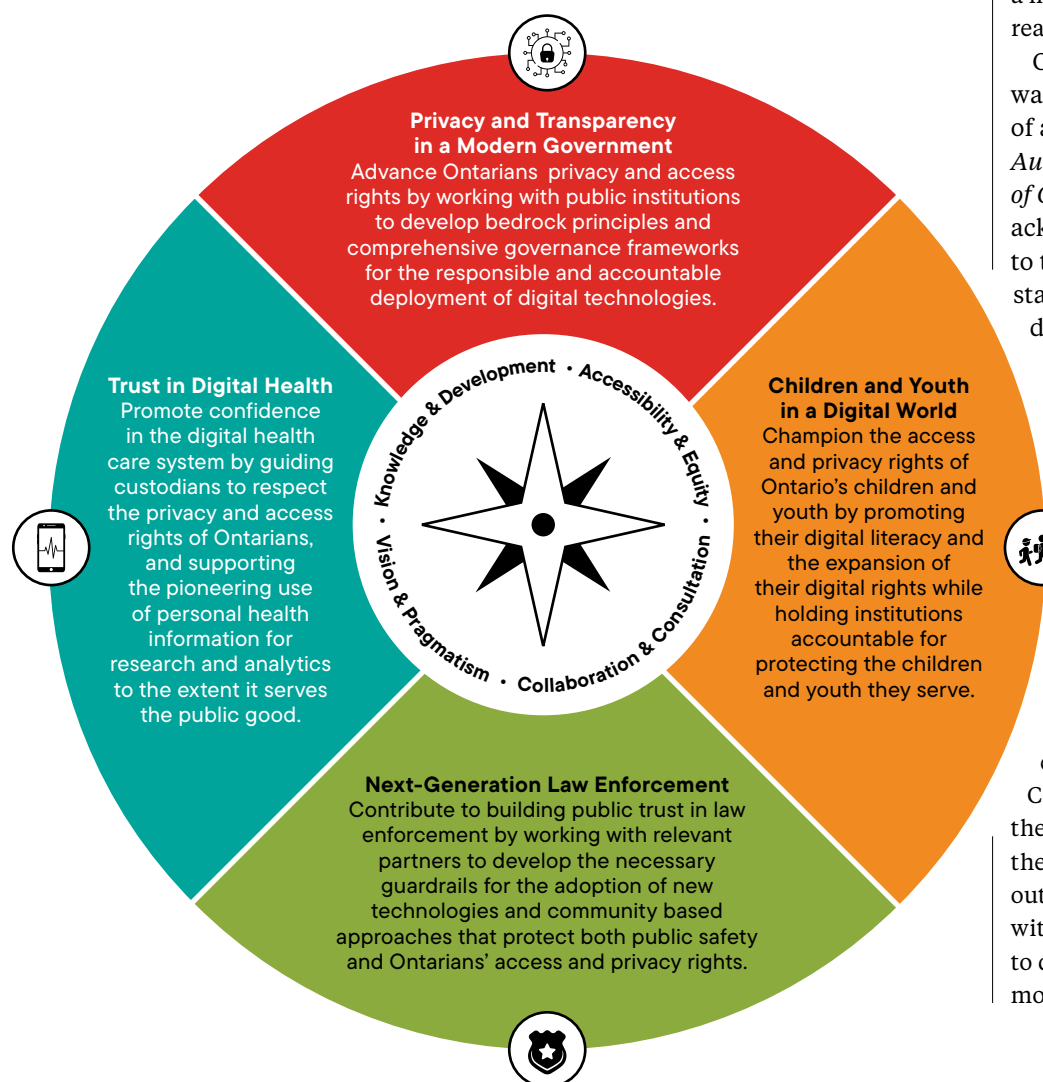
Welcoming IPC's second Scholar-in-Residence

This year, we had the privilege of welcoming our second scholar-in-residence, Dr. Khaled El Emam, an internationally recognized expert in deidentification, synthetic data, and other privacy-enhancing technologies. Having Dr. El Emam at the IPC for the year gave our Technology Research and Analysis team an exceptional opportunity to learn directly from one of the leading minds in the field. His insights helped shape our updated guidance and educational materials on deidentification, and his presence enriched the professional development of our staff in a way that few external learning opportunities could. ●



IPC summer students gain real-world experience supported by mentorship and hands-on learning.

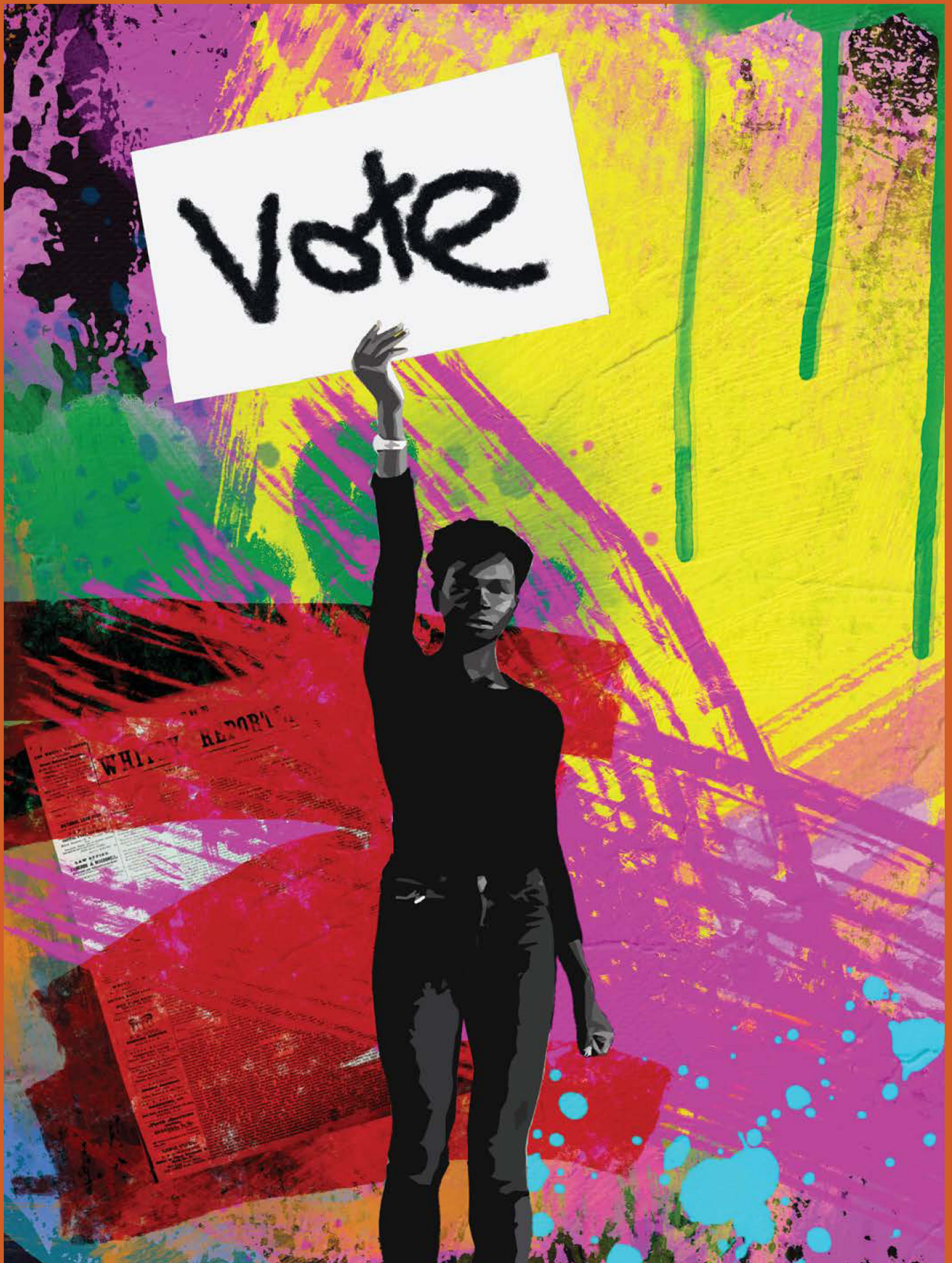
Strategic Priorities and Planning



In 2024, the IPC entered the final stretch of its 2021-25 Strategic Plan. To support successful implementation of the IPC's vision, mission and goals, the IPC continued to refine its Strategic Plan Framework. The framework outlines key activities for the year, expected outputs, desired outcomes and key performance indicators. The latter are particularly important to allow us to measure our progress against our goals, and ultimately, measure our real-world impact. The framework is designed to focus our resources in those areas that are of greatest strategic importance to Ontarians and has been instrumental in guiding our efforts towards becoming a modern and effective regulator with real world impact.

Our approach to strategic planning was recognized internationally as part of a global review, *Data Protection Authority Strategies: A Global Review of Current Practices*. This recognition acknowledges the IPC's commitment to transparency, consultation, and stakeholder engagement in setting the direction for our organization.

Building on the IPC's recognition among other global leaders in strategic planning, Commissioner Kosseim joined the Privacy Commissioner of Canada, Phillip Dufresne, along with other international data protection regulators in a closed session panel at the 2024 Global Privacy Assembly (GPA) focused on setting strategic priorities in an increasingly complex data protection environment. Commissioner Kosseim shared how the IPC's Strategic Plan has helped the IPC become more proactive and outcomes driven. By aligning priorities with clear objectives, the IPC continues to demonstrate global leadership in modern regulatory approaches. ●



Engagement and Outreach



Original artwork by Aedán
Crooke of Surface Impression,
commissioned for the IPC's
[Transparency Showcase](#).

Engagement and Outreach



Federal, provincial, and territorial information and privacy regulators gather in Toronto for their 2024 annual meeting.

Collaboration

The IPC collaborates with fellow regulators both domestically and globally, to speak with one voice on important issues and expand our public awareness initiatives. Throughout 2024, the IPC led, co-led, sponsored, and supported a select number of national and international resolutions and joint statements.

National

- › [Transparency by default – Information Regulators Call for a New](#)

[Standard in Government Service](#) (Federal Provincial and Territorial Information Commissioners and Ombuds, 2024, Toronto, Ontario)

- › [Identifying and mitigating harms from privacy-related deceptive design patterns](#) (Federal Provincial and Territorial Privacy Commissioners and Ombuds, 2024, Toronto, Ontario)
- › [Responsible information-sharing in situations involving intimate partner violence](#) (Federal Provincial and Territorial Privacy Commissioners and Ombuds, 2024, Toronto, Ontario)

International

- › [Transparency and digital age: the information commissioner's role and citizen empowerment](#), endorsed by the IPC at the 15th edition of the International Conference of Information Commissioners (ICIC), Tirana, Albania, June 2024
- › [Resolution on surveillance and protecting individuals' rights to privacy](#), adopted at the 2024 Global Privacy Assembly, Bailiwick of Jersey, October 2024

Stakeholder consultations and guidance

As part of our mandate to offer comments proposed legislative frameworks, programs, and information practices, organizations regularly [consult](#) the IPC on new initiatives with data privacy or access implications. For a list of informal consultations completed in 2024, visit our consultations [webpage](#).

IPC outreach efforts: Knowledge translation in action

The IPC regularly engages in public education efforts to raise awareness of and increase compliance with Ontario's access and privacy laws.

In 2024, the IPC developed several multi-media guidance materials and documents, delivered 88 [presentations](#) to various audiences (up from 57 last year), posted 10 blogs and released 11 Info Matters podcast episodes on access and privacy issues that matter most to Ontarians.

In 2024, the IPC responded to 97 requests by the media for comment and was mentioned in the media more than 1,100 times. Our social media engagement continued to climb. In 2024, we increased our LinkedIn followers by 11 per cent and our youth-focused Instagram account attracted a 30 per cent increase in followers. ●

Informing the Future of Access and Privacy in Ontario



Shaping the future of privacy: Research on emerging technologies

In 2024, the IPC launched a research and innovation hub, where we make publicly available for the benefit of others the results of independent research reports we commissioned on highly specialized

privacy and access topics. In 2024, the IPC commissioned or otherwise supported four reports by Canadian academics and researchers, as part of our efforts to contribute to broader discussions on emerging technologies and regulatory approaches that shape the future of privacy and access to information.

This work aligns with our commitment to fostering informed dialogue and evidence-based policymaking. The views expressed in these reports are those of the authors and do not necessarily reflect the views of the IPC.

Regulatory Sandboxes

Professor Teresa Scassa and Professor Elif Nur Kumru of the University of Ottawa explored the concept of a privacy regulatory sandbox. The report, *Exploring the Potential for a Privacy Regulatory Sandbox for Ontario*, funded by the Social Sciences and Humanities Research Council of Canada, examines how such an initiative could fit within the IPC's mandate.

Regulatory sandboxes provide a controlled environment where innovative products or services can be developed, tested, and validated under a regulator's supervision. The report outlines the potential for sandboxes to support innovation in areas such as artificial intelligence, while ensuring compliance with privacy laws. By consulting with experts and studying regulatory sandbox initiatives in jurisdictions like the UK, Norway, and France, the authors identified key elements and considerations for the potential creation of a privacy sandbox in Ontario. These findings highlight the role sandboxes could play in supporting innovation, enhancing regulatory expertise, and informing potential law reform.

