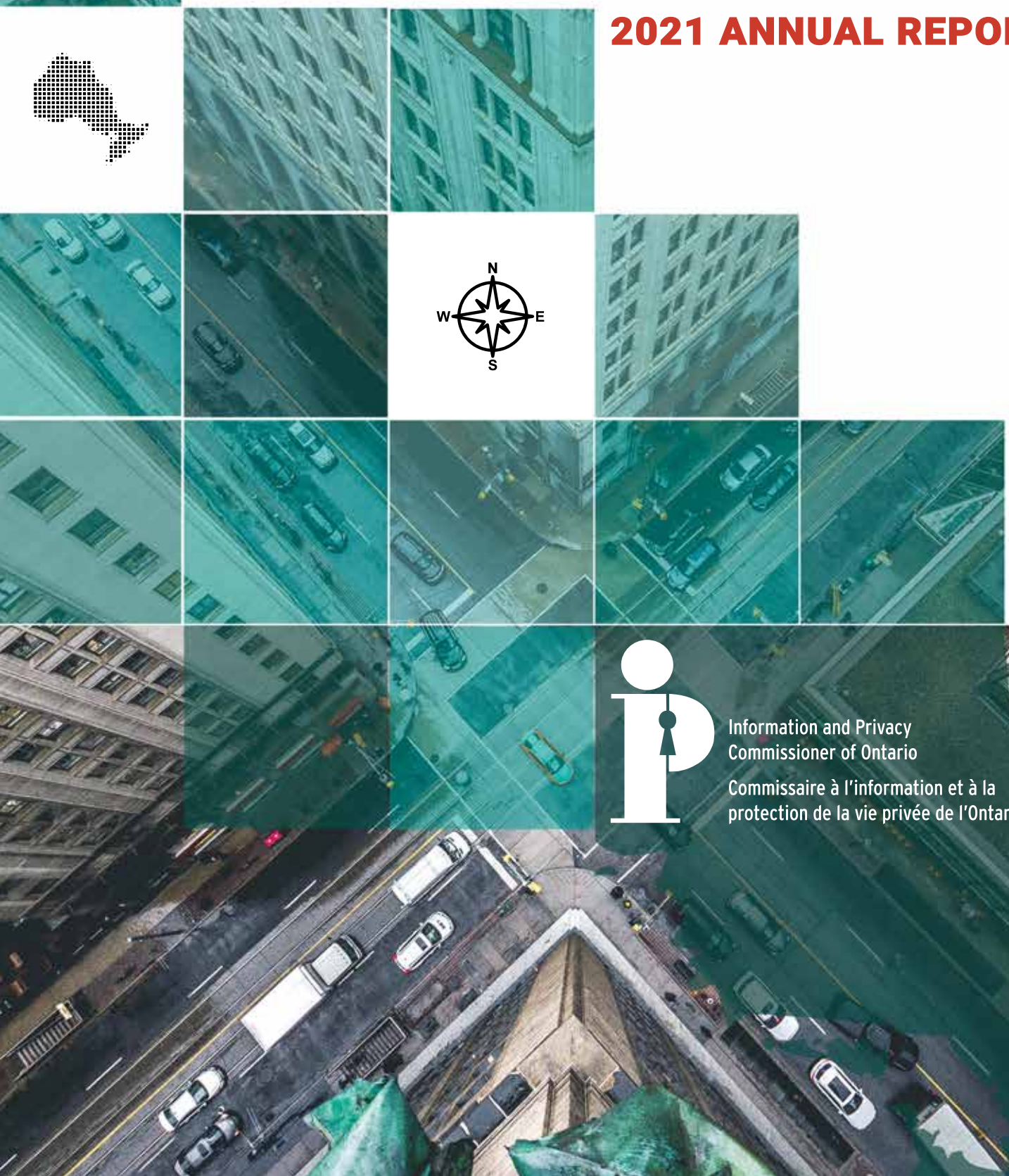
Access and Privacy: Cornerstones of a Digital Ontario

2021 ANNUAL REPORT



Information and Privacy Commissioner of Ontario

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

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

June 14, 2022

The Honourable Ted Arnott
Speaker of the Legislative Assembly of Ontario

Dear Mr. Speaker,

I am pleased and honoured to share with you the IPC's 2021 annual report, *Access and Privacy: Cornerstones of a Digital Ontario*. It covers the period from January 1 to December 31, 2021, providing a snapshot of notable activities, initiatives, and recommendations from the past year.

One of the most profound effects of the pandemic has been the accelerated digitization of our home and work lives. We are experiencing a historic shift in our evolution toward an ever increasingly digital society. This large-scale digital transformation is an enormous opportunity to improve people's lives, overcome obstacles, and support innovation in our province.

Access and privacy rights play a crucial role in ensuring that the foundations of an equitable digital Ontario are of solid construction, built to support the weight of the ever-expanding digital infrastructure.

I consider myself very fortunate to lead an organization whose mission is to uphold and advance access and privacy rights at such a critical point in our shared history. My office will continue to offer input and advice as we focus on Ontario's digital and data priorities and help shape a responsible and sustainable future together.

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

Yours sincerely,

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

With this, my second annual report, I reflect not only on the previous year's work but also on the unprecedented challenges — and opportunities — ahead as we continue to evolve in an increasingly digital society.

Patricia Kosseim
Information and Privacy Commissioner of Ontario

COMMISSIONER'S MESSAGE

The unrelenting impacts of the pandemic throughout 2021 and the accelerated digitization of almost every aspect of our lives continued to raise some of the most complex data access and privacy issues in the IPC's history. With this, my second annual report, I reflect not only on the previous year's work but also on the unprecedented challenges — and opportunities — ahead as we continue to evolve in an increasingly digital society.

After two years of living and working remotely, the pandemic has shown us that it is possible to do almost anything online. The public now expects and deserves to receive government services online through the most efficient and advanced means available. In response, the government unveiled a bold **Digital and Data Strategy** as an important step toward "making the province a world-leading digital jurisdiction," promising to deliver more convenient, reliable, and accessible online services to Ontarians. Building on this impetus, public institutions are progressively turning to complex technologies to improve government programs and services by enabling online access and developing means of verifying and authenticating digital identity.

At the same time, the pandemic has served as an alarming reminder of just how vital it is to gain timely access to intelligible data. Data can be used to better understand the scope and the nature of the challenges before us, enhance services to the particular needs of different communities, and support critical decision-making about our health and safety, education, and work. As part of building a digital Ontario, the government recognizes that "data represents an enormous opportunity to improve people's lives, solve challenges, generate new economic growth and provide a world-leading competitive advantage for our province."

As Ontario endeavours to realize the full benefits of increased efficiency and access to government information and services through technology, the rapid adoption of digital tools has the potential to raise significant privacy and access to information issues that affect us all.

Ontario's access and privacy laws were enacted long before any of the current technological solutions were even imaginable. As we hurtle toward a progressively digital world, Ontario's access and privacy laws must catch up to these technological advances and ensure they reflect the society they are meant to regulate. Privacy laws that do not incentivize proactive risk mitigation, require notification in the event of data breaches, or regulate the increasing role of private sector actors are no longer fit for today's realities. An access to information regime that takes years to process requests and obtain data that may have entirely lost its relevance is not a sustainable basis on which to build Ontario's promising digital future.

Access and privacy rights for all Ontarians play a vital role in ensuring that the very cornerstones of an equitable digital Ontario are of solid construction, built to support the weight of the ever-expanding digital infrastructure of our online existence.

I consider myself very fortunate and inspired to lead an organization whose mission is to protect and advance those rights at such a critical point in our history, when decisions and actions taken now will

In 2021, the commissioner (centre) was pleased to welcome aboard (from left) Jason Arandjelovic, Chief Financial Officer and Director of Corporate Services, Warren Mar, Assistant Commissioner, Tribunal and Dispute Resolution Services, and Eric Ward, Assistant Commissioner, Strategic Initiatives and External Relations. The IPC's new executive leadership team is working together and with their respective divisions to chart the path towards the IPC's vision of the future.

indelibly affect the kind of digital society we build for the future. A future in which our children can grow up confident that their fundamental privacy and access rights will continue to be respected and their democratic freedoms will remain solidly intact even amidst large-scale digital transformation.

With that future as our North Star, the IPC has set out a vision to chart our course for the next few years. Working with relevant partners, we will strive to enhance Ontarians' trust that their access and privacy rights are being respected by:

- actively focusing on key strategic issues that impact their lives the most
- responding to complaints and appeals in a fair, timely, and meaningful manner
- maintaining the organizational excellence and accountability of the IPC

Throughout 2021, we have made great strides in advancing this three-pronged vision.

Our Strategic Initiatives and External Relations Division, with the support of IPC's external **Strategic Advisory Council**, has focused our proactive education, communication, and guidance efforts to enhance our real-world impact in four key strategic areas: ***Privacy and Transparency in a Modern Government***; ***Children and Youth in a Digital World***; ***Next-Generation Law Enforcement***; and ***Trust in Digital Health***.

In 2021, our Tribunal and Dispute Resolution Division worked tirelessly to reduce the backlog of files accumulated during the early months of the pandemic. Valuable lessons learned through that pilot project will help inform a broader lean process review we have planned for 2022–2023 to gain further efficiencies and reduce timelines for processing appeals and complaints to our office in accordance with service standards Ontarians deserve.

Our Corporate Services Department has put in place the foundational building blocks of a management and accountability infrastructure that Ontarians have come to expect of the IPC as a public institution. This includes enhancing online access to our services, digitizing our records, adopting new communication and collaboration tools, and strengthening our information security systems to lead by example. We're also investing in people by building our internal capacity with the skills, technology, and know-how needed as a modern, agile, and effective regulator.

I am extremely honoured and privileged to lead such an extraordinary team of highly dedicated and knowledgeable professionals at the IPC. Despite the many changes and operational challenges of a remote workplace, they continue to demonstrate — day in and day out — an unwavering commitment to the highest standards of excellence and public service.

Our work in 2021 culminated in some noteworthy advancements for access and privacy rights in Ontario. I am pleased to share an overview of some of the most significant developments from the past year.

Patricia Kosseim
Commissioner

IPC VISION

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

ACTIVELY ADVANCING ONTARIANS' RIGHTS IN KEY STRATEGIC AREAS

In 2021, the IPC released its **strategic priorities for 2021-2025**. These priorities focus on promoting and protecting Ontarians' information rights in a data-driven world where institutions and organizations are rapidly accelerating their use of digital technologies and artificial intelligence.

These strategic priorities serve as a road map for proactively addressing key access and privacy issues that matter to Ontarians and where the IPC can have greatest positive impact. In 2021, the IPC made great strides along that journey, working to promote and protect Ontarians' information rights and help build the public's trust in the institutions and organizations that serve them.

Privacy and transparency in a modern government

In realizing our priority of ***Privacy and Transparency in a Modern Government***, our goal is to advance Ontarians' privacy and access rights by working with public institutions to develop bedrock principles and comprehensive governance frameworks for the responsible and accountable deployment of digital technologies.

Throughout 2021, we made several submissions to government, both formally and informally, to develop those principles and governance frameworks for the use of these technologies by Ontario's public institutions.

Policy framework for Ontario's digital identity program

In August 2021, the Ontario government held public consultations on the development of a policy framework for Ontario's Digital Identity Program. The IPC responded with an open letter to Ontario's chief digital and data officer. Our submission noted that the government's digital identity program is a significant initiative that could, over time, have far reaching impacts on government service delivery. Strong privacy and security will be critical drivers for ensuring public trust in the program. Its success will depend on a comprehensive statutory privacy framework with robust and effective oversight.

It will be critical to design a user-centric system that allows individuals to remain in control of their digital ID, deciding who they want to show it to and for what purposes. The IPC welcomed the government's commitment to work toward minimizing data collection and developing a decentralized model of storing and using digital IDs that gives citizens ultimate control over the use of their personal information. The overall effect of digital ID over time and across transactions will also need to be carefully managed to uphold the societal value we place on anonymity. In addition, ensuring the program is inclusive and accessible to all will be vital in protecting the rights and interests of vulnerable populations. In that regard, enrolment needs to address all potential economic, social, physical, or administrative barriers and provide alternatives for those who cannot, or choose not to, enrol.

We commend the government on its stated commitments to uphold individual privacy, security, and personal control. We encourage the government to take a privacy-first approach when designing and implementing its digital ID program and we look forward to continued consultations on this initiative throughout 2022.

A trustworthy artificial intelligence framework for Ontario

With the release of its **Digital and Data Strategy**, the government expressed its intention "to build a digital economy powered by ethical artificial intelligence (AI) rooted in democratic principles and individual rights."

The IPC submitted **comments** to the government's consultation on Ontario's **Trustworthy Artificial Intelligence (AI) Framework**, commending its principles-based approach. Among our 14 recommendations, we recommended the government:

- clarify the scope of application and definitions to reduce ambiguity and avoid accountability gaps
- expand transparency requirements to include which data are being collected and used, the purpose of the AI system, and how its effectiveness is being measured
- develop mechanisms for individuals to contest decisions or outcomes of AI systems based on bias, inaccuracy or inappropriateness
- adopt algorithmic impact assessment tools that integrate privacy risk assessment, are documented, and ongoing in nature
- require more robust and explicit accountability and governance measures throughout the lifecycle of an AI system, including human review of automated decisions and intervention, as appropriate
- align the province's AI strategy with existing legislative frameworks and proposed reforms
- establish clear "no-go zones" for AI practices beyond acceptable levels of risk or where Ontarians' human rights may be significantly negatively impacted
- carefully design strong and independent models of oversight and means of meaningfully consulting and engaging Ontarians

The IPC continues to build on our AI policy research in collaboration with regulatory authorities in Ontario, Canada, and around the world to foster a responsible approach to ethical AI governance consistently across provincial and municipal institutions.

The new provincial data authority to promote broader access to government data

As part of its proposed Digital and Data Strategy, the government also proposed the establishment of a new **provincial data authority**. The proposed data authority aims to provide greater access to more government data for Ontarians, businesses, and organizations and enable broader data sharing across the province. At present, the structure and scope of the data authority have not been determined. The IPC's **submission** recognized the valuable role a data authority

could play in promoting the virtues of open data and extending its benefits to all Ontarians based on inclusion, fairness, and equity. We addressed fundamental access and privacy considerations that the government should incorporate into the development of a proposed data authority. Our submission also included recommendations to focus on gaps in the existing system rather than duplicate existing structures. We recommended taking an integrated, cross-sectoral approach to privacy and security protection across our digital economy and society, emphasizing the importance of independent IPC oversight of government institutions' access and privacy decisions and practices.

Any additional legal powers or authorities granted to the government as a part of a broader data sharing strategy should be accompanied by enhanced privacy protections for Ontarians. We recommended long overdue updates to the *Freedom of Information and Protection of Privacy Act* (FIPPA). For example, including requirements for institutions to conduct privacy impact assessments for high-risk initiatives and report data breaches to Ontarians and the IPC above a certain threshold. Updates to FIPPA would signal to Ontarians that their government institutions are evolving in a good balance.

The next phase of the government's proposal should include additional details about the data authority's planned purpose, powers, duties, functions, and governance. Ontarians and interested stakeholders, including the IPC, should be further consulted on these details before steps are taken to create a new permanent structure or new legal authorities.

In addition to making formal policy submissions to government, the IPC launched new guidance for stakeholders and public education initiatives to promote a culture of openness and transparency as a hallmark of trust in a modern government.

Providing clarity on the public interest override

During **Right to Know Week**, the IPC put the spotlight on freedom of information by releasing new guidance on how and when public institutions can disclose records under the **public interest override provision** of Ontario's access and privacy laws. This guidance describes when and in what circumstances organizations can override certain access exemptions and disclose a record when there is a compelling public interest to do so.

The ability to override exemptions and release information in the public interest has been particularly important throughout the pandemic. The public needs to know the changing health and safety risks they are up against and understand how to effectively mitigate those risks for themselves and their loved ones. The public interest override is an important tool that any modern government should seriously consider in appropriate circumstances to foster openness and transparency.

Conversations about people, privacy, and access to information

In 2021, the IPC launched a successful new podcast called ***Info Matters*** aimed at educating the general public about privacy and access to information issues that matter to them. We dedicated several episodes to our strategic priority of advancing privacy and transparency in a modern government.

For example, ***Demystifying the FOI process*** explores the essential function of access to information in maintaining a healthy democracy. We walk listeners through the very practical steps of making a freedom of information request and filing an appeal with our office to obtain records they believe they are entitled to.

From FOI to front page news! delves into the critical role of journalists and how they depend on freedom of information to uncover details about government decisions and actions, and report about them, as a way of upholding transparency and accountability and keeping the public informed.

In ***First Nations data sovereignty***, we focus on the importance of respecting data sovereignty among First Nations peoples as part of the journey toward reconciliation. We discuss how the principles of data ownership, control, access, and possession (OCAP) promote the ethical use of data about First Nations, by First Nations, and for First Nations, to effect positive health and social change.

INFO MATTERS

Children and youth in a digital world

Today's children and youth are growing up with much more technology than previous generations. They're more connected, often at younger ages, and spending more time online sharing increasing amounts of personal information. Over the past decade, there has been growing recognition and concern that children's privacy, autonomy, and well-being are increasingly at risk in the evolving digital world.

That's why the IPC selected ***Children and Youth in a Digital World*** as one of our strategic priorities. Our goal is to champion the access and privacy rights of Ontario's children and youth by promoting their digital literacy and the expansion of their digital rights while holding institutions accountable for protecting the children and youth they serve.

To support this goal in 2021, we focused on promoting digital literacy among children and youth and ensuring that institutions understand their obligations when handling young people's personal information.

Standing up for children's digital rights

The IPC worked with the Global Privacy Assembly, an international forum for data protection and privacy authorities, to co-sponsor and adopt a **resolution** on children's digital rights. The resolution builds upon established international conventions and the work of leading data protection authorities. It's aimed at promoting children's

ability to exercise their fundamental rights in a digital environment where personal data is increasingly being processed and commercially exploited.

The resolution represents an acknowledgement by the IPC, together with the global community, that policies relating to children's digital rights must take into account their best interests and evolving capacities. They must strike an appropriate balance between accommodating children's emerging autonomy to take full advantage of the benefits of a digital environment, while also protecting children from privacy risks they may be less aware of and to which they are particularly vulnerable.

By co-sponsoring the resolution, the IPC committed to promoting the digital rights of children and youth in Ontario, working in collaboration with stakeholders, policy makers, and other data protection authorities.

Protecting student privacy rights in Ontario schools

In time for back-to-school, the IPC launched a webinar for Ontario educators about **protecting student privacy rights** to add to our already extensive collection of privacy guidance and lesson plans for schools, teachers, and parents.

Ontario's municipal privacy law, MFIPPA, requires public school boards and schools to ensure that online tools and data management systems protect students' personal information. Despite this obligation, it is not unusual for the IPC to hear from concerned parents and guardians about the adequacy of privacy and security measures in their kids' schools.

To help schools navigate this tricky terrain, support their compliance efforts, and maintain parents' and students' trust, the webinar offers a refresher on MFIPPA requirements. It also includes details about IPC-led investigations into the use of cloud-based data management systems and third party data processors by some of the largest public school boards in the province. Additional details about these investigations are summarized on page 33.