Exploring neurotechnology: Balancing innovation with privacy

Verónica Arroyo of The Citizen Lab (Munk School of Global Affairs) conducted research on the rapid advancements in neurotechnology and its use in health care, law enforcement, and employment. Neurotechnology refers to techniques and devices that can monitor or manipulate brain activity,

often with the aim of gaining insights into an individual's thoughts, emotions, or cognitive states. While these innovations hold great promise, they can also raise serious privacy and human rights risks when they are used to access or alter deeply personal mental information. The research paper, *Emerging Uses of Neurotechnology*, assesses the possible uses of these technologies by public and private sector organizations, explores their current and future applications — including the ability to tap into sub-conscious thoughts — and outlines the legal and ethical considerations surrounding their use.

The age of surveillance: Exploring the risks of Unmanned Aerial Vehicles (UAVs)

In response to the growing adoption of Remotely Piloted Aircraft Systems (RPAS), or drones, by law enforcement, the IPC engaged Dr. Scott Thompson of the University of Saskatchewan to research *The Existing and Emergent State of UAV/RPAS/Drones Surveillance Capabilities and Law Enforcement*. As RPAS technology has advanced and become more affordable, it has seen increased use in law enforcement, emergency response, and public safety, offering significant benefits such as enhanced aerial surveillance, quicker response times, and cost efficiencies. However, as UAV capabilities evolve with more sophisticated capabilities, concerns about potentially new forms of surveillance or intrusion into personal privacy have intensified. This paper explored the emerging privacy challenges posed by UAVs, helping the IPC better assess how the technology is being used and could potentially be used in Ontario.

Employee privacy in the digital workplace

In recent years, the Ontario government made changes to the Employment

Standards Act (ESA) that targets employer use of electronic surveillance and artificial intelligence (AI) in hiring. However, these aspects are only the tip of a much bigger iceberg of employee monitoring software and employment practices enabled by AI. Dr. Adam Molnar of the University of Waterloo prepared a research report, *Surveillance and Algorithmic Management at Work: Capabilities, Trends, and Legal*

Implications, that outlined contemporary employee surveillance technologies, along with a jurisdictional scan of how various national and international employment laws govern the unique features and unprecedented challenges of employee privacy in the modern workplace. This paper provides insight into the current and emerging regulatory trends, models, and concepts across the world. ●



Original artwork by Aedán Crooke of Surface Impression. Artwork commissioned for the IPC's [Transparency Showcase](#).

SUBMISSIONS ON PROPOSED LAWS AND REGULATIONS

As part of its mandate, the IPC is called upon to provide comments and recommendations on the privacy and access implications of proposed laws and regulations. Throughout 2024, the IPC made the following submissions to government and various committees of the legislative assembly:

› FEBRUARY 12

Submission for Bill 149, the *Working for Workers Four Act*, recommending safeguards for the use of AI in the workplace and a private sector privacy law in Ontario.

› FEBRUARY 20

Comments on Schedule 4 of Bill 157, *Enhancing Access to Justice Act*, which would repeal the robust accountability and transparency measures that support ongoing public engagement and promotion of public confidence in policing and community safety regulations under the *Community Safety and Policing Act*.

› APRIL 12

IPC feedback on the Second Additional Protocol to the Convention on Cybercrime: Enhanced Cooperation and Disclosure of Electronic Evidence, that would allow foreign authorities to request electronic evidence from Ontario organizations, raising concerns about privacy rights and the need for stronger safeguards and oversight.

› MAY 17

Submission on Bill 188, the *Supporting Children's Futures Act*, recommending that any changes related to the collection, use and disclosure of personal information must be transparent and matched by a proportionate level of robust privacy protection.

› JUNE 25

Transparency recommendations for a regulatory proposal regarding publication of Inspector General of Policing reports under the *Community Safety and Policing Act*.

Submission concerning Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act*, which would enact the *Enhancing Digital Security and Trust Act*, 2024, setting out a framework for public sector rules on cybersecurity, artificial intelligence, and digital information of minors (Schedule 1) and introduce amendments to the privacy related provisions of the *Freedom of Information and Protection of Privacy Act* (Schedule 2).

› JULY 22

Comments responding to the proposal to enhance personal health information contributed to the provincial electronic health record (EHR).

› SEPTEMBER 9

Commissioner's letter to the Ministry of Health recommending greater transparency and improved patient access related to proposed regulatory amendments under the *Personal Health Information Protection Act* to establish a digital identity system at Ontario Health.

› SEPTEMBER 20

IPC submission on new job posting rules under the *Employment Standards Act*, recommending a clear, consistent definition of AI, full transparency about its use in hiring, and stronger privacy protections for workers in Ontario.

› NOVEMBER 14

Commissioner Kosseim addressed the Standing Committee on Justice Policy in its review of Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act* (see above).

› NOVEMBER 18

The IPC's submission on Schedule 2 of Bill 212, the *Reducing Gridlock, Saving You Time Act*, that called for excluding certain information about controversial highway projects from FOI disclosure.

› DECEMBER 13

IPC submission on Schedule 6 of Bill 231, *More Convenient Care Act*, raising concerns about proposed changes to PHIPA that would potentially limit Ontarians access to their own health records and introduce a broad digital health identity tool that could put their privacy at risk.

“

SCHEDULE 2 OF THE REDUCING GRIDLOCK, SAVING YOU TIME ACT NOW BLOCKS ACCESS TO INFORMATION ABOUT PRIORITY HIGHWAY PROJECTS BY AUTOMATICALLY DEEMING RELATED RECORDS AS CONFIDENTIAL THIRD-PARTY INFORMATION UNDER FIPPA. IT OVERRIDES DECADES OF CASE LAW, BY DOING AWAY WITH THE OBLIGATION TO PROVE CONFIDENTIALITY AND REMOVING INDEPENDENT OVERSIGHT. EXPEDIENCY AT THE EXPENSE OF TRANSPARENCY DENIES ONTARIANS INSIGHT INTO MAJOR BUILDING PROJECTS OF SIGNIFICANT PUBLIC INTEREST.”

What's new in 2024



Guidance, Videos, Bulletins and Policies

Guidance issued in 2024

- › [Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services](#)
- › [Facial Recognition and Mugshot Databases: Guidance for Police in Ontario](#)
- › [Privacy and Access in Public Sector Contracting with Third Party Service Providers](#)
- › [Sharing Information in Situations Involving Intimate Partner Violence: Guidance for Professionals](#)
- › [Guardrails for Police Use of Investigative Genetic Genealogy in Ontario](#)
- › [A Privacy Management Handbook for Small Health Care Organizations](#)

Videos created in 2024

- › [IPC FYI: Sharing Health Data](#)
- › [IPC FYI: A guide to AMPs](#)
- › [IPC FYI: Understanding PHIPA](#)
- › [IPC FYI: Filing an appeal with the IPC: Intake](#)
- › [IPC FYI: Expedited process](#)
- › [IPC FYI: Mediation at the IPC](#)
- › [IPC FYI: Adjudication of appeals](#)
- › [Privacy Day 2024 Event: Artificial Intelligence in the Public Sector](#)
- › [FPT 2024 – Toronto: Part I](#)
- › [FPT 2024 – Toronto: Part II](#)
- › [FPT Toronto – The Debaters](#)



Manuals and Addenda updated in 2024

- › [Manual for the Review and Approval of Prescribed Persons and Prescribed Entities under the Personal Health Information Protection Act \(PHIPA\) \(the Manual\)](#)
- › [Child, Youth and Family Services Act Addendum to the Manual](#)
- › [Coroner's Act Addendum to the Manual](#)
- › [Manual for the Review and Approval of Prescribed Organizations](#)

Code of Procedure practice directions, and policies revised in 2024

- › [Code of Procedure for Appeals Under FIPPA and MFIPPA](#)
- › [Practice Direction #1 - Providing Records to the IPC During an Appeal](#)
- › [Practice Direction #2 - Participating in a Written FIPPA or MFIPPA Inquiry](#)
- › [Practice Direction #5 - Direction to Institutions When Making Representations](#)

- › [Practice Direction #6 - Affidavit and Other Evidence](#)
- › [Practice Direction #7 - Sharing of Representations](#)
- › [Practice Direction #13 - Expedited Processes](#)
- › [Abandoned Files policy](#)
- › [File Processing Limits policy](#)
- › [Voluminous Records policy](#)

Interpretation bulletins developed in 2024

- › [Cabinet Records](#)
- › [Danger to Safety or Health](#)
- › [Records Relating to an Ongoing Prosecution](#)
- › [Draft By-Law/Closed Meeting](#)
- › [Advice or Recommendations](#)
- › [Third party information](#)
- › [Economic and Other Related Interests](#)
- › [Solicitor-Client Privilege](#)
- › [Information Available to the Public](#)

For a full list of interpretation bulletins, visit our [website](#).

Presentations

In keeping with our focus on outreach, engagement, and collaboration, throughout 2024, the IPC actively participated in events and conferences



across a broad range of stakeholder groups. The commissioner, assistant commissioners, and legal, policy, and tribunal staff delivered 88 speeches and presentations. For a list of 2024 presentations, visit our [media centre](#).



From the Commissioner's desk: IPC blogs

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

› FEBRUARY 1

[Artificial Intelligence in the public sector: Building trust now and for the future](#)

› MARCH 7

[AI on campus: Balancing innovation and privacy in Ontario universities](#)

› MAY 2

[Embarking on my new journey as the IPC's Scholar-in-Residence](#) (guest blog by Khaled El Emam)

› JULY 31

[Everyone knows someone who knows someone impacted by IPV](#)

› AUGUST 21

[School's out for the summer — or is it?](#)

› SEPTEMBER 27

[An impromptu visit from Sidney B. Linden, Ontario's first Information and Privacy Commissioner](#)

› OCTOBER 17

[Ontario IPC hosts access and privacy authorities from across Canada](#)

› NOVEMBER 20

[Empowering young people in today's digital world](#)

› DECEMBER 2

[Bill 194: Ontario's missed opportunity to lead on AI](#)

› DECEMBER 19

[Upholding Ontarians' privacy and access rights in 2024: Not only the what, but the how](#)

The Info Matters podcast: Conversations that count

In its fourth season, the IPC's award-winning podcast, Info Matters, continued to explore access and privacy issues that affect Ontarians. Hosted by Commissioner Kosseim, in 2024 we welcomed a diverse range of guests to discuss topics including tweens' privacy concerns, navigating homelessness and privacy, why mediation matters, disclosing information in situations involving intimate partner violence, artificial intelligence in health care, and more.

› EPISODE 1

[In their own words: Students from Westboro Academy speak out about privacy](#)

› EPISODE 2

[At face value: Facial recognition technologies and privacy](#)

› EPISODE 3

[No government ID: Navigating homelessness, identity, and privacy](#)

› EPISODE 4

[Artificial intelligence in health care: Balancing innovation with privacy](#)

› EPISODE 5

[Addressing intimate partner violence: Information sharing, trust, and privacy](#)

› EPISODE 6

[Why mediation matters: Improving outcomes in FOI appeals](#)

› EPISODE 7

[The beauty and benefits of transparency: Ontario's public institutions rise to the challenge with innovative projects](#)

› EPISODE 8

[Indigenous led innovation: Aligning technology with community values](#)

› EPISODE 9

[Technology in the classroom: Digital education, privacy, and student well-being](#)

› EPISODE 10

[Lessons in health privacy: Key takeaways from 2024](#)

› EPISODE 11

[The best of season 4 ●](#)



IPC Outreach by the Numbers 2024

368,202
website visits

9,501
unique email subscribers




14,107
LinkedIn followers


419
Instagram followers


4,867
X followers

8,700
INFO emails



5,500
INFO calls


1,182
media mentions


97
media statements


12
policy submissions


49
policy consultations


88
presentations


1,819
guidance downloads

5,694
downloads

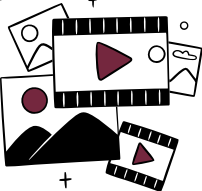
11
Info Matters podcasts



10
commissioner blogs

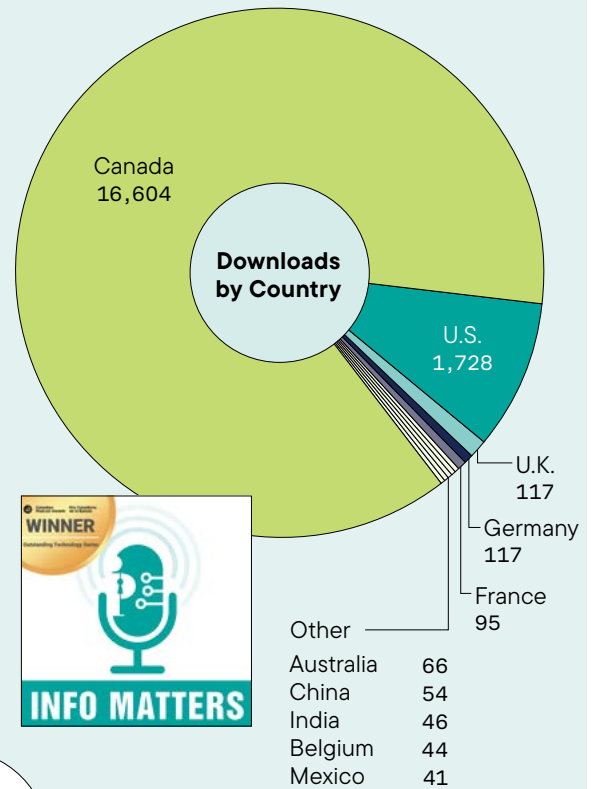
742
subscribers

40,392
YouTube views



Spotlight on Real-World Impacts 2024

As this annual report demonstrates, the IPC was certainly busy throughout 2024. However, the true measure of our success as a modern and effective regulator is how we convert this work into meaningful impacts for the benefit of Ontarians. Below is a selection of some of the positive impacts our office has had in 2024, and over time.