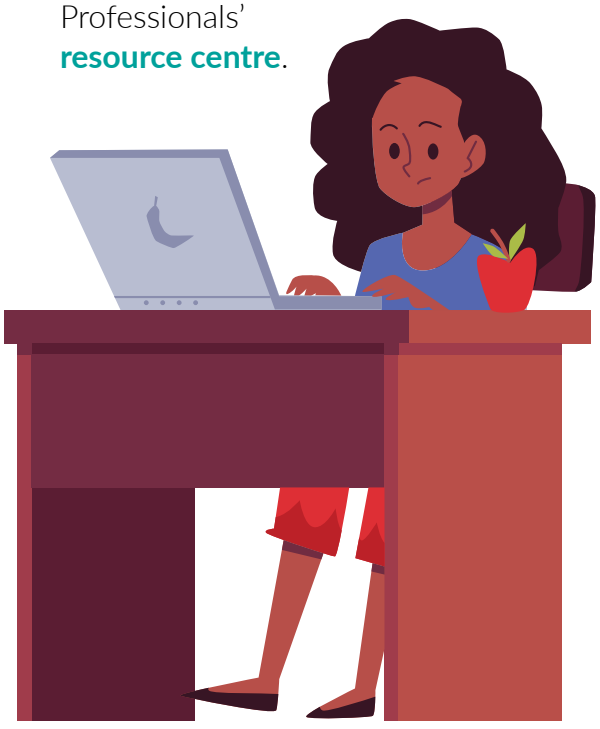
COMMISSIONER'S RECOMMENDATION

Digital technologies offer undeniable opportunities for young people to connect, learn, and collaborate in ways that simply didn't exist before. While the online world provides many benefits, it also comes with real world safety and privacy risks. It is essential to equip children and youth with the skills to navigate the digital environment safely and ethically. This includes a solid understanding of their privacy rights, taught as part of the Ontario primary and secondary school curricula.

Privacy Pursuit! Games and Activities for Kids

In 2021, the IPC launched a fun new resource for children, ***Privacy Pursuit! Games and Activities for Kids***.

Privacy Pursuit! is a kid's activity book designed to help children learn about online privacy through play. It features games like word searches, crossword puzzles, cryptograms, and word matches, among other activities. The activity book provides easy-to-understand tips to help kids identify scams, protect their privacy, and stay safe online. Thought-provoking questions also guide kids through a process of self-discovery, encouraging them to reflect on what privacy means to them and how to respect the privacy of others through caring and empathy. This new resource was provided to school boards, parent associations, and child and family service providers across Ontario. It was also shared with the YMCA and Boys and Girls' Clubs of Ontario, and featured on the International Association of Privacy Professionals' **resource centre**.



First decisions under Part X of CYFSA

In 2021, the IPC issued its first decisions under Part X of the *Child, Youth and Family Services Act* (CYFSA), which took effect in January 2020. Part X of the CYFSA protects the privacy rights of children and youth in care and grants them the right of access to their personal information from their service providers, subject to certain exceptions. These first CYFSA decisions set down important precedents by determining what constitutes the provision of service covered by Part X and defining the scope of adoption records excluded from the act.

Descriptions of these decisions are available on page 35.

Advocating for children's data rights in the private sector

Ontario's ***White Paper on Modernizing Privacy in Ontario*** proposed a private sector privacy law that would include special protections to guard against potentially dangerous data practices targeting children. Proposed safeguards include introducing a minimum age of valid consent and prohibiting organizations from monitoring children to influence their decisions or behaviour.

In our **submission** to the government, the IPC applauded the government's proposal to address important issues such as substitute decision-makers and the minimum age thresholds for valid online consent in an Ontario private sector privacy law. We recommended several further enhancements, including the right for youth to have the information they've posted about themselves

de-indexed, removed or deleted altogether, subject to narrow exceptions, and the right for mature minors to object to their parents' consent, access or take down requests.

Never before has the need for statutory protections for children's privacy been so critical. This is particularly the case in the private sector where organizations aim to collect and commercialize children's personal information for profit. Some organizations are even turning to surveillance technologies surreptitiously embedded in games and toys to monitor children's voices and actions. Others are increasingly deploying artificial intelligence tools to segment children into different target audiences and influencing, if not nudging, their behaviour in potentially adverse ways. We urge the government to continue the important conversation that has been started around the critical need for a made-in-Ontario private sector privacy law to fill current statutory gaps left behind by the constitutional limits of a federal law.

COMMISSIONER'S RECOMMENDATION

In today's increasingly digital landscape, it is more important than ever to have modern, efficient, and effective laws in place that provide enhanced privacy protections and better align with our province's unique values, realities, and culture. The time has come for Ontario to fill important gaps in its existing legislative frameworks and integrate privacy protection across its public, private, and health sectors. The government's consultations on a made-in-Ontario private sector privacy law were promising, but efforts must continue to leverage the momentum toward stronger and more integrated privacy protection for all Ontarians.

Helping children and teens understand their privacy rights was a hot topic on the ***Info Matters*** podcast in 2021. ***Teaching kids about privacy*** provides parents and teachers with tips and resources to explain the importance of privacy to kids in a way they can understand from a very young age. ***Teenage confidential: Teens, technology, and privacy*** explores some of the ways teens are using online technologies and how parents can help them navigate the digital world safely and ethically.

Trust in digital health

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

We undertook several initiatives in 2021 to further our progress toward achieving this goal.

COVID-19 proof of vaccination

Ontarians' trust in their digital health system was certainly tested throughout 2021 as the pandemic continued to wreak havoc on their lives. The IPC provided feedback and guidance focused on ensuring that appropriate privacy and

security safeguards were considered during the development and implementation of the government's mandatory proof of vaccination certificate program. The IPC's guidance was founded on the privacy principles set out in the federal/provincial/territorial privacy commissioners' 2021 joint statement on privacy and COVID-19 vaccine passports.

In addition to reviewing and commenting on a broad range of government documents, including several privacy impact assessments, the IPC recommended that the program be restricted to specific purposes that meet necessity, effectiveness, and proportionality tests. The IPC also recommended that only as much personal information be collected, used, or disclosed as is needed to achieve the intended purpose of curbing the spread of COVID-19. We also advised that the proof of vaccination certificate program should end once the program no longer meets the public health purpose of curbing the spread of the virus.

Virtual health care

Virtual health care, accelerated by the pandemic, is here to stay. In February, the IPC released new guidelines, ***Privacy and Security Considerations for Virtual Health Care Visits***. Our guidance highlights the key elements of virtual health care that health information custodians must consider — with a reminder that Ontario's health privacy law, the *Personal Health Information Protection Act* (PHIPA), applies to virtual care as it does to in-person care.

The guide outlines some key requirements of PHIPA (for example, data minimization and safeguards) relevant to all custodians, including those providing health care in a virtual context. It recommends steps for custodians to enhance privacy and security in virtual health care, including privacy impact assessments, staff training, vendor selection, consent, and technical, physical, and administrative safeguards for providing virtual care visits. The guide also has specific advice on additional safeguards needed to address privacy risks associated with email and video conferencing.

The *Info Matters* podcast episode ***Putting patient trust at the centre of virtual health*** explores the unique privacy and security considerations when using digital technologies to provide virtual health care, and what individual health providers and patients need to know when communicating through digital means.

Digital health

In May, we released ***Digital Health under PHIPA: Selected Overview***. This guide conveniently brings together in one document a number of recent legislative and regulatory changes to PHIPA that have been made to facilitate digital health in Ontario. These amendments — some of which are not yet in force — set out new requirements concerning:

- The Electronic Health Record (EHR), a province-wide system maintained by Ontario Health
- Interoperability of digital health assets of custodians
- Electronic audit logs that custodians will be expressly required to maintain
- Consumer electronic service providers (e.g., health apps)
- An individual's right to access records in electronic format that meets prescribed requirements

These changes are in addition to earlier amendments made to PHIPA in 2020, ushering in administrative penalties that have yet to come into force. The IPC provided recommendations on the possible content of regulations to support the implementation of administrative penalties. We continue to urge the government to press forward with these important changes to support Ontarians' trust in digital health care by providing them with assurances that egregious privacy violators will be effectively sanctioned and others will be seriously deterred from doing the same.

To mark **Digital Health Week**, we released a special *Info Matters* podcast focused on digital health transformations in large health care settings. ***From the bedside to the board: Building a culture of privacy and security in health institutions*** explored how C-suite executives and boards of large hospitals must work together to set the right tone from the top. A culture of integrated privacy and security is essential for building effective governance programs to oversee major digital health investments, minimizing risks to patients' privacy, and ultimately enhancing the patient-centred experience.

COMMISSIONER'S RECOMMENDATION

In 2020, significant amendments to PHIPA were introduced and came into force, but will only take effect at a future date, pending the adoption of regulations. One such amendment sets out the IPC's powers to impose administrative monetary penalties directly against individuals and organizations for serious breaches of Ontario's health privacy law. The details of the administrative penalty scheme must be set out in regulations without further delay so the IPC can begin to impose real consequences on the few bad actors who undermine the confidence of Ontarians in the entire health system.

Data sharing for the public good

Throughout the pandemic, our office received many calls and emails from the public and the media about the level of information public institutions could or should release to keep Ontarians safe.

Our response emphasized that Ontario's privacy laws do not prevent health authorities from sharing as much non-personal information as is necessary to protect public health without identifying individuals. Given the level of public interest and the need for enhanced transparency during the pandemic, we issued guidance to clarify the current provisions of Ontario's health privacy law that allow for certain exceptional disclosures for public health purposes.

In July 2021, we issued the publication ***Use and Disclosure of***

Personal Health Information for Broader Public Health Purposes. The guide describes how PHIPA allows personal health information to be used or disclosed for purposes beyond the immediate patient-provider relationship.