Close to
20,000
downloads
since launch

From January 2021 to
January 2025, more than

18,200

listeners have downloaded
our award-winning Info Matters
podcasts, and

6,300

attendees participated in
IPC Privacy Day events!



ADVOCACY



TRANSPARENCY SHOWCASE 2.0

featured in Municipal World,
the IAPP Digest, and The National
Observer



GLOBAL PRIVACY ASSEMBLY

IPC invited to showcase our
leading work in children's privacy at
the Global Privacy Assembly (GPA),
in the Bailiwick of Jersey, 2024

PRIVACY PURSUIT!

Lesson plans enter
digital textbooks in Ontario's
school system

SINCE 2023



75%

increase
in YouTube
views


24%

increase
in YouTube
subscribers


11%

increase
in LinkedIn
followers


30%

increase in
Instagram
followers


368,202

website visits



54%

increase in
presentations
delivered


15%

increase
in media
mentions


9%

increase in
public contacts
activity

ACCOUNTABILITY

5,968

applications for 29 job postings – an
average of 206 applicants per posting,
well above the OPS average


GLOBALLY RECOGNIZED

IPC is recognized globally as a model
for its strategic planning and priority
setting process in Data Protection
Authority Strategies report, 2024


TOP EMPLOYER

IPC shortlisted as one of Canada's
Top Employers for 2024

8%

IPC staff turnover
rate is just
8% in 2024, below
industry average
of 12%

RESPONSIVENESS



17%

increase in
incoming files,
since 2023 (all
time record high)


4%

more files closed
in 2024 over
2023 (all time
record high)

88%

of files
successfully closed
using informal
methods of dispute
resolution


8.5%

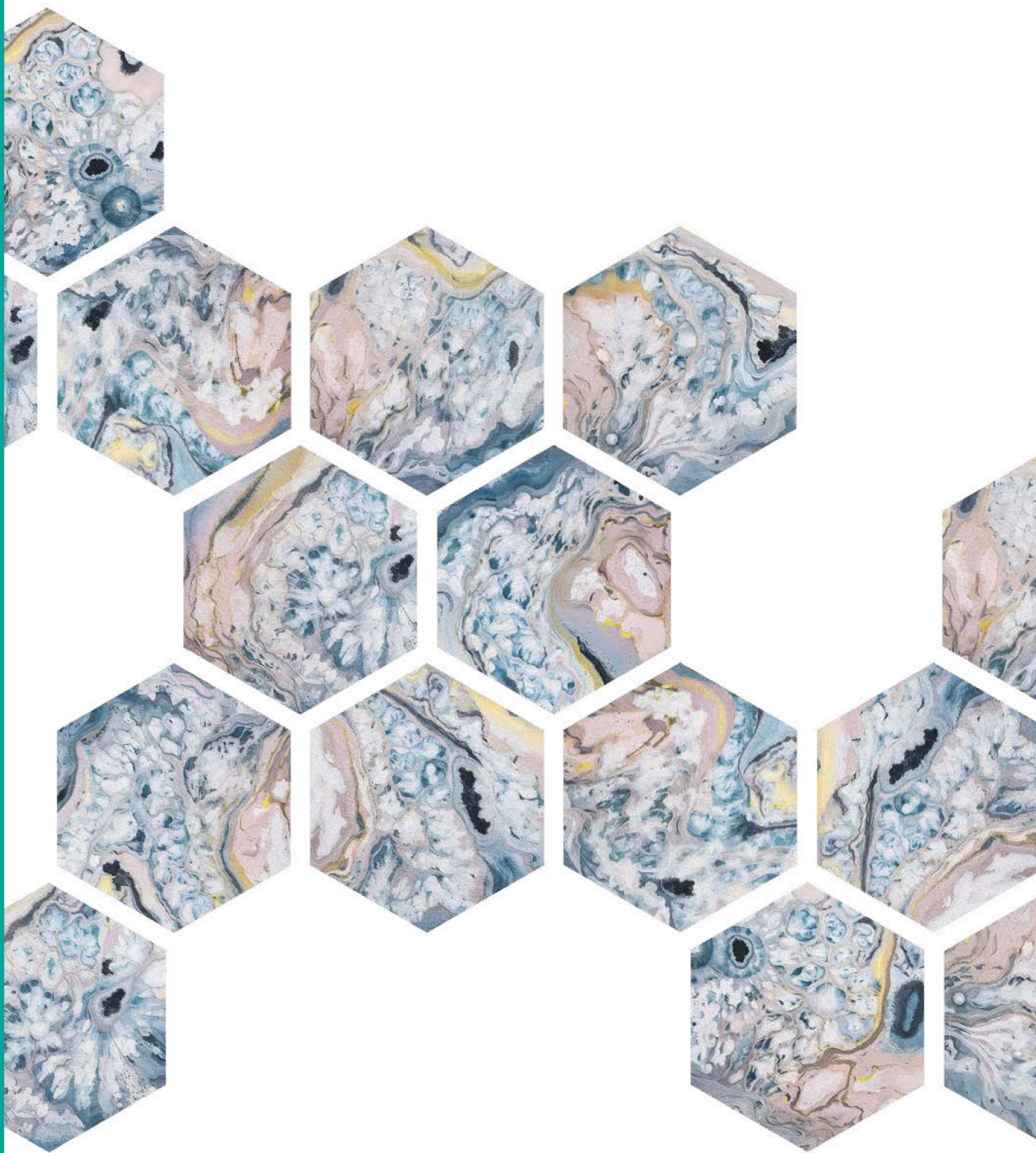
decrease in average
time to resolve
privacy complaints,
compared to 2023


7.5%

decrease in average
time to resolve
access appeals,
compared to 2023


17%

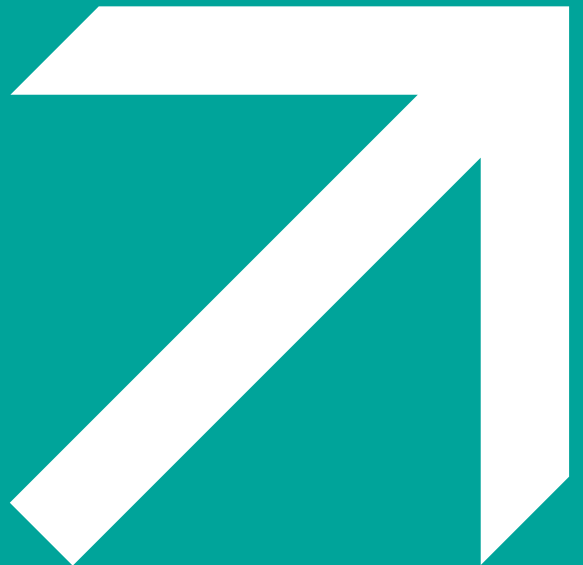
reduction in
case backlog
since 2023



Statistical Highlights



Original artwork by Aedán
Crooke of Surface Impression,
commissioned for the IPC's
[Transparency Showcase](#).



OVERALL OPENED FILES 2020-2024

15,027

Year	FIPPA	MFIPPA	PHIPA	CYFSA	TOTAL
2020	923	768	926	151	2,768
2021	736	1,029	993	165	2,923
2022	682	916	884	92	2,574
2023	844	1,121	1,047	137	3,149
2024	919	1,249	1,286	159	3,613

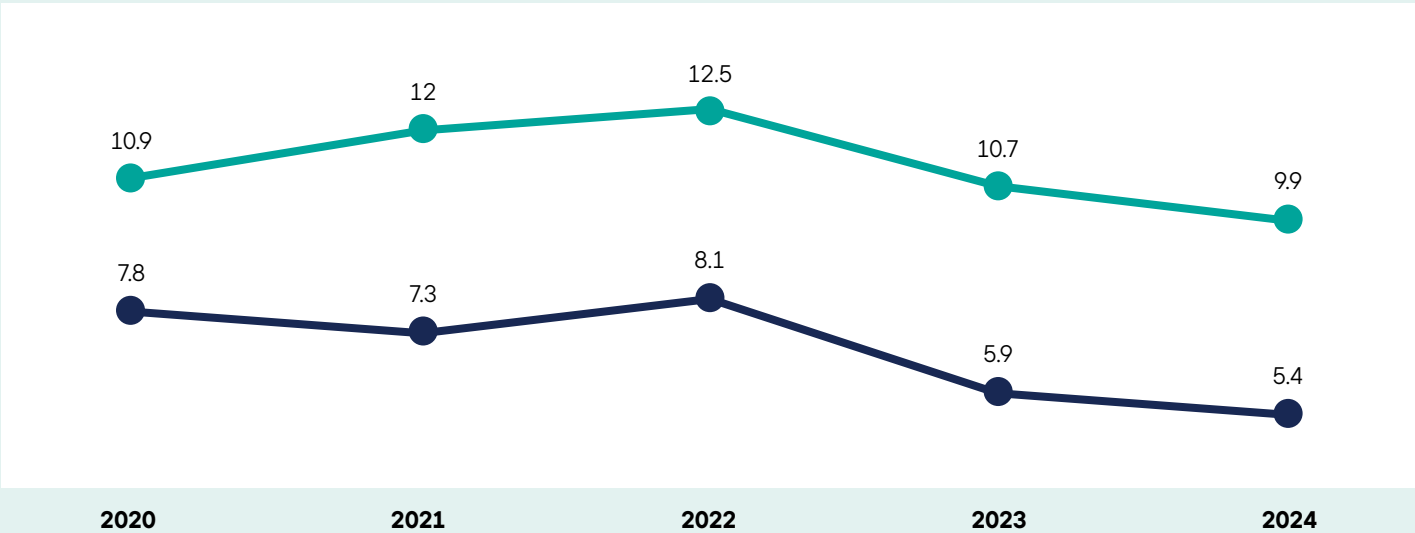
OVERALL CLOSED FILES 2020-2024

13,903

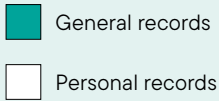
Year	FIPPA	MFIPPA	PHIPA	CYFSA	TOTAL
2020	771	569	624	55	2,019
2021	708	1,021	1,079	168	2,976
2022	731	1,066	965	95	2,857
2023	763	1,087	988	129	2,967
2024	779	1,048	1,135	122	3,084

AVERAGE DURATION (IN MONTHS) TO PROCESS AND CLOSE A FILE 2020-2024

Access Appeals Privacy Files

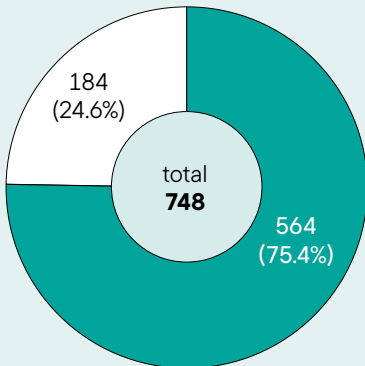


ACCESS APPEALS OPENED IN 2024, BY TYPE OF RECORD

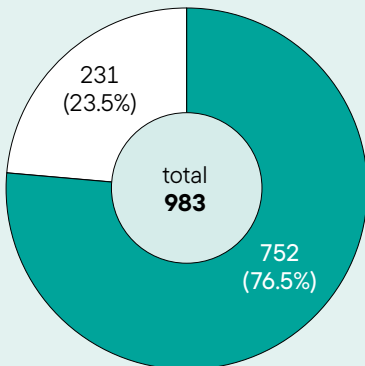


1,731

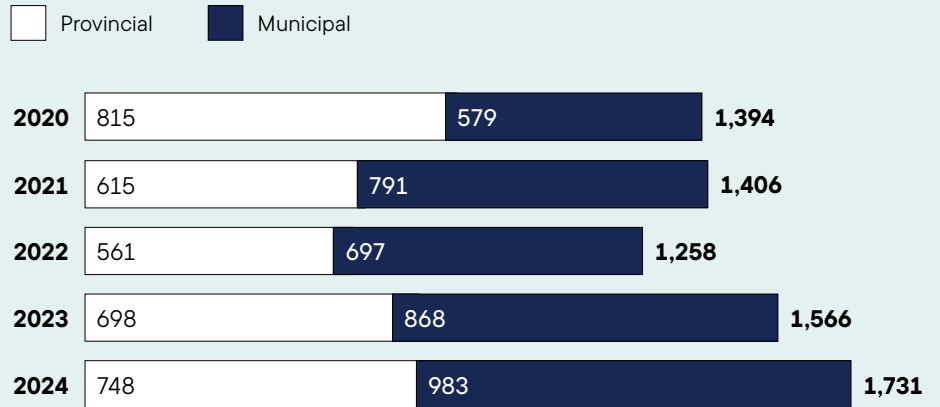
Provincial



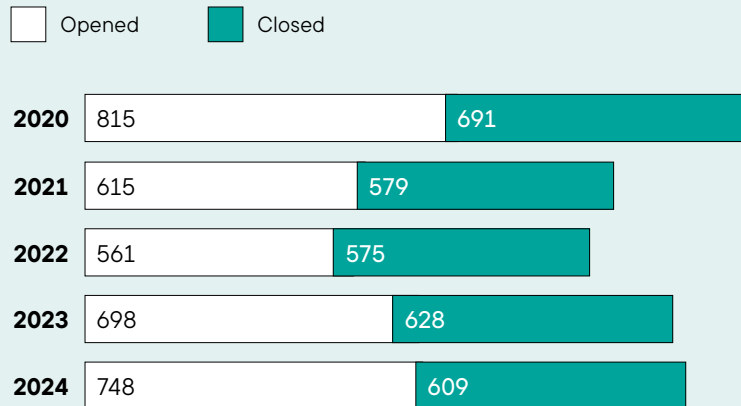
Municipal



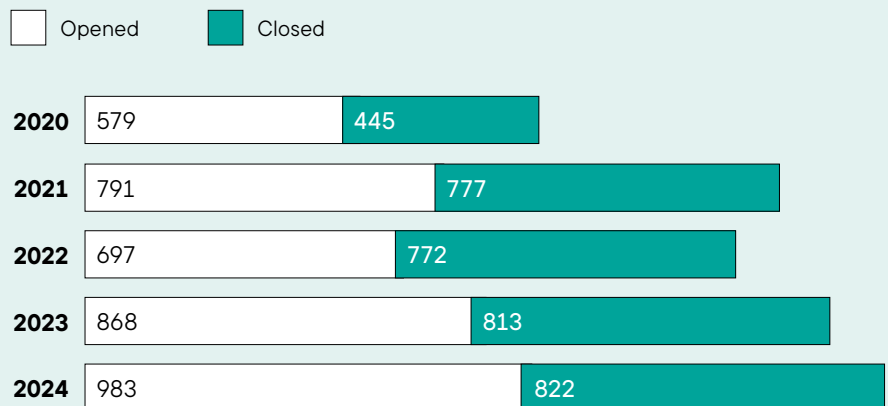
APPEALS OPENED BY JURISDICTION, 2020-2024



PROVINCIAL ACCESS APPEALS OPENED/CLOSED 2020 - 2024

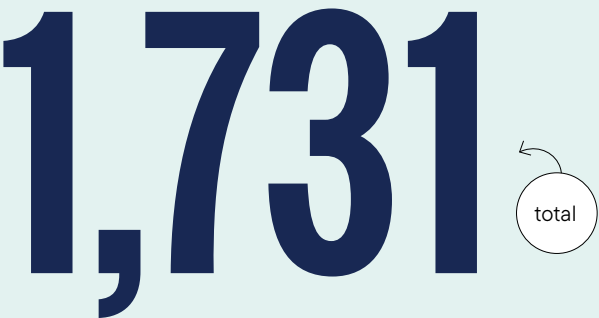


MUNICIPAL ACCESS APPEALS OPENED/CLOSED 2020 - 2024



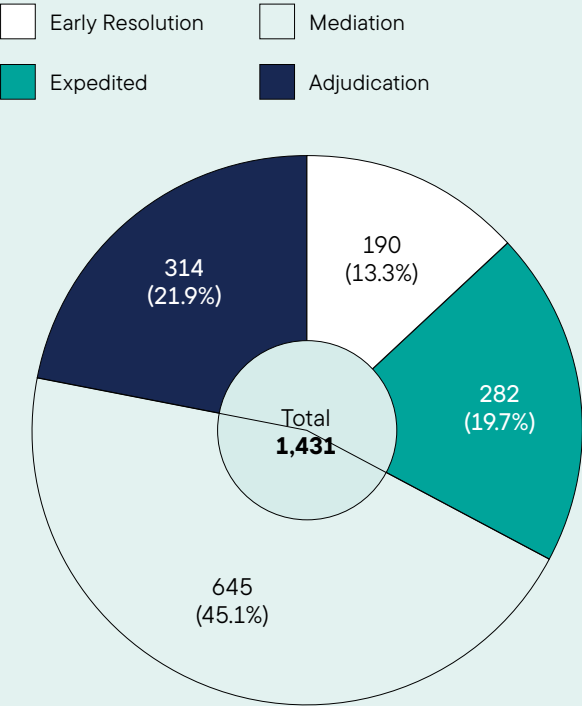
*Does not include files that were resolved, abandoned, withdrawn, or dismissed without an inquiry during adjudication

ISSUES IN ACCESS APPEALS OPENED IN 2024

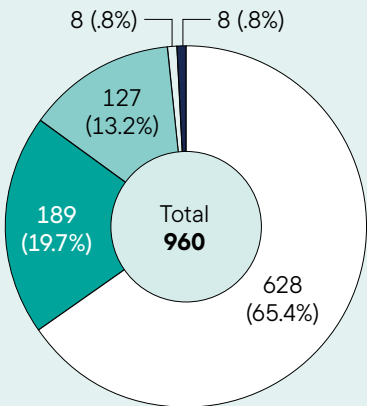
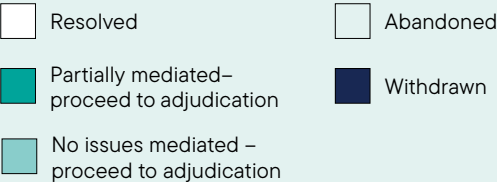


Issues	TOTAL
Exemptions	759
Deemed refusal	226
Reasonable search	183
Third party appeals	178
Act does not apply	156
Other	229

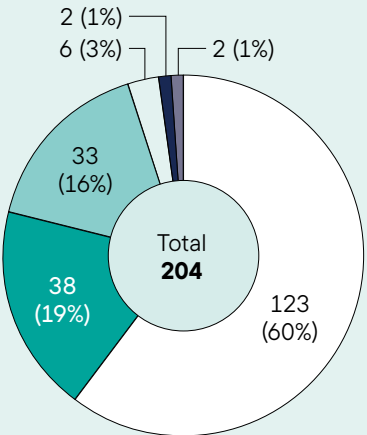
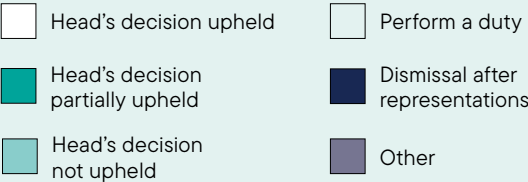
ACCESS APPEALS RESOLVED BY STAGE 2024



MEDIATED APPEALS, BY DISPOSITION 2024

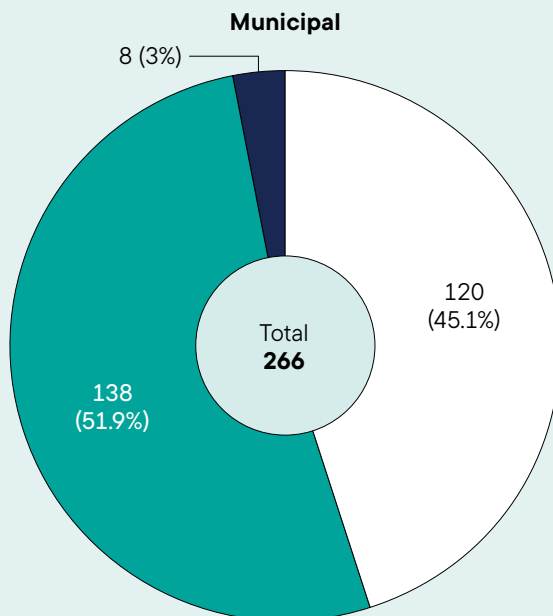
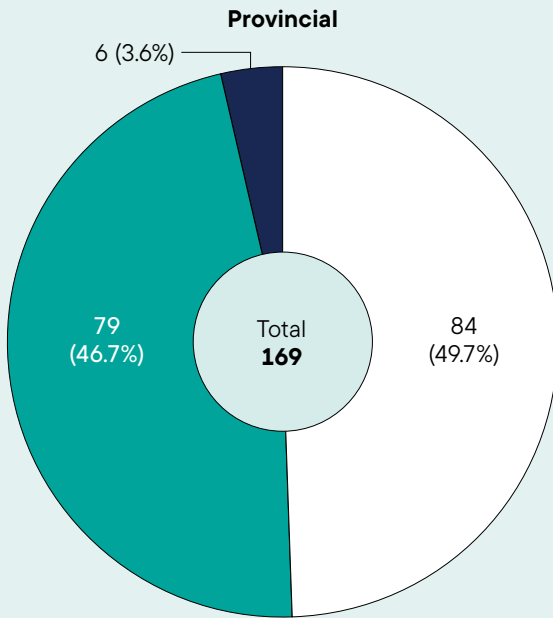
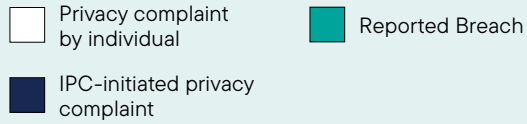


OUTCOME OF APPEALS CLOSED BY ORDER 2024*

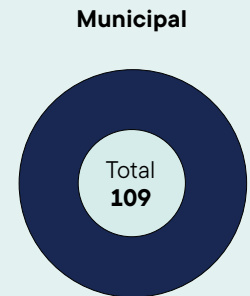
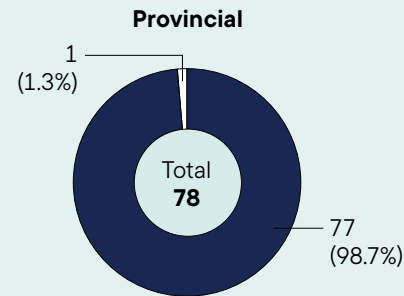
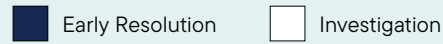


*Does not include files that were resolved, abandoned, withdrawn, or dismissed without an inquiry during adjudication

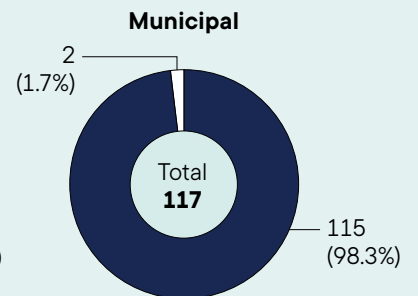
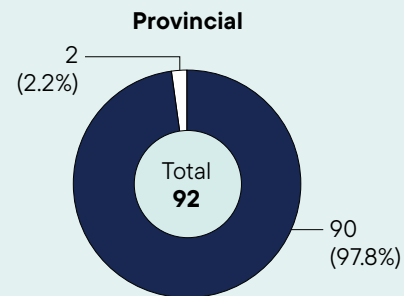
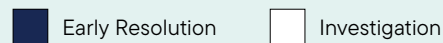
**PRIVACY COMPLAINTS, IPC-INITIATED
PRIVACY COMPLAINTS, AND SELF-REPORTED
BREACHES OPENED 2024**



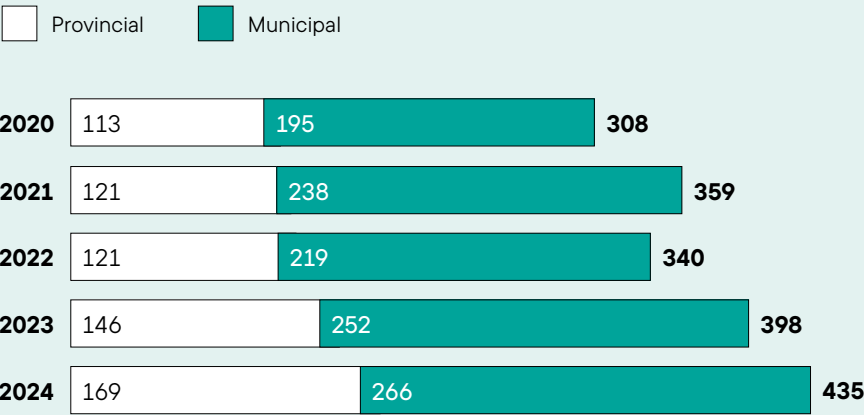
**PRIVACY COMPLAINTS RESOLVED AT EARLY RESOLUTION
AND INVESTIGATION**



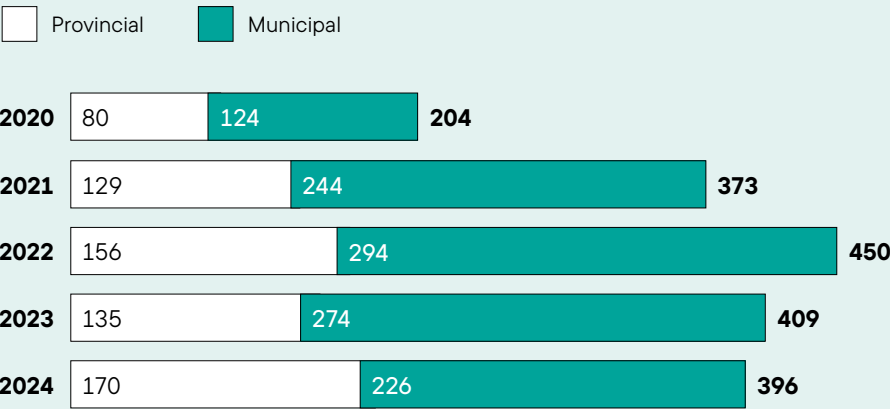
**SELF-REPORTED BREACHES AND IPC-INITIATED PRIVACY
COMPLAINTS RESOLVED AT EARLY RESOLUTION AND
INVESTIGATION**