These broader permitted purposes include:

- conducting research subject to conditions that reflect a balance between the public benefit and individual privacy
- planning, evaluating, and managing the health system by allowing the disclosure of personal health information to prescribed entities, such as the Canadian Institute for Health Information, for analysis and compiling statistical information
- maintaining a registry of personal health information to improve the provision of health care by allowing the disclosure of personal health information to a prescribed person, such as the Ontario Institute for Cancer Research, to maintain a registry of personal health information for purposes of facilitating or improving the provision of health care
- protecting and promoting public health where, for example, personal health information may be disclosed to a medical officer of health for the purposes of preventing the spread of disease or disclosed to others if there are reasonable grounds to believe it is necessary to eliminate or reduce a significant risk of serious bodily harm

Data sharing is crucial for an effective COVID-19 response plan and for addressing other urgent public interests. Sustaining the trustworthiness of these initiatives requires establishing robust and effective privacy and data security safeguards. To this end, the IPC co-sponsored an international **resolution on data sharing for the public good** that the Global Privacy Assembly unanimously adopted in October 2021. The IPC is a member of a working group that will seek to identify practical approaches to sharing and using personal data to enable innovation and growth while protecting individual rights and promoting public trust.

Initial review of Ontario Health as a prescribed organization

In 2021, the IPC completed the initial review of Ontario Health as a prescribed organization under PHIPA, marking an important milestone in the province's efforts to develop a provincial electronic health record system. As a prescribed organization, Ontario Health has the power and duty to develop and maintain the electronic health record for the province under Part V.1 of PHIPA and **Ontario Regulation 329/04**. Following an iterative review process, the IPC issued a **report** that summarizes the review and a **letter** approving the practices and procedures of Ontario Health as a prescribed organization. Ontario Health will continue to consult with the IPC in 2022 to address the recommendations described in the report and approval letter.

Consultation on three-year reviews under PHIPA

Every three years, the IPC reviews the practices and procedures of other prescribed entities and prescribed persons who are entrusted with large volumes of personal health information and have significant roles and responsibilities delegated to them under Ontario's health privacy law. The purpose of the review and approval process is to ensure their practices and procedures protect the privacy of individuals whose personal health information they receive and maintain the confidentiality of that information in accordance with PHIPA. This is a unique mechanism to provide entrusted organizations with greater day to day flexibility to process personal health information without consent for public good purposes, subject to closer regulatory scrutiny of their practices and procedures once every three years.

In 2021, the IPC engaged in extensive consultations with relevant stakeholders to revise, streamline, and modernize the three-year review process and update the ***Manual for the Review and Approval of Prescribed Persons and Prescribed Entities***. The intention is to move towards a more efficient and meaningful review process based on areas of greatest risk. We will report on the results of our consultation in 2022.

Next-generation law enforcement

Our goal in this priority area is to contribute to building public trust in law enforcement by working with relevant partners to develop the necessary guardrails for the adoption of new technologies and community based approaches[1] that protect both public safety and Ontarians' access and privacy rights.

To support this work, we kicked off 2021 with a Privacy Day **webcast** about law enforcement and surveillance technologies, bringing together leaders from law enforcement, access and privacy law, human rights, academia, and the media to discuss this important and timely issue. The panelists provided an array of insights and unique perspectives on the use of these technologies, emphasizing the vital role that accountability and transparency must play to build and maintain public trust in law enforcement.

Law enforcement agencies are increasingly turning to surveillance technologies to improve operational efficiencies and enhance public safety. The question is how to ensure law enforcement uses these new technologies appropriately — with transparency, accountability, fairness, and privacy considerations embedded in the policies and procedures governing their use.

1 We added "community based approaches" to this priority in 2021 to reflect the fact that innovative data-centric approaches to policing do not always involve new technologies.

Police body-worn camera programs

Building on the knowledge and experience gained through our consultations with the Toronto Police Service on their body-worn camera (BWC) program, in July 2021, the IPC released a **model governance framework** for the use of BWCs by police.

The framework is designed to help Ontario's police services design effective BWC programs that support public safety objectives while respecting the fundamental rights of individuals and communities.

Specifically, the governance framework aims to enhance transparency and accountability of police-civilian encounters — including with respect to the use of force by police — while at the same time respecting the public's reasonable expectations of privacy, fairness, and access to information.

The model governance framework will aid Ontario's police services as they plan and implement their BWC programs to ensure a consistent level of rights protection across the province in accordance with Ontario's access and privacy laws.

Use of facial recognition technology by police

In 2021, the IPC, together with its federal, provincial, and territorial (FPT) counterparts, released draft **guidelines** for the use of facial recognition technology by police, calling for public and stakeholder input.

While **facial recognition technology** offers Canadian law enforcement agencies the enhanced potential to solve serious crimes and find missing persons, it also has the potential to be highly intrusive unless clear legal controls and effective privacy protections are in place.

In response to the FPT consultation on the draft guidelines, we received highly valuable submissions from a broad range of stakeholders. Our office also brought together representatives from police services, academia, government ministries, and civil society groups, among others, for a roundtable discussion to receive feedback on Ontario-specific issues. These discussions raised important issues that we continued to work through in consultation with federal, provincial, and territorial privacy authorities with a view to finalizing the guidelines and accompanying policy framework in 2022. We will report on the results of this initiative in our next annual report.

Speaking out about the expansion of closed-circuit television systems

In July, the IPC issued a **response** to the Ontario government's funding announcement of $2 million to expand the coverage of closed-circuit television (CCTV) systems across the province.

CCTV camera systems may be effective in helping deter or detect crime and potentially provide evidence for use in criminal investigations. However, when taken too far, video surveillance footage can often capture the personal information of people in Ontario just going about their everyday lives, and can create a chilling effect on freedoms and liberties.

The IPC strongly encouraged police services or municipalities considering implementing or enhancing CCTV camera systems to consult with the IPC to ensure appropriate policies, procedures, and training are in place to safeguard the personal information they collect.

New community based approaches to policing

In 2021, the IPC worked collaboratively with various organizations on new community-based police initiatives to contribute to building public trust in law enforcement.

As a member of Toronto's Police and Community Engagement Review (PACER) committee, the IPC provided input on the development of the Toronto Police Service's *Know Your Rights* **video**. The video aims to educate the public about their rights and police officer's responsibilities when it comes to police-civilian encounters associated with carding, informal interactions, Ontario's street check regulation, and the *Trespass to Property Act*.

Through its work with the Provincial Human Resources and Justice Coordinating Committee, the IPC provided input on a framework and toolkit for mobile crisis response teams expected to be released in 2022. These teams involve police officers and crisis workers working together to respond appropriately and sensitively to an addiction, mental health, neurodevelopmental or other crisis situations where police have been called.

In episode six of the *Info Matters* podcast, ***Building privacy and transparency into sexual assault investigations*****,** we inform listeners about an innovative approach to investigating crimes involving sexual violence. It embeds community experts into the investigative process to improve outcomes for complainants and enhance the transparency and accountability of police decisions. The program is intended to increase chances that reported cases of sexual assault will result in charges being laid, encouraging sexual assault victims to report cases while also protecting their privacy.

RESPONDING TO COMPLAINTS AND APPEALS IN A FAIR, TIMELY, AND MEANINGFUL MANNER

Throughout the year, the IPC initiated efforts to review its current tribunal dispute resolution processes with a view to enhancing internal efficiencies and reducing timelines for responding to Ontarians' complaints and appeals. This is a multi-year effort, which began in earnest in 2021 and will continue to be reported on next year.

Backlog reduction project

As a result of the pandemic, IPC staff transitioned to working from home. During the time it took for our office to acquire the infrastructure and create the processes necessary to work from home securely, our tribunal could not operate as usual.

This disruption caused a delay in processing files, resulting in a backlog at the early resolution and mediation stages as we received new requests for our services. In 2021, the IPC undertook a targeted effort to clear this backlog, hiring temporary staff and streamlining processes resulting in a 92 per cent reduction in backlog files at the

conclusion of the project. Remaining files continue to be reviewed and processed mainly using existing IPC resources, and have been prioritized for completion as appropriate.

The success of this project provided a unique opportunity to test process changes and improvements that we have adopted on a broader, more permanent basis. Building on this momentum, the IPC is undertaking a lean process review in 2022 to drive continuous improvement in the delivery of tribunal services to the people of Ontario.

Enhanced customer service

In 2021, we implemented a few organizational changes with the aim of improving customer service. This included creating a new registrar position to support the more rapid intake, processing, and oversight of incoming appeals and complaints. This position helps ensure that, despite the challenges of working through the reduction of the backlog, Ontarians could continue to rely on the tribunal to begin processing their files and addressing their concerns in a timely fashion.

Similarly, the tribunal established the tribunal information officer position to support the registrar and directly respond to questions and concerns of Ontarians regarding their submitted appeals and complaints. This role provides a one-stop service person for Ontarians to contact regarding questions or concerns they may have about the status of their files and how their files are being handled.

Capacity building

Our tribunal mediators continued to hone their skills by taking courses to assist them in diffusing difficult situations. This allows our mediators to have the most up-to-date, world-recognized training to successfully address the most difficult scenarios and situations that complainants bring to the IPC. Many of our staff also took project management courses in 2021, setting the foundation for the numerous large projects and initiatives that the IPC has planned for upcoming years, such as the lean process review project.

Through two virtual conferences with our federal, provincial, and territorial counterparts in 2021, our tribunal investigators were able to learn new investigative techniques and, in turn, share their knowledge and experience with other investigators throughout Canada. This provided an important opportunity to improve service delivery to Ontarians through the exchange of different ideas and perspectives, resulting in the implementation of new investigatory methods and best practices.

Notable tribunal trends

Throughout 2021, the IPC's tribunal services team observed a few notable trends across the complaints and appeals that came into the office.