TOTAL PRIVACY FILES OPENED (PROVINCIAL/MUNICIPAL) 2020-2024

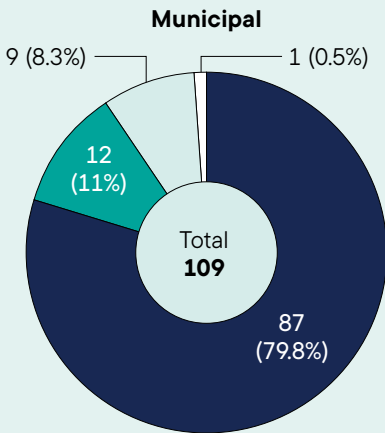
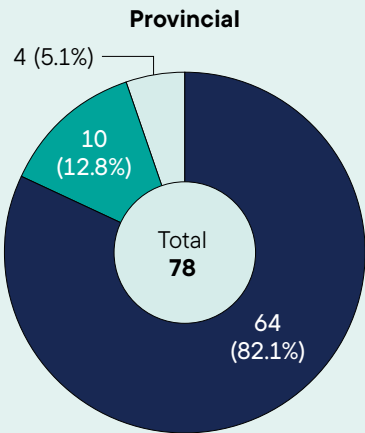


TOTAL PRIVACY FILES CLOSED (PROVINCIAL/MUNICIPAL) 2020-2024



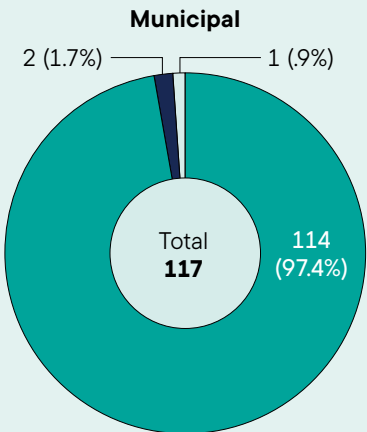
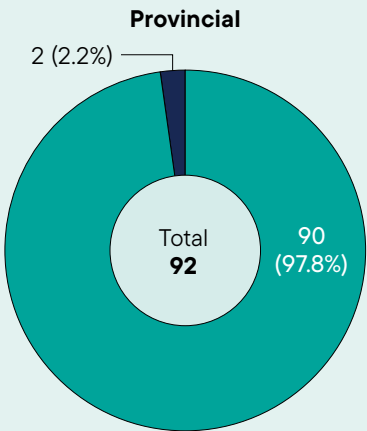
INDIVIDUAL PRIVACY COMPLAINTS CLOSED BY TYPE OF RESOLUTION 2024

Screened out Resolved Withdrawn Abandoned



SELF-REPORTED BREACHES AND IPC-INITIATED PRIVACY COMPLAINTS CLOSED BY TYPE OF RESOLUTION 2024

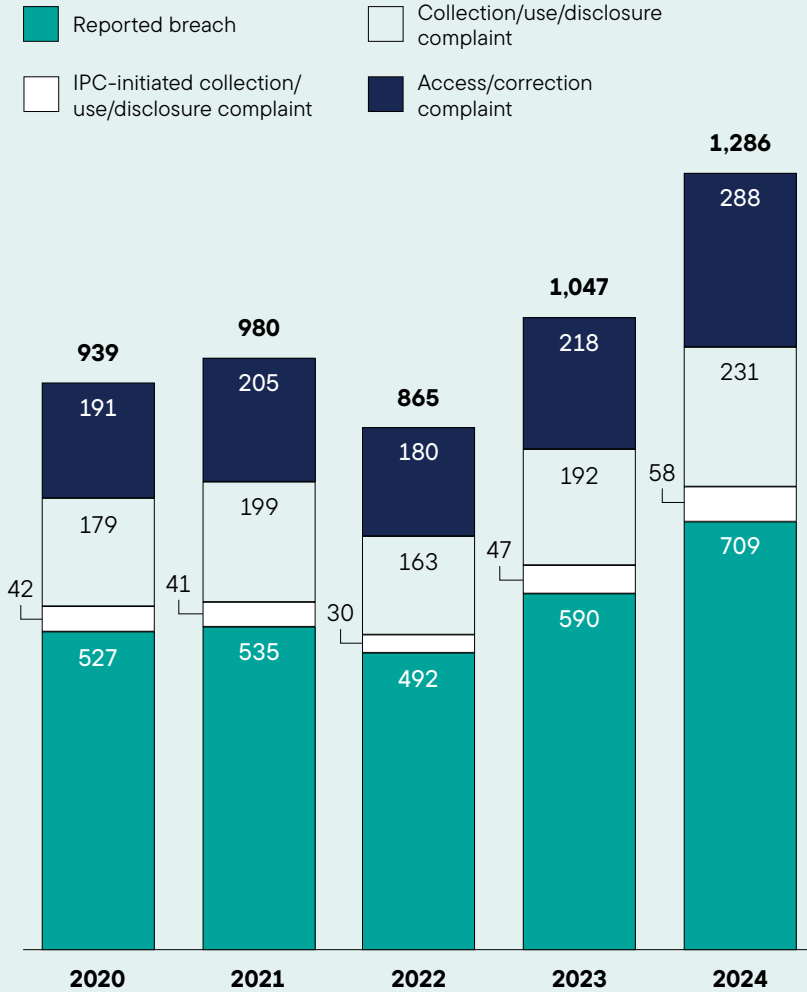
Resolved Investigation report Order/Decision Issued



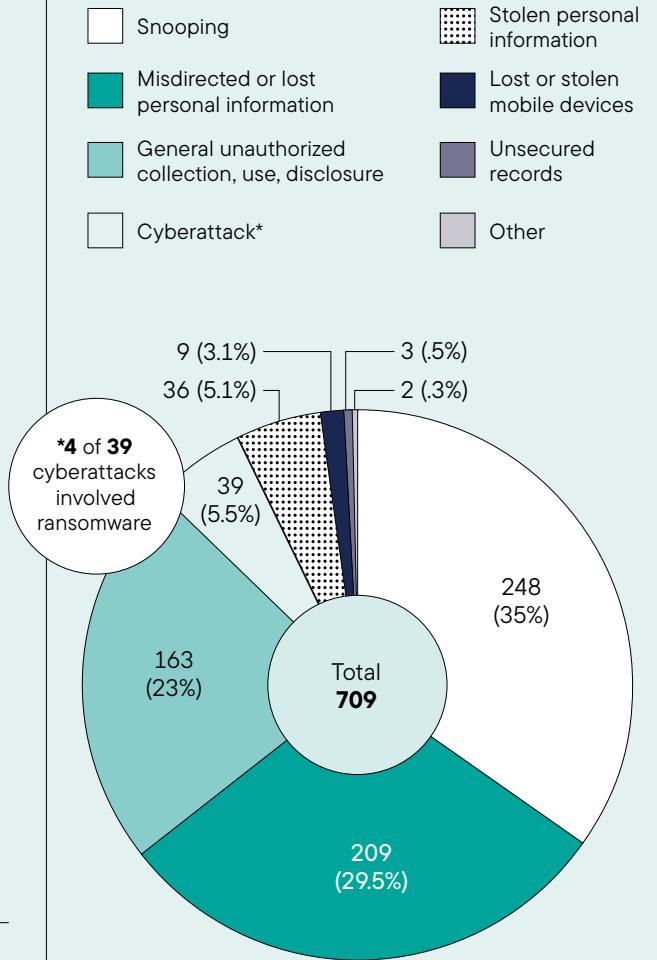
total

209

TYPES OF HEALTH FILES OPENED 2020 TO 2024



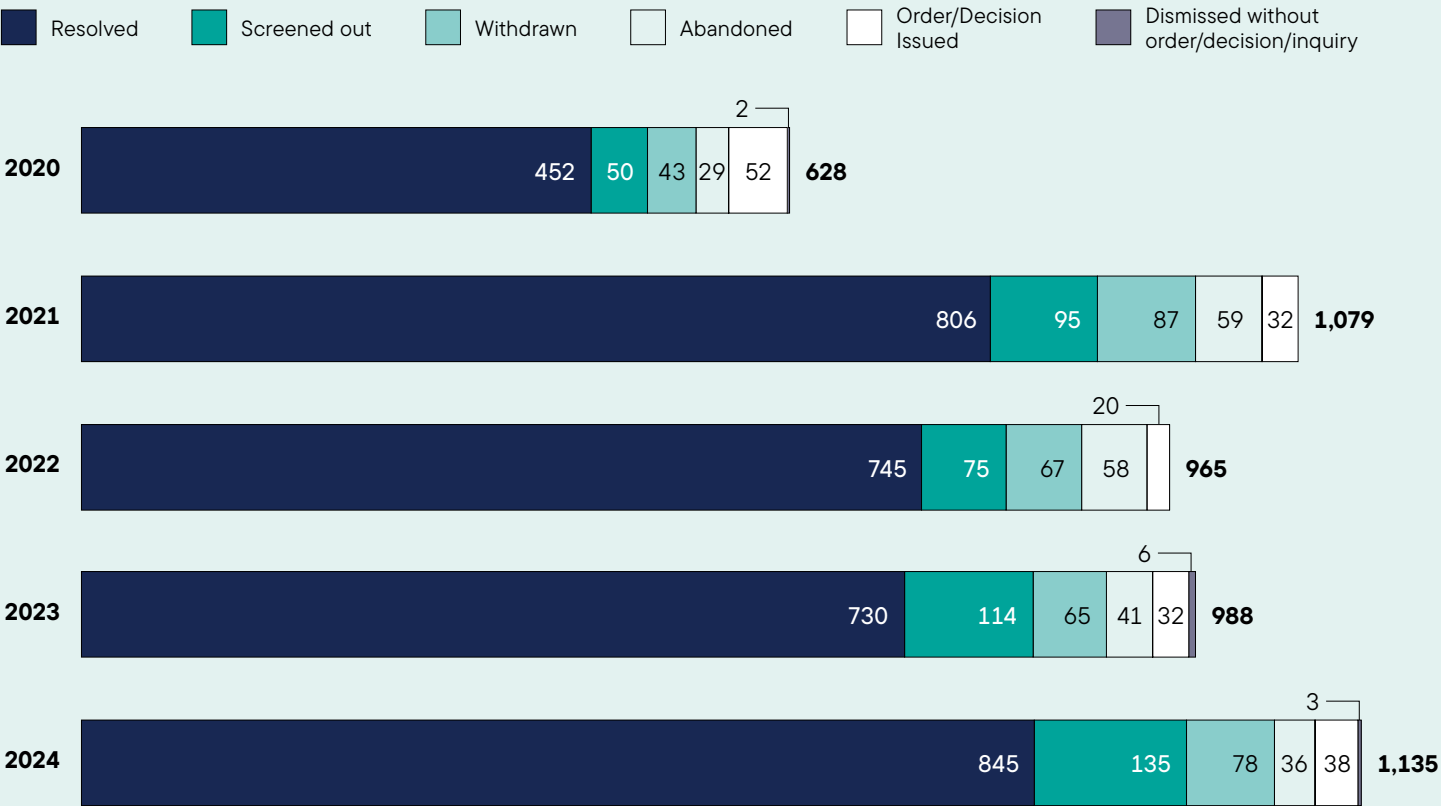
SELF-REPORTED HEALTH PRIVACY BREACHES OPENED BY CAUSE 2024



SELF-REPORTED HEALTH PRIVACY BREACHES CLOSED BY STAGE AND CAUSE 2024

	Early Resolution	Investigation	Adjudication	TOTAL
Snooping	223	2		225
Misdirected or Lost PI	192			192
General Unauthorized CUD	143		1	144
Stolen PI	33			33
Cyberattack*	21	1	2	24
Lost or Stolen Mobile Devices	8			8
Unsecured Records	4			4
Ransomware	4	1	1	6
Total	628	4	4	636

OUTCOME OF HEALTH FILES CLOSED 2020 - 2024

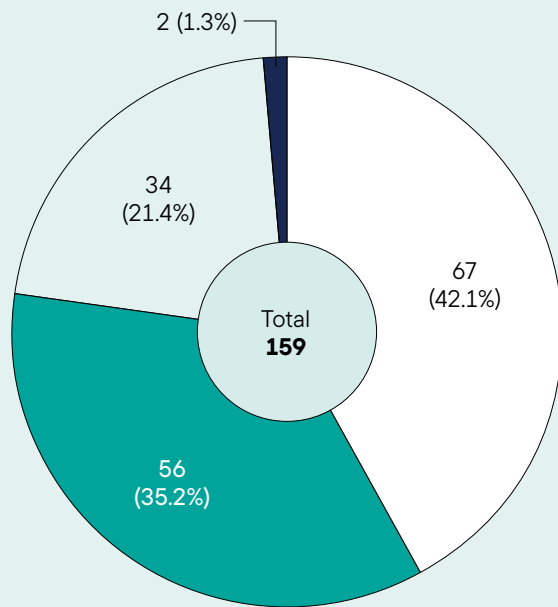
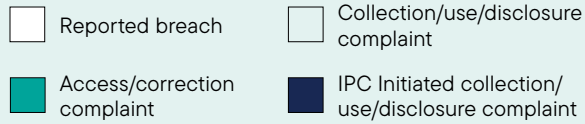


OUTCOME OF HEALTH FILES CLOSED
IN 2024, BY STAGE

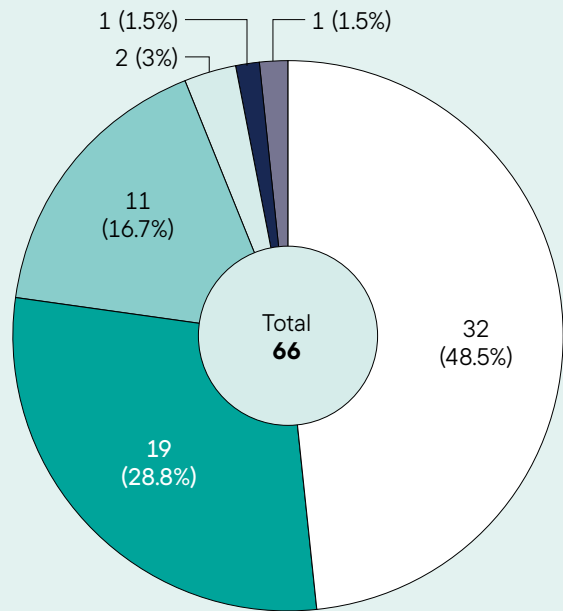
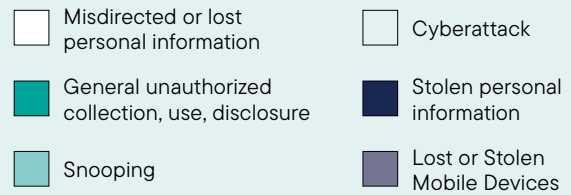


	Early Resolution	Expedited	Mediation	Investigation	Adjudication	TOTAL
Resolved	706	76	61		2	845
Screened out	124	11				135
Withdrawn	64		10		4	78
Order/Decision Issued	5		2	6	25	38
Abandoned	30	2	3		1	36
Dismissed without Order/ Decision/Inquiry					3	3
Total	929	90	76	6	34	1,135

CYFSA FILES OPENED BY ISSUE IN 2024



SELF-REPORTED CYFSA PRIVACY BREACHES BY CAUSE 2024

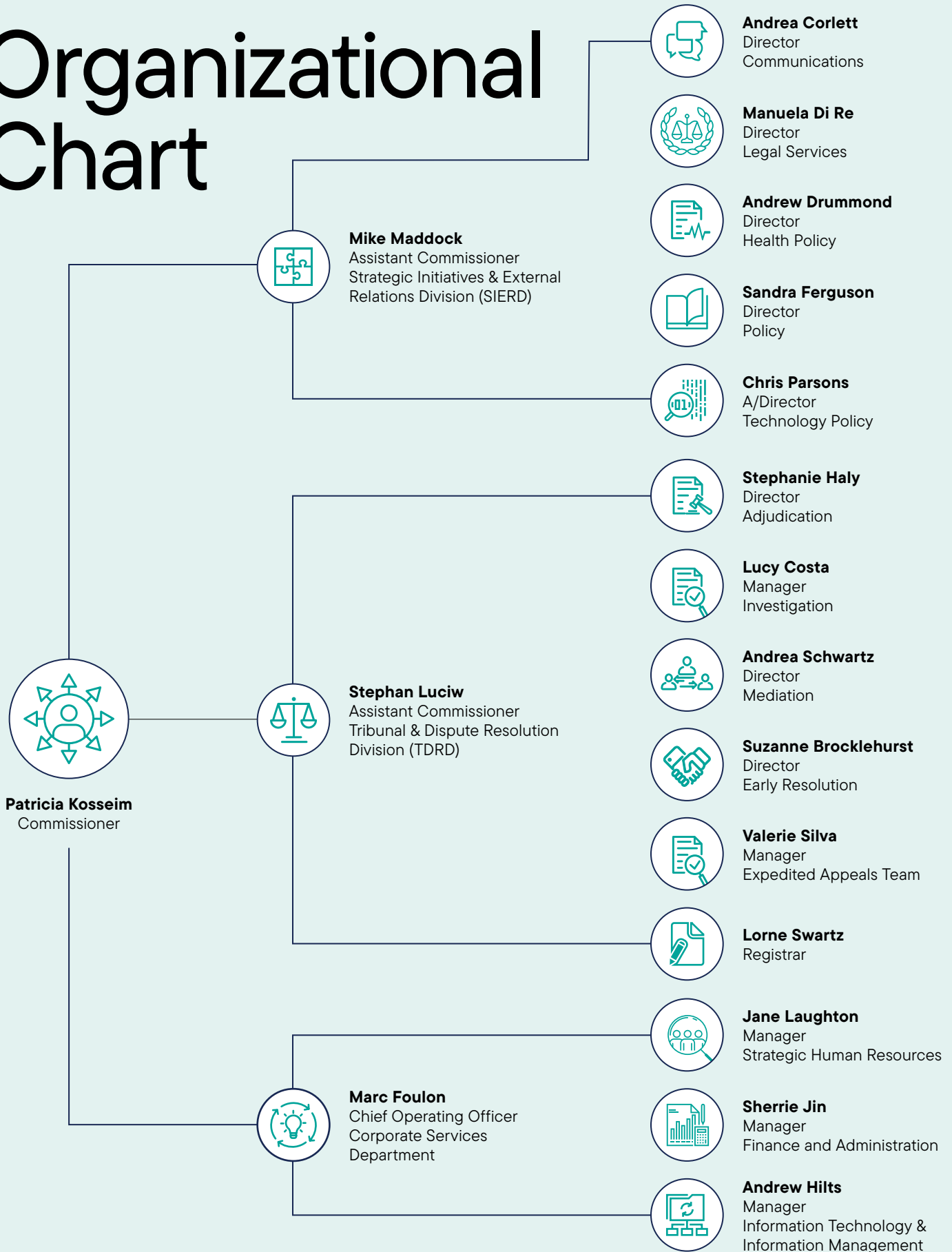


OUTCOME OF CYFSA FILES CLOSED IN 2024, BY STAGE

122

	Early Resolution	Expedited	Mediation	Adjudication	TOTAL
Resolved	59	6	17	1	83
Screened out	15	3			18
Withdrawn	11		2	1	14
Order/Decision Issued	1			4	5
Abandoned	2				2
Total	88	9	19	6	122

Organizational Chart



Financial Summary

	2024 2025 Estimate \$ (unaudited)	2023 2024 Estimate \$ (unaudited)	2023 2024 Actual \$ (unaudited)
Salaries and wages	21,132,000	17,586,000	17,626,270
Employee benefits	5,492,400	4,653,300	3,773,576
Transportation and communications	185,300	185,300	129,280
Services	4,242,800	4,612,100	5,307,625
Supplies and equipment	161,100	162,600	311,472
TOTAL	31,213,600	27,199,300	27,148,223

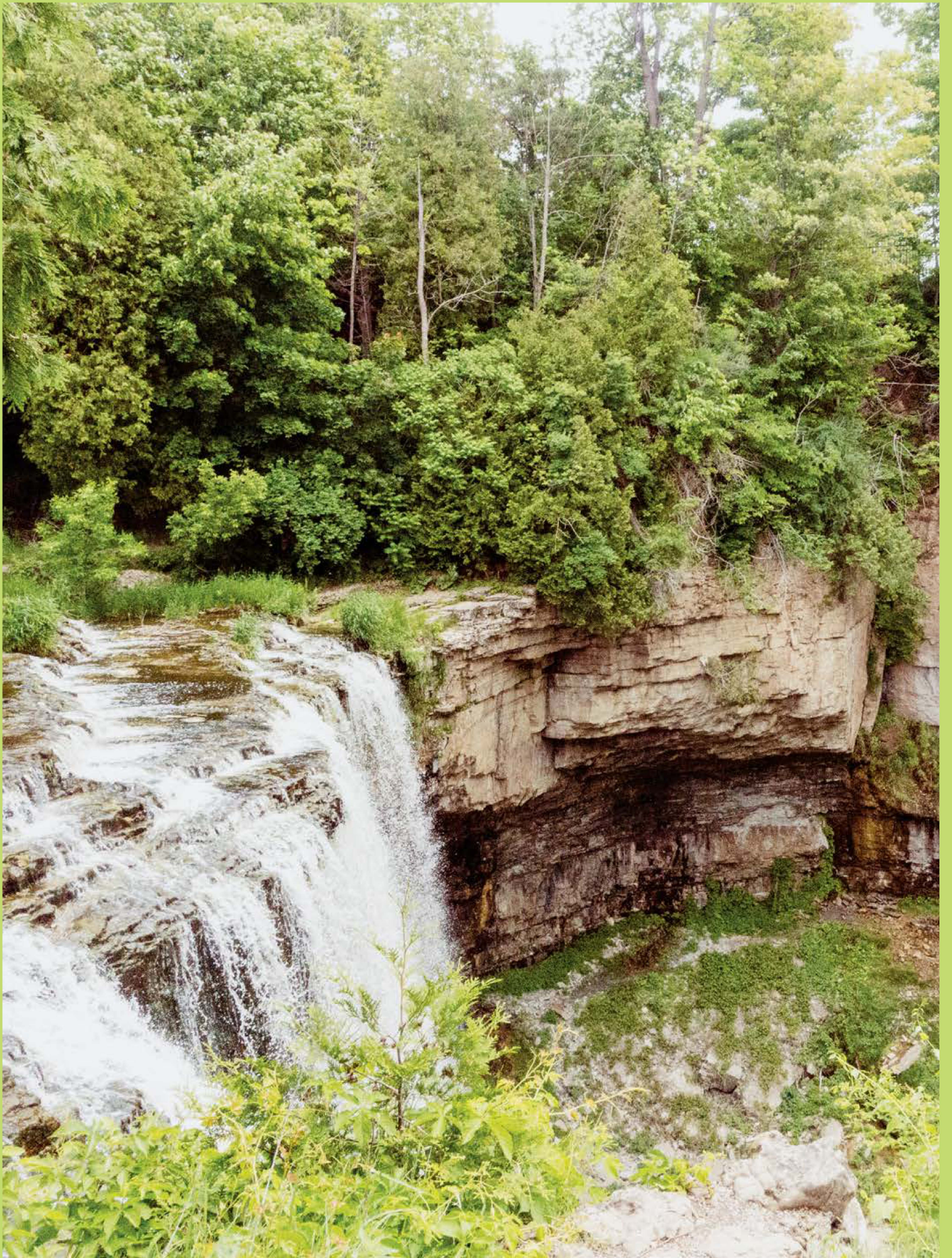
Notes:

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

**2024 Appeals Fees Deposit \$
(calendar year)**

30,307.00

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.



Ontario's Greenbelt

Access to information and
government transparency



Decisions affecting Ontario's Greenbelt are of significant public interest, engaging important environmental and governance implications. Established in 2005, the Greenbelt was designed to protect environmentally sensitive land, agricultural areas, and natural heritage systems from urban sprawl. Any changes to its boundaries or protections must be carefully deliberated and decided with utmost transparency and accountability.

In 2022, the government [announced](#) the removal of almost 2,000 acres of land from the Greenbelt to support housing development. This decision sparked widespread public outcry, particularly given previous [assurances](#) that the Greenbelt would remain untouched. Investigations by the [Auditor General of Ontario](#) and [Ontario Integrity Commissioner](#) later revealed serious flaws in the decision-making and record-keeping processes, raising concerns about transparency, fairness, and legal compliance.

Throughout 2022 and 2023, the IPC received 30 freedom of information appeals filed by researchers, members of the media, and other concerned individuals seeking access to records documenting government discussions, decisions, and actions related to the Greenbelt.

The appeal process under the Freedom of Information and Protection of Privacy Act (FIPPA) grants the IPC broad authority to review the government's responses to access to information requests. This includes the authority to review the reasonableness of the government's search for requested records and any government claims that the records either do not exist, are not within its custody or control, or are exempted or excluded from access under the act.

While many appeals are mediated and informally resolved at earlier stages of the IPC's dispute resolution process, some cases proceed to

adjudication. At the end of a formal adjudication process, the IPC may uphold the institution's decision as compliant with FIPPA and dismiss the requester's appeal. Conversely, the IPC may issue binding orders requiring the institution to, for example, conduct another search, issue another decision, or release responsive records to the requester in whole or in part.