Cyberattacks on the rise

While the COVID-19 pandemic slowed down almost every aspect of our society, cybercriminals **were busier than ever** in 2021. This is part of a global trend in the rise of cybercrime, particularly an increase in ransomware attacks worldwide.[2]

In the health sector, 24 health privacy breaches reported to our office through statistical submissions[3] were due to cyberattacks, double

2 Canadian Centre for Cyber Security, "**Cyber threat bulletin: The ransomware threat in 2021**" (December 9, 2021)

3 Full details available in the IPC's ***2021 Statistical Report***

the number of cyberattacks reported to us in the previous year.

Other large public institutions and critical infrastructures were also a prime target. A 2021 **cyberattack** affecting municipalities in Ontario was connected to the Accellion file transfer software, a legacy product linked to breaches in organizations around the world as part of a massive spree of cyberattacks.

Our **review** of a privacy breach at the Regional Municipality of Durham relating to the use of this Accellion software found that the municipality had a number of reasonable safeguards in place to help protect its networks from cyber breach of this nature. However, more needed to be done to detect and manage future cybersecurity incidents. Our recommendations included putting in place logging requirements for monitoring and detecting security events to raise the alarm at the first sign of trouble.

Municipalities and other government organizations are particularly attractive targets for attackers as their systems are storehouses of sensitive information used to provide a range of vital services to communities. A breach of such sensitive personal information can have devastating impacts on those affected. Public institutions need to be mindful that they are ultimately responsible for continually monitoring their systems to ensure that any personal information in their custody and control is secure and protected. Outsourcing data management services does not relieve public sector organizations of accountability for protecting personal information.

The attack serves as a cautionary tale for all organizations to ensure their software is up to date and that measures are in place to vigilantly monitor computer networks for abnormal activity, often the first sign of large-scale data theft. These systems need to be continually updated to ensure they meet security industry standards and best practices.

Employee snooping continues to undermine trust

While the increased use of digital tools requires enhanced privacy and security measures to guard against sophisticated cyberattacks, other distinctly human factors also contribute to breaches, particularly in the health sector.

Reports to our office in 2021 reveal that snooping by health care workers accounted for 21 per cent of self-reported health privacy breaches. This is slightly higher than the number of reports we received in 2020, indicating there is still work to be done.

Whether out of curiosity, personal gain or simple concern about the health of friends and family, **snooping** through medical records can have devastating consequences for patients, health professionals, and the health system as a whole. It's time to curb health privacy breaches by stamping out snooping once and for all.

Misdirected emails and faxes continue to be a problem

Misdirected emails continue to be a common source of privacy breaches, resulting in the unauthorized disclosure of personal information. In the health sector, the number of breaches resulting from

these incidents has continued to grow from just over 430 in 2018 to nearly 1,200 in 2021 — a 271 per cent increase in that time period.[4]

The IPC routinely receives calls from the media and the public about breaches of personal information due to **misdirected emails**. In 2021, we were informed of a breach involving a mass email sent with the email addresses in the carbon copy (CC) field instead of the blind carbon copy (BCC) field. This resulted in the disclosure of not only names and email addresses, but also the individuals' health status. Another incident related to the vaccination status of staff members who received a group email reminding them of the importance of getting vaccinated or undergoing regular antigen testing if they weren't already fully vaccinated. Other incidents involved unencrypted documents containing the personal information of individuals sent to mass email lists as attachments.

While these kinds of breaches can often be attributed to simple human error, they serve as a reminder to every organization of how important it is to have explicit policies and administrative safeguards in place when handling the personal information of individuals. Employees need to be trained and reminded to be acutely aware of potential privacy risks and follow proper policies and procedures to avoid privacy breaches. This includes being vigilant about how they format people's personal information before pressing send on an email.

In addition to email errors, the IPC continued to see a seriously troubling number of incidents related misdirected faxes as many custodians unfortunately insist on prolonging this outdated mode of communication. In

> It is high time for all custodians to phase out their dependence on fax machines and to encrypt email communications in service delivery. More modern and trusted communication methods are now reasonably affordable and amply available. As technologies evolve, so too should our response to privacy risks.

4 Full details available in the IPC's ***2021 Statistical Report***

2021, 4,848 health information privacy breaches were due to misdirected faxes.

Managing third party processing risks

Some digital and online service delivery platforms are designed, built, and operated by third parties on behalf of government institutions and organizations.

Even though these activities are handled by a third party, institutions are still ultimately responsible for identifying and managing the risks arising from these outsourcing arrangements. This includes ensuring that robust contractual provisions are included in the agreement between the institution and the third party processor to bind the third party processor to the same obligations expected of the institution to protect personal information in accordance with Ontario's privacy laws. In addition, it means ensuring that the institution has effective mechanisms in place to monitor the third party's compliance with the terms of the agreement, including through effective oversight, such as regular review, reporting, and auditing functions.

In 2021, the IPC conducted three privacy investigations in response to complaints about the use of **online educational tools and services** by Ontario school boards. More details about these investigations are available on page 33.

Access and compliance trends

In 2021, 55,578 freedom of information requests were filed across Ontario. This was a more than a 26 per cent increase from the previous year, representing a near return to 2019 pre-pandemic levels.

Compliance rates, in terms of percentage access requests completed within 30 days, continued to vary by sector. For provincial institutions, only about 64 per cent of access requests were completed within 30 days, representing a decrease of three per cent from 2021. Municipal institutions recorded an 80 per cent compliance rate, increasing the number of access requests completed within 30 days by two per cent from 2020. The health sector achieved an impressive 92 per cent compliance rate, completing the majority of requests for access to, and correction of, personal information in 30 days.

An overview of 2021 tribunal statistics is available on page 49 of this report. A full breakdown of all statistics submitted to the IPC is available in the IPC's ***2021 Statistical Report***.

MAINTAINING ORGANIZATIONAL EXCELLENCE AND ACCOUNTABILITY

Responding to current and future challenges

As an independent office of the Legislative Assembly of Ontario, the IPC is committed to the highest standards of organizational excellence and accountability. Strong, evidence-based fiscal planning, performance analysis, and enterprise risk management are critical components of organizational success, ensuring effective outcomes and value for public funds. In 2021, the IPC took steps to strengthen its accountability and management infrastructure to ensure more strategic and efficient deployment of our financial, human, and technology resources now and into the future.

Investing in our people

Our office recruited a new chief financial officer (CFO) and director of corporate services as part of our diverse and inclusive leadership team. The CFO position required recruitment of an individual with a chartered professional accountant designation to ensure effective oversight of the IPC's resources and robust financial controls.

The IPC's corporate services were further enhanced with the recruitment of a

specialized human resources manager to develop a modern and integrated human resource plan for the organization. This includes a robust performance management program, training and capacity building in key areas, employee engagement tools and initiatives, as well as a diverse recruitment and succession planning strategy that supports inclusion, diversity, equity, and accessibility. Continuous knowledge transfer is another key corporate priority to help ensure a sustainable and successful future for the organization.

In 2021, the IPC also added an information technology officer to the corporate services team. As staff continued to work from home, additional support for our virtual workforce was crucial. The information technology officer responds to daily troubleshooting requests from staff to enhance efficient operations remotely. They also help maintain the security of our systems by regularly monitoring for software vulnerabilities, taking necessary actions to apply essential upgrades and patches, and supporting regular training to raise employee awareness of threats and minimize cybersecurity risks to our IT systems.

Data is a valuable asset to any organization to support evidence-based decision-making and a robust management and accountability infrastructure. In 2021, the IPC recruited a corporate data analyst to provide the relevant data analyses and insights to support fiscally responsible decisions and informed allocation of financial and human resources. As part of this work, the IPC is moving forward with the development of performance indicators to support the evaluation and reporting of performance outcomes.

Our office engages in many complex technology consultations with organizations from Ontario's public, health, and education sectors seeking our guidance on the use of cloud-based technologies and digital platforms to enhance service delivery and protect against the growing risks of cyberattack and ransomware. Technical knowledge is also an indispensable part of our increasingly complex investigations into privacy complaints involving cloud services, digital platforms, and third party technology service providers. To support our work in this area, in 2021, we recruited two new senior technology advisors as part of our policy team to provide in depth technology expertise and advice.

As part of its investments in people, all IPC staff completed Sanya's Indigenous Cultural Safety Training to increase knowledge, enhance self-awareness, and support positive partnerships with Indigenous people accessing our services. Staff providing tribunal services participated in situational training to enhance their interactions with the public. Members of the executive also completed structured project management training to enhance project efficiency, timeliness, consistency, and management of financial and human resources.

Digitizing our services

The government's move toward enhanced digital services, accelerated by the pandemic, has also increased demands on the IPC's own capacity to become more digitally accessible to Ontarians and provide more efficient services online. In 2021, the IPC successfully introduced a secure process to transmit and receive documents electronically. This secure document exchange process greatly minimized service disruptions during the pandemic. Efforts were also made to modernize and improve our website to support current and future digital service delivery to Ontarians. More website upgrades are expected in 2022, including the launch of a new online payment system that will make it possible for Ontarians to file appeals and pay associated fees online.

Securing our information systems

Given the concerning risks of cyberattacks and ransomware during the pandemic, the IPC took proactive measures in 2021 to enhance its own security posture and ensure systems were well protected from any external threats. Three organizational threat risk assessments were undertaken to analyze our security infrastructure environment, including IT operations, core business processes, and communication collaboration tools. These risk assessments provide a roadmap for the IPC to mitigate any potential infrastructure vulnerabilities and will inform future opportunities for the organization to modernize its work environment to support the move towards more digitization.