This appeal process before an independent decision-maker, like the IPC, provides a fair and impartial means for ensuring compliance with FIPPA and reinforcing Ontarians' fundamental right to access government information. It also provides our office with a broad overview of multiple access requests in respect of the same or related matters and how they are treated across institutions. This gives us a unique vantage point to identify systemic issues or trends and make recommendations for achieving the act's purposes of access to information and transparency in relation to government decision-making.

To date, the IPC has processed 19 access to information appeals related to the proposed changes to the Greenbelt boundaries. Collectively, these cases revealed some concerning issues of a systemic nature, including the following:

Deletion of emails

In her Greenbelt report of 2023, the Auditor General observed that emails relating to changes to the Greenbelt were regularly being deleted by political staff, contrary to the Archives and Record Keeping Act (ARA). This observation raised concerns that records relating to the Greenbelt decision making process that were the subject of access requests and appeals might be lost or destroyed. Accordingly, the IPC issued an exceptional pre-emptive order in one of the first Greenbelt-related appeals. In this

interim order (PO-4449-I), the IPC required the Ministry of Municipal Affairs and Housing to take all reasonable measures to preserve any responsive records relating to the withdrawal of lands from the Greenbelt Plan in accordance with its obligations under the act and the ARA. If any such records had been deleted or destroyed, the IPC ordered the ministry to take steps to recover them.

In response to this order, the ministry provided affidavit evidence outlining the steps it had since taken to preserve records relating to Greenbelt Plan amendments and to recover deleted emails to the extent reasonably possible. The adjudicator was satisfied with the measures taken despite the technical limitations of recovering any permanently deleted emails.

Use of code words

The use of code words when referring to the Greenbelt project has had the unfortunate effect of frustrating freedom of information searches. See, for example, Orders [PO-4634](#), [PO-4611-I](#) and [PO-4644](#). Inconsistent use of code words such as "special project" or "SP — GB" or "GB" or "special project — GB" when referring to the Greenbelt project made it unduly difficult for the government to find responsive records using standard search methodology. Worse, the use of the codeword "G*" made it virtually impossible to find relevant records, given that the asterisk ("*") is used as a technical wildcard when conducting text searches, returning any word starting with "G". Trying to search with "G*" would have returned a massive number of records, rendering it wholly impossible to sort through.

Practically, that meant having to forego using the codeword "G*" as a search term, which may have missed some responsive records. Unfortunately, given the technical impossibility to search for records using this term, it remains impossible to know either way.

9000+

potentially responsive records reviewed by the Cabinet Office during the IPC's inquiry.

6 were ultimately found to be relevant.

Use of personal email and devices

The Auditor General also observed that political staff used personal email accounts and devices as a conduit through which government-related messages were forwarded to or from government accounts. This practice had the effect of circumventing the record-keeping obligations of FIPPA and limiting access to key decision-making records. It also rendered such emails and text messages vulnerable to loss on personal devices, which did occur. The Auditor General noted the practice of using personal devices to conduct government-related business is contrary to Ontario Public Service (OPS) guidelines on information security and acceptable use of I&IT. It also ignores long-standing IPC guidance that strongly warns against the use of personal email or messages to conduct government business.

When dealing with access to information appeals, the IPC will typically not order a search through the personal devices of government or political staff for privacy reasons, given the personal nature of communications on these devices. However, where there was credible evidence to suggest that government-related emails or messages existed on personal devices

of individual staff, as in several Greenbelt-related cases, the IPC ordered the institution to require those individuals to search for responsive records on their personal devices, including the Premier himself. (See orders [PO-4577-F](#), [PO-4638](#), [PO-4639-I](#), and [PO-4640-I](#))

Since the Auditor General's Report, Cabinet Office now requires all Premier's Office and ministers' staff to annually attest to using only government systems and accounts for government business and ensure any government records inadvertently received on a personal email account are transferred into the government system for proper record retention.

Control over personal emails of former staff

Some institutions claimed they had no custody or control over government-related records in the personal email account of former staff, despite credible evidence that personal email accounts were used during the Greenbelt decision making process. For example, the Ministry of Municipal Affairs refused to assert control over such records on the grounds that it had limited legal recourse to do so once the employment relationship had terminated.

However, in Orders [PO-4639-I](#) and [PO-4640-I](#), and [4652-I](#), the IPC found that institutions have legal responsibility over all government-related records arising from their recordkeeping and record management obligations under the ARA. Where there was reason to believe government records may exist in personal email accounts of former staff, the IPC ordered the institution to assert control over the records and to direct former staff to produce them. Any recovered records would then have to be transferred to, retained, and preserved on government-sanctioned information systems in accordance with OPS Guidelines and IPC [Guidance on Personal Email Accounts and Instant Messaging](#).

Lack of proper documentation

It was surprising to find so few responsive records documenting any government decisions or actions, how and when they were made, and by whom. The near-total absence of decision-making documentation is particularly concerning, especially on a file as high profile and consequential as changes to the Greenbelt. Despite evidence of meetings and discussions involving Premier's Office staff and ministry staff about the Greenbelt, there was very little documentation of what was said or decided in those conversations, aside from a few contemporaneous notes taken by ministry staff. These notes reflect what staff understood at the time to be directives from the Premier's Office. Yet, as the Integrity Commissioner found, these directives likely came from the ministry's chief of staff, not the Premier's Office. Unfortunately, the lack of proper documentation only added to the murkiness of decision making. (See Orders [PO-4638](#), [PO-4611-I](#), and [PO-4644](#))

Regardless of who issued the directives, and whether they were



verbal or written, the dearth of documentation of any discussions, decisions or actions runs counter to basic record-keeping requirements and undermines government transparency.

Lessons learned

The Greenbelt-related appeals offer a clear example and cautionary tale about the consequences of inadequate recordkeeping. When key government decisions are not properly documented, when code words are used, or when records are stored in fragmented ways across personal

and official systems, transparency suffers, and with it, public trust.

There are several important lessons to be learned from the Greenbelt-related orders issued to date.

- › The use of opaque codewords to refer to discussions and decisions about important government matters weakens transparency. These practices not only violate legal record-keeping obligations, they also erode public trust in the integrity of government decision-making. The public has a fundamental right to know how and why decisions are made, especially those that impact

protected lands like the Greenbelt. When records are obfuscated and made difficult, if not impossible, to find through evasive code words, transparency is compromised, and oversight becomes illusory.

- › The absence of records raises serious accountability concerns and undermines public trust. Whether digital, handwritten, or verbal, decisions of public importance must be documented. Without a full and accurate record of decision-making, when, by whom and on what basis, the public is left in the dark about government actions that affect their

communities and the environment. When records are lost, destroyed, obfuscated, or never created in the first place, it raises more questions than answers.

- › Institutions cannot avoid FIPPA obligations based on where a record is stored. When there is credible evidence that official records exist outside government systems, including in the personal email accounts of current or former staff, institutions are obligated to take proactive steps to assert control over them and retrieve, transfer, and preserve them on government information systems. This serves to protect government records from security vulnerability as well as to facilitate reasonable searches in response to FOI requests.
- › The lack of a robust records management system reflects a poor level of commitment. The IPC's findings in these appeals highlight the urgent need for stronger records management practices, regular staff training, clear policies prohibiting the use of personal email accounts and devices for conducting government business, and a clearly articulated, unwavering commitment to transparency and public accountability. Without a full and accurate record of decision-making, the public is left in the dark about government actions that affect their communities and the environment.

Recommendations for strengthening transparency and public trust

Through its guidance on [Instant Messaging and Personal Email Accounts: Meeting Your Access and Privacy Obligations](#), the IPC has consistently emphasized the need for sound record-keeping practices and compliance with FIPPA and ARA to ensure transparency and public

accountability. This guidance has been reinforced by numerous presentations delivered to government and political staff on access and privacy obligations, explaining the serious consequences of poor records management.

These concerns were already articulated in the IPC's 2013 special report, [Deleting Accountability](#), which exposed systemic failures in record-keeping and highlighted the risks of improper deletion and lack of retention of key government records. These lessons of more than a decade ago have come back full circle. To address the systemic issues raised in these appeals, the IPC reiterates the following recommendations to government:

- › **Review and modernize record-keeping and retention practices.** Institutions must ensure that their retention policies and practices are regularly reviewed and updated, and that their implementation is supported by clear practice and procedure guides. Ministers' offices and the Premier's Office should prioritize documenting verbal directions, discussions, and decisions. Special attention should be given to preserving contemporaneous records of meetings and avoiding the use of evasive code words.
- › **Prohibit the use of personal tools for official business.** Institutions should adopt clear policies prohibiting the use of personal email accounts and personal devices for official business, emphasizing that records relating to institutional business — even if created or stored on personal devices or accounts — remain subject to FIPPA. Where their use may be unavoidable and staff have sent or received business-related communications using unauthorized tools or accounts, staff should immediately, or within a reasonable time, transfer records to their official or authorized email account or the institution's computer or network.

These policies should be clearly incorporated as binding terms of staff members' contracts of employment.

› **Train early and often.**

Staff must be trained on their record-keeping obligations. This training should be delivered immediately following changes in staffing or a change in government and on an ongoing basis thereafter. Staff should be informed that all business-related communications are subject to disclosure and retention requirements, regardless of the tool, account or device used, and that they will have to provide a copy of all business-related communications upon request. Staff should also be reminded that when they are collecting records in response to an access to information request, they must search for and produce any relevant records from instant messaging and personal email accounts, even if they exist contrary to policy.

› **Monitor for compliance.**

Staff must be held accountable for complying with record keeping requirements throughout their employment, up to and including upon departure. Institutions should designate a senior official responsible for compliance. They should regularly monitor for compliance over time, by conducting annual reviews as well as occasional spot-checks or surveys of staff practices. Where non-compliance

“
WHEN RECORDS ARE
LOST, DESTROYED,
OBFUSCATED, OR NEVER
CREATED IN THE FIRST
PLACE, IT RAISES MORE
QUESTIONS THAN
ANSWERS.”

is found or suspected, institutions must take immediate action to preserve the records and prevent further loss of information.

› **Codify a duty to document.**

To avoid many of the pitfalls associated with Greenbelt-related access to information appeals, the IPC recommends that FIPPA and its municipal counterpart, MFIPPA, should be amended to include an explicit duty to document communications, decisions and actions. These laws should also include an explicit requirement for institutions to define and implement appropriate retention measures.

These steps would go a long way toward strengthening public trust and ensuring that the right of access to government-held information is

not undermined by weak practices, disregard of policies, or incorrect assumptions. A functioning access to information regime depends not only on strong laws but on a culture and commitment to follow them.

Postscript

In response to the serious concerns raised by the Auditor General and the Integrity Commissioner, Cabinet Office and relevant ministries have made several efforts to strengthen their record-keeping practices. This includes compiling and safeguarding all records previously submitted to the Auditor General and Integrity Commissioner during their respective investigations.

At a May 6, 2024 [appearance](#) before the Standing Committee on Public Accounts on the consideration of the

AG's Special Report on Changes to the Greenbelt, the Secretary of the Cabinet outlined additional measures to improve transparency and information management, including:

- › a joint memo with the Premier's chief of staff reminding all OPS and political staff to preserve and manage all records in accordance with record-keeping requirements
- › increased frequency of records management training for all political staff, reinforcing the requirement that all government business must be conducted on government networks and accounts and any public records or communication inadvertently received on a personal account or device must be forwarded to their government account
- › annual record-keeping attestation for staff in the Premier's and ministers' offices

The Secretary emphasized that these steps, among others, were implemented within 90 days of the Auditor General's report and are intended to reinforce compliance with Ontario's access and record-keeping laws.

In 2024, the IPC conducted six information sessions organized by the Premier's Office, highlighting the principles of access to information and the importance of strong record keeping and retention practices, reinforcing their responsibilities under FIPPA and the Archives and Recordkeeping Act.

With respect to IPC orders related to the Greenbelt, the government has complied or stated its intention to comply with several, including [PO-4449-I](#), [PO-4505-F](#), [PO-4638](#), and [PO-4611-I](#), with the exception of [PO-4577-F](#) in respect of which the government is seeking judicial review.

These steps signal positive movement toward compliance, though ongoing oversight remains essential to ensure corrective measures are not only implemented but sustained. ●

“
THE NEAR-TOTAL ABSENCE OF DECISION-
MAKING DOCUMENTATION IS PARTICULARLY
CONCERNING, ESPECIALLY ON A FILE
AS HIGH PROFILE AND CONSEQUENTIAL
AS CHANGES TO THE GREENBELT.”



Summaries of Greenbelt-Related Cases to Date

In several cases, cooperative mediation between the parties led to additional records being disclosed or further searches conducted, successfully resolving the matter without requiring a formal order.

Three complex appeals involving over 76,000 pages of records related to the Greenbelt boundary were resolved based on the commitment of the parties to work with an IPC mediator. The appellant worked to clarify and narrow the issues and formulate questions and the ministry worked to provide a detailed and satisfactory response. The parties were able resolve these appeals without the need for formal adjudication, saving time and resources.

As for the cases that did not successfully resolve at mediation or went straight to adjudication, the following is a summary of their outcomes in chronological order.