Preparing for a new future of work

The IPC is committed to ensuring the health, safety, and well-being of its employees as we gradually return staff to the office in some form of hybrid work arrangement. We are also committed to providing a modern and flexible physical environment that is adaptive to the changing needs and expectations of existing and future employees who have grown accustomed to working from home, and are generally happier with the work-life balance offered by some form of hybrid work arrangement. Throughout 2021, our efforts continued to focus on building an agile and modern workplace that aligns with our future of work strategy. We worked to actively nurture a renewed sense of community and organizational culture as part of the new normal, and ensure staff have the physical, technical, and administrative supports needed to thrive as key contributors to the IPC's success. We will report further on the development and implementation of our future of work strategy in our next annual report.

IPC BY THE NUMBERS

Website visits
156,000+

YouTube video views
16,100+

Responses to Info@IPC public inquiries
9,600+

Commissioner's blogs
18

Info Matters podcast downloads
3,376

Consultations with stakeholders
41

Media mentions
430

Media

Media statements
73

Submissions to government
14

Legal hearings
3

Guidance publications
7

Judicial review files heard or closed
2

UPHOLDING ONTARIANS' RIGHTS

Openness and transparency are essential to maintaining the public's trust and confidence in government institutions. A vital element of the IPC's mandate is to resolve access to information appeals under Ontario's access and privacy laws.

Early resolution
The early resolution team has the delegated authority and responsibility to attempt to resolve appeals, complaints, and self-reported breaches right up front, in the most expedient manner possible. In 2021, the early resolution team successfully resolved more than 50 per cent of all IPC files across all sectors. Here are a few examples of their critically important work.

The snooping pharmacist
A pharmacy department discovered that an employee had inappropriately accessed 68 patient records while without any justified professional reason for doing so. The breaches were discovered through audit reports generated from the pharmacy's electronic health record system. The pharmacy reported the breach to the IPC and notified all patients and affected parties. The pharmacist was reported to their regulatory college and their employment was terminated.

Inappropriate changes to patient file
A staff member at a medical clinic inappropriately accessed their relative's health record, changing key information in the patient file to enhance the prospects of their insurance claim. A doctor at the clinic discovered the breach when they could not retrieve the patient's electronic health record. The staff member was fired from their job. The IPC advised the clinic to make significant improvements to its privacy program, including comprehensive privacy training and confidentiality agreements for staff. The IPC also recommended the clinic conduct regular audits of its electronic health records system to monitor more closely for any unauthorized access to patient files in the future.

Giving out the information of others

An individual requested their medical chart from a records storage company. They received their personal health information as well as the information of three other individuals. The IPC investigated the breach and recommended the company update its procedures for processing access requests. We also recommended that all staff receive additional privacy training to emphasize the importance of safeguarding personal health information and to reinforce their obligations under Ontario's health privacy law.

Responding to a ransomware attack

A pharmacy reported a ransomware attack that locked staff out of 500 to 750 patient records. The IPC worked with the pharmacy to ensure it took reasonable steps to contain the reported breach, notify the patients, and prevent future occurrences. In addition to providing cybersecurity training for staff, the pharmacy put in place additional safeguards, including upgrades to its file backup system, firewall, and antivirus software.

Best practices when selling a dental practice

A patient informed the IPC that their former dentist sold and disclosed their personal health information to the new owners of a dental practice. The IPC contacted the new owners and advised them of best practices for transferring patient information. The new clinic owners posted a public notice informing patients of the change of ownership and the transfer of their personal health information from their former dentist.

UPHOLDING ONTARIANS' RIGHTS

Mediation

When access appeals cannot be closed at early resolution, our team of trained mediators works to actively resolve or narrow the issues between the parties with a view to finding a mutually agreeable solution. This typically involves listening to each side and relaying the perspective of each party to the other in a manner that seeks to find common ground or acceptable compromise. When appeals are resolved or partly resolved at mediation, this results in fewer cases going forward to formal adjudication, which can be a much longer, more labour-intensive and expensive process. Here are a few examples of cases successfully resolved through mediation in 2021.

Providing families with emotional closure

A sibling sought access to video footage capturing their brother's final moments after being found in a non-responsive state on a zip line. Initially, the individual was denied access to the video footage on the grounds that it contained personal information. The IPC discussed the compassionate grounds provisions of the act with officials who then agreed to release the video to the appellant. The IPC mediator also arranged for the chief of police to be available to answer the family's questions about the incident. The police chief spent two hours with the family, helping them better understand what happened to their loved one.

Remediating the environment

City officials requested environmental information from a ministry about properties close to a city water well they wanted to rehabilitate. The well had been shut down decades earlier after it was contaminated with a known carcinogen, suspected to have come from industrial work on nearby properties owned by private companies. Through an IPC-led mediation, the requested records were disclosed to the companies, and the ministry agreed to provide the records to the city so they could develop solutions to restore the well.

Helping trace and heal from the past

A requester wanted access to records from the early 1980s relating to abuse in a foster home where the requester had been placed by a children's aid society. The children's aid society could not locate any records related to the abuse. During mediation, the requester provided names and dates to help locate the records. The children's aid society provided the information to the Archives of Ontario, where the records were located and provided to the requester.

Finding resolution through compassion

A father sought access to police records related to his daughter's death and was granted partial access. When his request for additional records was denied, as they contained personal information of the deceased, he filed an appeal with the IPC. Following discussions with an IPC mediator, the police service agreed to speak directly with the requester to answer his questions about the records. The police also released additional information to him on compassionate grounds.

Correcting errors that could have adverse consequences

A patient requested a hospital remove references to two medical conditions that were incorrectly added to their electronic health record and were affecting their insurance coverage. The hospital advised the patient that a note stating they did not have the conditions was scanned into their record. The patient complained to our office, unsatisfied with the correction, which didn't acknowledge the hospital's initial error. During mediation, the hospital agreed to make the correction to the record and remove the scanned note.

UPHOLDING ONTARIANS' RIGHTS

Privacy investigations

Our team of investigators gathers information and resolves privacy complaints, and investigates privacy breaches. Following their investigation into a privacy matter, IPC investigators issue recommendations to the institution or organization that are most often accepted and adopted. These are some of the privacy complaints our office investigated in 2021.

Accessing patient records for educational purposes

PHIPA Decision 168

A medical resident, who was also a patient, withdrew consent for a hospital to use their personal health information for educational purposes under the hospital's policy. Believing other residents were accessing their health records without authorization, they filed a complaint with the IPC. The IPC examined the hospital's practices for the use of personal health information for educational purposes and provided recommendations on how it could improve them. These included amending the hospital's information practices to clearly and consistently state the conditions for consent and the consequences for inappropriately accessing personal health information in violation of the hospital's information practices.

Inappropriate disclosures for alleged financial interests

PHIPA Decision 147

A hospital reported a privacy breach after a patient complained their personal health information was disclosed without authorization following treatment for injuries from a motor vehicle accident. Concerns were raised regarding a "quality audit" by a physician who was allegedly referring motor vehicle accident patients to his wife, a personal injury lawyer. While an investigation was unable to conclude whether the physician had in fact inappropriately disclosed patients' personal health information to his wife, his quality audit was found to be an unauthorized use of personal health information under the act. The investigation also concluded that the hospital's vague policies, practices and procedures regarding quality audits, and the complete lack of privacy training for physicians, did not amount to taking reasonable steps to protect the personal health information within the meaning of section 12(1) of the act. In response to the breach, the hospital put in place explicit policies, practices, and procedures for quality audits and privacy training for physicians to ensure compliance with Ontario's health privacy law.

Disproportionate access to the COVID-19 web portal

PR20-00027

The Ministry of the Solicitor General reported a breach of its web portal for first responders to look up the COVID-19 status information of individuals they were responding to in the context of an emergency or other police encounter. Specifically, the ministry advised that an audit of the portal found a disproportionate number of database inquiries by police services that were conducting broad ranging community searches rather than performing a more specific search of individuals tested for COVID-19. The IPC investigation concluded that the ministry did not have adequate measures to protect personal information in the portal and did not respond adequately to the breaches at the time. The portal has since been retired.

Town of Leamington discloses complainant's personal information

MC18-23

An individual's personal information was posted on social media after an email they sent to the local municipal council about an annual motorcycle rally was disclosed to the rally's organizers. The individual wrote to the municipality suggesting it consider holding a more family friendly fun summer festival instead. The IPC found the council had breached the resident's privacy and that disclosure of the email without consent and for a purpose that was not consistent with the resident's original reason for writing was inappropriate under Ontario's municipal access/privacy law. Based on the IPC's recommendation, the municipality revised its policies and procedures for email and correspondence with its residents.

The school board trilogy

MC18-48, MC17-52, and MC18-17

In 2021, the IPC investigated three privacy complaints about the use of online educational tools and services by Ontario school boards. While each investigation differed in important ways, all three cases involved:

- school board procurement and use of cloud-based tools offered by third party private sector service providers
- use of online account-based tools and services by students, parents and guardians
- concerns from parents and guardians alleging the potential collection, use, and disclosure of students' personal information in unlawful ways

While the IPC's investigations found the school boards were generally in compliance with MFIPPA when using third party software or platforms, our office also found deficiencies and made recommendations to each of the boards, such as:

- improving public transparency of data management practices, including enhanced notices of collection to parents and students
- establishing clear privacy and security requirements, consistent with MFIPPA obligations when evaluating online educational tools and services for use
- ensuring privacy and security requirements are reflected in contractual arrangements with third party service providers, updated as services evolve, and enforced
- ensuring that vendor agreements clearly set out the use of students' personal information for educational purposes as required by the school board, and explicitly prohibiting the use of such personal information for marketing or advertising purposes

The privacy complaint reports issued in these investigations can guide school boards on the types of provisions they should seek to include in their contracts with third party technology providers. They are also a reminder that protecting privacy requires more than just having a strong contract in place — it must be coupled with appropriate monitoring and oversight to ensure compliance with the terms of the agreement.

UPHOLDING ONTARIANS' RIGHTS

Adjudication

When a resolution cannot be found through early resolution, mediation, or investigation, files are forwarded to an adjudicator who will decide whether to conduct a formal inquiry or review. The adjudicator collects and reviews evidence and arguments from the parties and issues a final and binding decision that is published. These are a few select examples of orders published in 2021.

Niagara Health System
PHIPA Decision 164

A complainant was denied access to video surveillance footage taken of them during an involuntary hospitalization. While the video footage did not include images of other patients or visitors, the hospital denied access to the footage on the grounds it could result in serious harm to staff and impact their treatment and recovery. The hospital was ordered to grant the individual access to the footage as there was insufficient evidence to indicate the footage could result in serious harm.

Ministry of the Solicitor General
PO-4190

An individual sought access to a 911 recording made by an anonymous caller related to an incident involving their spouse. The Ministry of the Solicitor General denied access to the recording claiming, among other things, the personal privacy exemption under Ontario's access and privacy laws. The IPC adjudicator found that although the call was made anonymously, the caller could be identified by their voice. The adjudicator ordered the ministry to disclose the 911 recording on compassionate grounds after distorting the voice of the anonymous caller.

Children's Aid Society of Ottawa

CYFSA Decision 2

An adoptee tracing their family history requested access to personal information and information about their birth parents from the Children's Aid Society of Ottawa. The society provided partial access to the information, redacting details that could identify the birth parents. The IPC adjudicator found that the birth parents' identifying information was subject to an exception under Part X of the CYFSA, and the requester did not have a right of access.

Children's Aid Society of Toronto

CYFSA Decision 1

A complainant, an alleged wrongdoer named in a report about a child, sought the IPC's review of a decision by the Children's Aid Society of Toronto to refuse their request for access to records of service. The society denied access to the records on the basis that they did not relate to the provision of services to the complainant, as they were not a child or a family member receiving services as defined under the act. The IPC adjudicator agreed with the society's decision and dismissed the complaint.

PUBLIC EDUCATION AND OUTREACH

The mandate of the IPC includes educating the public about their access and privacy rights under Ontario's laws and informing them about our role and activities. In carrying out this mandate, we develop practical guidance for stakeholders and general education materials for the public, as well as participate in speaking engagements throughout the year.

3,375
Downloads

7
Guidance

46
Presentations

9,600
info@ipc responses

Info Matters: A podcast about people, privacy, and access to information

In 2021, the IPC expanded its outreach efforts and took to the digital airwaves, launching ***Info Matters***, a podcast about people, privacy, and access to information. As host, Commissioner Kosseim spoke with experts about everything from avoiding online scams to navigating the access to information process and talking to kids about privacy.

Episode 1: Don't get caught! Protect yourself against phishing

Episode 2: À la rencontre des Franco-Ontariens | Reaching out to Franco-Ontarians

Episode 3: Demystifying the FOI process

Episode 4: Teaching kids about privacy

Episode 5: Putting patient trust at the centre of virtual health

Episode 6: Building privacy and transparency into sexual assault investigations

Episode 7: First Nations data sovereignty

Episode 8: From FOI to front page news!

Episode 9: Teenage confidential: Teens, technology, and privacy

Episode 10: From the bedside to the board: Building a culture of privacy and security in health institutions

INFO MATTERS

Resources and guidance

In 2021, the IPC issued a number of resources and guidance documents for stakeholders to explain their obligations under Ontario's access and privacy laws and encourage compliance. Many of these materials were tailored for general audiences, such as a special portal to provide COVID-19 related information, to explain Ontarians' access and privacy rights and how to meaningfully exercise those rights through appeals and complaints to our office. Here is a selection of IPC public education resources released in 2021.

- **COVID-19 Information and Resources**
- **Digital Health under PHIPA: Selected Overview**
- **Frequently Asked Questions: Health Cards and Health Numbers**
- **Model Governance Framework for Police Body-Worn Camera Programs in Ontario**
- **Public Interest Disclosure Under FIPPA/MFIPPA**
- **Privacy Pursuit! Games and Activities for Kids**
- **Privacy and Security Considerations for Virtual Health Care Visits**
- **Use and Disclosure of Personal Health Information for Broader Public Health Purposes**
- **Your Health Information and Your Privacy**

Presentations

Throughout 2021, the IPC accepted invitations to speak at a number of venues and conferences organized by various stakeholders across different sectors within our jurisdiction. The commissioner, assistant commissioners, legal, policy, and tribunal staff delivered keynote speeches and participated on discussion panels which, on account of the continuing pandemic conditions, occurred online rather than in person.

- York University Certificate in Information Privacy, ***Smart Cities and Privacy***, January 18, 2021, Jennifer Rees-Jones, Senior Policy Advisor
- OPTrust, ***Privacy in a Pandemic,*** January 28, 2021, Fred Carter, Senior Policy and Technology Advisor
- Osgoode Professional Development Certificate in Cybersecurity Law, ***Overview of Canadian Privacy Law***, February 2021, Dara Lambie, Legal Counsel
- Osgoode Professional Development, ***Critical and Emerging Issues in School Law for K-12 Education Professionals***, February 4, 2021, Dara Lambie, Legal Counsel
- Woman Abuse Council of Toronto, ***Exploring Legislation on Information Sharing for Organizations Supporting Women Experiencing Intimate Partner Violence***, February 10, 2021, Stephen McCammon, Legal Counsel
- Ontario Association of School Business Officials, ***Privacy in Virtual Schooling,*** February 18, 2021, Fred Carter, Senior Policy and Technology Advisor
- IAPP KnowledgeNet, ***Moving Forward at the IPC: Strategic Priorities***, February 23, 2021, Patricia Kosseim, Commissioner
- PHIPA Connections Summit, ***Balancing Risk and Compliance***, February 24, 2021, Dara Lambie, Legal Counsel
- PHIPA Connections Summit, ***A Conversation with Ontario's Information***

and Privacy Commissioner, February 24, 2021, Patricia Kosseim, Commissioner

- PHIPA Connections Summit, ***Highlights from the Latest IPC Guidance***, February 25, 2021, Debra Grant, Director of Health Policy
- Association of Records Managers and Administrators Southwestern Ontario, ***The Future of Privacy and Access,*** March 23, 2021, Renee Barrette, Director of Policy
- Osgoode Certificate in Regulatory Compliance and Legal Risk Management, ***Meet the Regulators***, March 25, 2021, Lauren Silver, Senior Policy Advisor
- Association of Native Child and Family Services Agencies of Ontario, ***Part X of the CYFSA: Reflecting on the First Year***, April 1, 2021, Renee Barrette, Director of Policy; Suzanne Brocklehurst, Director of Intake and Early Resolution; Emily Harris-McLeod, Senior Policy Advisor
- Simcoe Muskoka Family Connexions, ***Requirements under Part X of the CYFSA***, April 13, 2021, Emily Harris-McLeod, Senior Policy Advisor
- Federal/Provincial/Territorial Investigators Conference, ***Dealing with Difficult Behaviours***, April 26, 2021, Patricia Kosseim, Commissioner
- NetDiligence Cyber Risk Summit, ***Provincial Regulatory Update***, April 27, 2021, Patricia Kosseim, Commissioner
- Association of Municipal Managers, Clerks, and Treasurers of Ontario, ***A Time for Reflection and Renewal***, May 20, 2021, Patricia Kosseim, Commissioner
- Ministry of Government and Consumer Services, IPA Town Hall Forum, ***Update from the Commissioner: Moving Access and Privacy Forward***, June 1, 2021, Patricia Kosseim, Commissioner
- Future of Privacy Forum, ***Privacy in Smart Cities***, June 4, 2021, Angela Orasch, Senior Policy and Technology Advisor
- Ontario Association of Committees of Adjustment and Consent Authorities, ***Privacy and Access Rights and Obligations under MFIPPA***, June 8, 2021, Renee Barrette, Director of Policy
- Seneca@York's Post-Graduate Certificate in Government Relations, June 9, 2021, Patricia Kosseim, Commissioner
- ASIS Toronto, ***Privacy Updates for Corporate Security Professionals***, June 9, 2021, Vance Lockton, Senior Policy and Technology Advisor
- Ontario Association of School Board Officials, ***Video Conferencing and Recordings in Schools***, June 10, 2021, Fred Carter, Senior Policy and Technology Advisor
- Osgoode Certificate in Privacy Law and Information Management in Healthcare, ***Electronic Health Record Systems: ESPs, HINPs, Shared Systems and Recent PHIPA Amendments***, June 11, 2021, Brendan Gray, Legal Counsel
- 2021 Ontario Community Confab, June 21, 2021, Fred Carter, Senior Policy and Technology Advisor
- Canadian Association of Police Governance, Panel on the Toronto Police Service's Board Body-Worn Camera Policy, June 30, 2021, Stephen McCammon, Legal Counsel