Ministry of Municipal Affairs and Housing

Interim Order PO-4449-I
(October 13, 2023)

Final Order PO-4505-F (April 8, 2024)

Orders PO-4449-I and PO-4505-F relate to a request for a high volume of

records respecting the Greenbelt land removals. Given that the Ministry of Municipal Affairs and Housing had failed to issue a final access decision on time, and the passage of several months since the deadline, the IPC issued an order requiring the ministry to preserve and recover records. This step was particularly important in light of the Auditor General's observations that political staff had used personal emails to conduct government business and may have deleted records.

In response, the ministry submitted affidavit evidence outlining the steps it has taken to preserve relevant records. These included:

- › creating a dedicated internal SharePoint site to store Greenbelt-related files
- › collecting and maintaining records shared with the Auditor General and Integrity Commissioner
- › extracting email data from Ontario.ca mailboxes of current and former staff
- › attempting to recover records from personal accounts (with limited success)
- › confirming record retention practices aligned with the Archives and Recordkeeping Act.

The adjudicator was satisfied that measures were put in place to preserve Greenbelt-related records. At the same time, the adjudicator acknowledged the limits of recovering data permanently deleted data from Ontario.ca email accounts before these safeguards were implemented. As the ministry's attempts to recover Greenbelt-related emails from former staff had not been successful, the adjudicator noted that there remained a risk that personal emails relating to the Greenbelt might have been lost.

While not ruling on whether all responsive records were adequately preserved, the adjudicator recommended improvements to recordkeeping and accountability. These include reinforcing training on retention obligations, emphasizing the importance of using official channels for government work, and designating a senior official responsible for compliance.

Final Order PO-4505-F reinforces the principle that preserving access to records is critical for government transparency, and that ministries must follow strict guidelines to maintain accountability and preserve public trust.

Cabinet Office

PO-4577-F (November 29, 2024)

The primary issue in this appeal was whether call logs from the Premier of Ontario's personal cell phone should be considered government records subject to FIPPA. An individual submitted two access requests seeking a list of all incoming, outgoing, and missed calls from the Premier's personal device between October 31 and November 6, 2022. Cabinet Office denied access, arguing that because the phone was privately owned and not assigned to a government account, the records were not in its custody or control and therefore did not fall under FIPPA.

The requester appealed, arguing that the Premier used his personal phone for government business and that records of those calls should be accessible under the law. During the inquiry, the IPC reviewed arguments from Cabinet Office, the Premier, and the appellant. The adjudicator ultimately rejected Cabinet Office's position, finding that while some of the Premier's calls may have been personal, there was sufficient evidence to conclude that the Premier also used his personal cell phone to conduct government business. Since Cabinet Office would reasonably expect to obtain and provide records of government-related calls made on an official phone, the same access principles should apply when government-related calls are made or received using a personal device.



THIS APPEAL HIGHLIGHTS SIGNIFICANT GAPS IN RECORD-KEEPING PRACTICES RELATED TO THE GREENBELT DECISION-MAKING PROCESS, INCLUDING THE RELIANCE ON VERBAL INSTRUCTIONS, THE USE OF PERSONAL EMAIL ACCOUNTS BY POLITICAL STAFF, AND CONCERNS ABOUT DELETED OR UNDOCUMENTED COMMUNICATIONS.”

(PO-4611-I (Ministry of Municipal Affairs and Housing))

The IPC ordered Cabinet Office to obtain those government-related call log entries from the Premier. The adjudicator emphasized that personal and constituency-related calls remain outside Cabinet Office's control, and that any privacy concerns could be addressed through appropriate redactions or exemptions under FIPPA.

The order reinforces the principle that public officials cannot bypass transparency requirements by using personal devices for government work. What matters is the content and purpose of the communication, not the device used.

The government is seeking judicial review of this order.

Ministry of Municipal Affairs and Housing

Interim Order PO-4611-I
(February 20, 2025)

An access request was submitted for records of directives from the Premier's Office to the Ministry of Municipal Affairs and Housing regarding the removal of lands from the Greenbelt. The ministry responded that no responsive records existed aside from the Premier's June 2022 mandate letter, which was withheld under the Cabinet confidentiality exemption. The requester appealed, arguing that reports and testimony suggested such directives had been issued.

The IPC found that there was a reasonable basis to believe responsive records existed and that the ministry had taken an overly narrow approach to interpreting the request. While the ministry's search for email records was upheld as reasonable, the IPC determined that other types of records, such as meeting notes documenting verbal directives, had not been properly searched. Reports from the Auditor General and the Integrity Commissioner indicated that key Greenbelt decisions were communicated verbally through

the minister's chief of staff, who referenced the Premier's Office in discussions with ministry staff. Notes taken by officials contained references to the Premier's Office and the Premier, whether yet the ministry had not included these records in its search.

The IPC ordered the ministry to conduct a new search focusing on meeting notes and other contemporaneous records of verbal direction. This appeal highlights significant gaps in record-keeping practices related to the Greenbelt decision-making process, including the reliance on verbal instructions, the use of personal email accounts by political staff, and concerns about deleted or undocumented communications.

Ministry of the Solicitor General

PO-4634 (April 1, 2025)

A journalist requested records from the Ministry of the Solicitor General related to the Ontario Provincial Police security detail for the Premier, specifically seeking the dates the Premier attended a specific restaurant. The request covered records created between February 1 and December 1, 2022, tied to any meetings the Premier held at that location. While the ministry located officers' notes as responsive records, it denied the appellant access to them under the personal privacy exemption. The appellant appealed the ministry's decision, clarifying they were only seeking access to the dates the Premier was at the restaurant, and argued that the public interest override might apply.

The IPC acknowledged that the Premier may have conducted government or business meetings at the restaurant but observed that releasing specific dates, without being able to recall or otherwise determine



which ones related to government business, would reveal something of a personal nature about the Premier. The totality of dates without such distinction would show the frequency or regularity with which the Premier attends the restaurant and could reveal a pattern in the Premier's personal choices and habits, and therefore qualifies as the Premier's personal information. The IPC concluded that the disclosure of the dates the Premier attended the restaurant would be an unjustified invasion of the Premier's personal privacy.

The IPC also found that the public interest in disclosure of the dates did not outweigh the privacy concerns. While the IPC recognized that the Premier is a public figure and the actions and decisions relating to the Premier's public office are of public interest, the Premier was still entitled to privacy with respect to personal matters, including the dates on which he attends a local restaurant. In the result, the IPC upheld the ministry's decision and dismissed the appeal.

The IPC has consistently distinguished between personal

records and those created during government work. Records such as emails, call logs, or directives that relate to official business are subject to access under FIPPA. Personal matters, even involving a public figure, are not.

Cabinet Office **PO-4638 (April 10, 2025)**

An individual requested all records in the Premier's Office relating to the proposed removal of Greenbelt lands from January 2021 to October 2022.

Cabinet Office initially located only one responsive record. The requester appealed, claiming additional records should exist and citing freedom of information responses from the Ministry of Municipal Affairs. Those responses referred to communications involving Premier's Office staff, including references to "PO decision points," and testimony by ministry staff suggesting that directions may have come from the Premier's Office.

During the IPC's inquiry, Cabinet Office conducted broader searches using refined search terms and reviewed over 9,000 potentially responsive records. Only six records were found to be relevant. The IPC found that Cabinet Office had conducted a reasonable search, relying on experienced staff and a broad interpretation of the request.

The adjudicator expressed concern about the surprisingly low number of responsive records found, given the significance and profile of the Greenbelt issue. The adjudicator observed that it is unusual, and concerning from a recordkeeping perspective, that so few records were identified given the importance of the Greenbelt matter which involved senior level decision-making across multiple ministries.

The IPC ordered Cabinet Office to conduct a further search after the appellant provided evidence that the original search failed to locate a government-related Teams meeting invitation received at the personal email address of a former senior Premier's Office employee. The IPC directed Cabinet Office to ask the former employee to search their personal accounts for responsive records. The IPC also directed Cabinet Office to ask former staff who did not sign a 2024 attestation of compliance with recordkeeping requirements to search their personal accounts for responsive records.

“

IT IS UNUSUAL, AND CONCERNING FROM A RECORDKEEPING PERSPECTIVE, THAT SO FEW RECORDS WERE IDENTIFIED, GIVEN THE IMPORTANCE OF THE GREENBELT MATTER WHICH INVOLVED SENIOR LEVEL DECISION MAKING ACROSS MULTIPLE MINISTRIES.”

(Order PO-4638 (Cabinet Office))

While institutions are not typically required to search personal accounts, they may be required to do so when there is credible evidence that official records may exist outside government systems. This further emphasizes the importance of using only government-issued devices and accounts to conduct government business. When staff use personal accounts or devices, it undermines efforts to preserve the public record and the freedom of information process. Moreover, the small number of responsive records suggests an absence of record creation and preservation which is also problematic.

Ministry of Municipal Affairs and Housing

Interim Orders [PO-4639-I](#) and [PO-4640-I](#) (April 15, 2025)

These two appeals from the decisions of the Ministry of Municipal Affairs and Housing related to requests for access to the personal emails of the former minister's Chief of Staff.

The appellants made requests for access to emails in the former Chief of Staff's personal email account relating to the Greenbelt. The ministry provided some records of personal emails that had been forwarded by the former Chief of Staff to their official government email account. However, the ministry maintained that any relevant personal emails on the former employee's personal account, if they existed, were not under its control.

The adjudicator examined whether personal emails held by the former Chief of Staff to Ontario's Minister of Municipal Affairs and Housing are "under the control" of the ministry for access purposes under FIPPA.

In these interim orders, the adjudicator found that any personal emails relating to the Greenbelt amendment, if they exist, are under the ministry's control, even if they are on a personal email account. This is because:

- › any responsive emails, if they exist, relate directly to government business
- › the ministry has duties under FIPPA and the Archives and Recordkeeping Act to retain and preserve public records and must take active steps to assert control over them
- › given the nature of the public service employment relationship, it is reasonable to expect that a public servant's duties to their employer extend beyond the termination of employment and include the requirement to produce any government records in their possession.

The adjudicator ordered the ministry to assert control over the records and direct the former Chief of Staff to provide any responsive emails from their personal account or swear an affidavit confirming no such records exist. The adjudicator noted that the ministry may have potential remedies under law to compel the return of any

responsive records. The adjudicator also noted that the IPC has the authority to summon and examine, under oath, any individual who may have information relating to an inquiry.

This order again reinforces the principle that under FIPPA, institutions have custody or control of records about government business, regardless of whether those records are stored in a government account, in a personal account, or anywhere else.

Ministry of Municipal Affairs and Housing

PO-4644 (April 23, 2025)

An access request was submitted for records of directives from the Premier's Office to the Ministry of Municipal Affairs and Housing regarding the removal of lands from the Greenbelt. Cabinet Office initially advised that no responsive records existed, but during mediation, it located two: the Premier's mandate letter and a draft mandate letter. The requester appealed, arguing that additional records should exist, and that Cabinet Office had not conducted a reasonable search.

The IPC found that Cabinet Office conducted a reasonable search and dismissed the appeal. The adjudicator accepted that Cabinet Office adopted a broad and appropriate interpretation of the term "directive," applied multiple search terms (including code words like "special project" and "GB"), and searched the accounts of 29 current and former Premier's Office staff. Cabinet Office also searched records provided to the Auditor General and asked staff to transfer any responsive records from personal accounts to official systems.

Although the appellant pointed to reports and testimony suggesting that the Premier's Office gave direction to ministry officials, the IPC found no evidence that such direction, if it existed, was ever documented in writing or been deleted. Unlike the findings in Order PO-4638, discussed below, the IPC found no basis to require searches of personal accounts.

This order highlights how the use of verbal instructions, informal communication channels, and coded language can frustrate transparency and accountability. Even where there is evidence that government direction

was given, the absence of documented records leaves little recourse under access to information laws. The decision reinforces the importance of consistent and accurate record-keeping, especially in matters of significant public interest.

Cabinet Office

Interim Order PO-4652-I (May 5, 2025)

The appellant submitted a request for the calendar of the former senior official in the Premier's Office for the period from June 1 to December 31, 2022. Cabinet Office located the responsive records and granted the appellant partial access to them.

The appellant appealed Cabinet Office's decision, claiming that it did not conduct a reasonable search because it ought to have searched the individual's personal calendar. In this interim order, the adjudicator found the individual's personal calendar was not within the scope of the appellant's request and upheld Cabinet Office's decision not to search it. However, the adjudicator found Cabinet Office's search of the individual's government Outlook calendar was not reasonable because it did not provide sufficient evidence to support its claim that the entries marked "Private" in the individual's official government calendar were, in fact, private or personal in nature. The adjudicator ordered Cabinet Office to obtain an affidavit from the individual confirming the nature of the calendar entries marked "Private" in their government Outlook calendar. In the case that any of the entries marked "Private" were found to relate to government business, the adjudicator orders Cabinet office to require the individual to search their personal calendar for any corresponding entries and provide any such records to Cabinet Office so it can render a revised access decision. ●



From Vision to Impact

Five Years of Privacy and Transparency in a Digital Ontario



2024 Annual Report



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