- Simcoe County Clerks and Treasurers Association, ***Procurement and Privacy Legislation***, September 10, 2021, Ayesha Kapadia, Policy Analyst
- M'Chigeeng First Nation, ***Privacy Standards and Best Practices for Situation Tables***, September 22, 2021, Stephen McCammon, Legal Counsel
- Public Service Information Community Connection 2021 Right to Know Week, Commissioners' panel, September 28, 2021, Patricia Kosseim, Commissioner
- Alliance for Healthier Communities, ***Virtual Health Care***, September 29, 2021, Debra Grant, Director of Health Policy
- Privacy and Security Forum, ***Canadian Privacy Update***, September 30, 2021, Vance Lockton, Senior Policy and Technology Advisor
- Osgoode Professional Development, ***Understanding Privacy and Access in an Education Setting***, October 7, 2021, Fred Carter, Senior Policy and Technology Advisor
- Canadian Association of Counsel to Employers, ***Privacy: Looking Over the Horizon***, October 7, 2021, Patricia Kosseim, Commissioner
- Ministry of Government and Consumer Services, ***Update from the IPC: Exceptions from the Right of Access & Strategic Priorities***, October 26, 2021, Eric Ward, Assistant Commissioner, Strategic Initiatives and External Relations
- York University Professional Practice in Computing, ***Privacy Fundamentals: Technology, Public Policy, and Privacy Law in Canada***, October 28, 2021, Fred Carter, Senior Policy and Technology Advisor
- Ontario Bar Association, ***Privacy Law 2021 Update***, November 5, 2021, Patricia Kosseim, Commissioner
- Ontario Legislature Internship Programme, ***Freedom of Information and Privacy at the IPC***, November 5, 2021, Eric Ward, Assistant Commissioner, Strategic Initiatives and External Relations
- AdvantAge Ontario, ***Tribunal Processes of the IPC and Annual Breach Reporting***, November 16, 2021, Brendan Gray, Legal Counsel
- Federal, Provincial, Territorial Investigators Conference, ***Panel on AI and Investigations***, November 17, 2021, Andrew Hilts, Senior Policy and Technology Advisor
- Canadian Bar Association Access to Information and Privacy Law Online Symposium, ***The Regulators' Perspective***, November 19, 2021, Patricia Kosseim, Commissioner
- Canadian Anonymization Network, ***Perspectives for Regulating De-Identified Data in Canada***, November 24, 2021, Patricia Kosseim, Commissioner
- Municipal Internal Auditors Association, ***Cybersecurity Frameworks***, November 24, 2021, Fred Carter, Senior Policy and Technology Advisor
- Osgoode Professional Development, ***Consent, Capacity and Substitute Decision-Making Under Ontario's Access and Privacy Statutes***, December 6, 2021, Brendan Gray, Legal Counsel
- Organisation for Economic Co-operation and Development, ***Data Ethics: Balancing Ethical and Innovative Uses of Data***, December 10, 2021, Patricia Kosseim, Commissioner

ADVICE AND CONSULTATIONS

Formal advice and submissions

An important part of IPC's mandate is to offer comment on the access and privacy implications of proposed legislative schemes of government programs. We do this through formal advice and submissions in the context of public consultation processes. Here are the formal submissions made by the IPC to various standing committees, government ministries, and public institutions in 2021.

- **Letter to Toronto Police Services Board and Toronto Police Service regarding the Governance Framework for Toronto's Police Body-Worn Camera Program**
- **Letter to Melissa Kittmer regarding Proposal Number: 21-SOLGEN001 – *PRCs Reform Act, 2015*, O. Reg. 347/18 Exemptions, Exemptions Proposal**
- **Submission to the Standing Committee on Justice Policy of the Legislative Assembly of Ontario: Bill 251, the *Combating Human Trafficking Act, 2021***
- **Submission on Ontario Bill 283, Advancing Oversight and Planning in Ontario's *Health System Act, 2021***

- **Submission to the Standing Committee on Finance and Economic Affairs of the Legislative Assembly of Ontario: Bill 288, the *Building Opportunities in the Skilled Trades Act, 2021***
- **Comments on the Ontario Government's Consultation on Ontario's Trustworthy Artificial Intelligence (AI) Framework**
- **Submission to the Ministry of the Solicitor General on Regulation Registry Proposals under the *Community Safety and Policing Act, 2019***
- **Comments on the Ontario Government's White Paper on Modernizing Privacy in Ontario**
- **Response to the Ontario Government's Consultation on a New Provincial Data Authority**
- **Response to the Ontario Government's Public Consultation on a Policy Framework for Ontario's Digital Identity program**
- **Submission on Proposed New Guidance for Broad Consent under the Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans**
- **Submission to the Standing Committee on Social Policy of the Legislative Assembly of Ontario: Schedule 4 of Bill 27, the *Working for Workers Act, 2021***
- **Submission on Proposed Amendment to O. Reg. 329/04 under the *Personal Health Information Protection Act* on the Right to Access Records in Electronic Format**
- **Submission to the Toronto Police Services Board's Public Consultation Regarding its Use of New Artificial Intelligence Technologies Policy**

Informal consultations and engagement

In addition to formal submissions, the IPC works informally with governments and public institutions to consult and provide advice and input at the early stages of programs and initiatives, including with respect to privacy impact assessments. This up-front engagement is instrumental in encouraging a privacy by design approach and helping initiatives get off on the right foot. The IPC continues to be generally very pleased with high level of openness and receptivity shown by stakeholders in receiving our input through these informal processes.

City of Burlington

- Implementation of a customer relationship management program

College of Physicians and Surgeons of Ontario

- Medical assistance in dying policy
- Professional obligations and human rights policy
- Social media draft policy
- Virtual care draft policy

Elections Ontario

- Elections Ontario employee privacy and security training

Independent Electricity System Operator

- Smart metering entity application to the Ontario Energy Board for a third party access plan

Ministry of the Attorney General

- Race-based data collection related to accused persons appearing in bail court

Ministry of Education

- Online cyber-safety tool

Ministry of Government and Consumer Services

- New OPC protocols for email record management – Capstone Approach
- Comments on National Chief Information Officer Sub-Committee on Information Protection position paper on *Protecting Sensitive Information Throughout the Access to Information and Privacy Process*
- Adoption disclosure — irregular birth registrations

Ministry of Labour, Training, Skills and Development

- Bill 288, the *Building Opportunities in the Skilled Trades Act, 2021*

Ministry of Northern Development, Mines, Natural Resources and Forestry

- Amendments to the regulations under the *Oil, Gas and Salt Resources Act*

Ministry for Seniors and Accessibility

- Amendments to the *Retirement Homes Act* as proposed in Bill 37, *Providing More Care, Protecting Seniors and Building More Beds Act, 2021* (Schedule 3) and amendments to O. Reg. 166/11.

Ontario Cannabis Retail Corporation

- Data management issues
- Research access requests

Ontario Digital Service

- Ontario government's digital initiatives
- Trustworthy Artificial Intelligence (AI) Framework

Ontario Health

- Release of the patient summary and mental health and addictions provincial data set interoperability specifications

Ontario Health Data Council

- Participation as an ex officio member

Prescribed Persons and Prescribed Entities

- Triennial review process and the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*

Various Ontario government ministries

- Proof of Vaccination initiative re: privacy and information security aspects of the Ontario Vaccination Certificate, enhanced QR code certificate and Verify Ontario app
- Outreach to unvaccinated individuals by the Provincial Vaccine Contact Centre
- Sending roster of unvaccinated and vaccinated patients to primary care providers from COVaxON database

PricewaterhouseCoopers

- Virtual care privacy and security standard

St. Thomas Police Service

- Body-worn cameras

Waterloo Regional Police Service

- New policing technologies, including GrayKey and BriefCam

IPC IN THE COURTS

Cabinet Office
PO-3973

The Court of Appeal dismissed a challenge to the IPC's 2019 decision ordering Cabinet Office to disclose the Premier's mandate letters. The court held the IPC was reasonable in finding the letters were not exempt under section 12 of FIPPA because they did not "reveal the substance of deliberations" of the Premier in formulating the government's policy initiatives or the deliberations of cabinet at any meeting. The court agreed that the IPC's decision "strikes a balance between a citizen's right to know what government is doing and a government's right to consider what it might do behind closed doors." (The Supreme Court of Canada has since granted the Ontario government leave to appeal the decision.)

Laurentian University

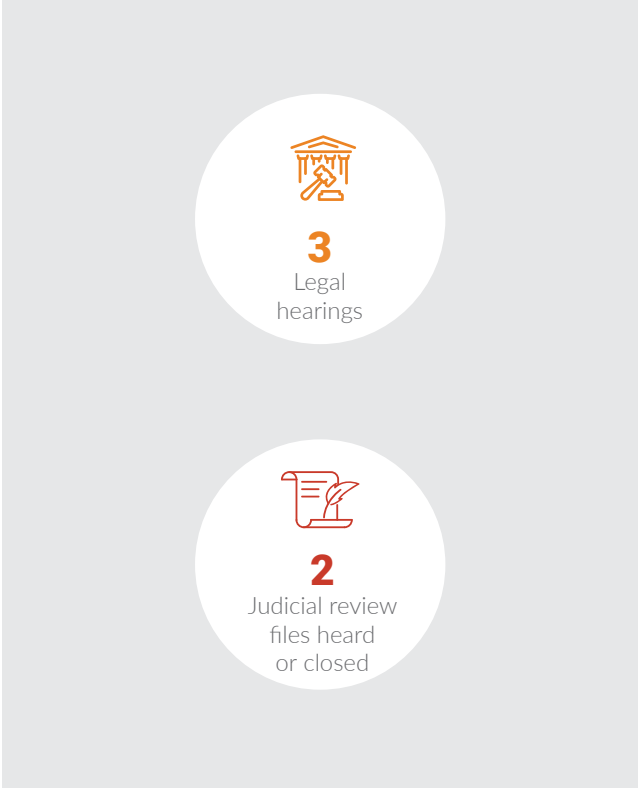
In February 2021, the Superior Court of Justice granted the Laurentian University of Sudbury, which at that time was insolvent, a temporary stay of its obligations to respond to FIPPA access to information requests. This stay, or suspension, was granted under the *Companies' Creditors Arrangement Act* and appeared to be unprecedented. Laurentian stated that it expected to

receive a high volume of FIPPA requests and that responding to them would require resources the university needed to devote to its restructuring. The IPC initially took no position on Laurentian's request for the stay, but made submissions to the court to provide some context about FIPPA and to express concerns about a precedent of a broad suspension of access rights. While the court granted the stay, it provided a condition that the IPC could request that this issue be revisited in 30 days and, if the IPC was dissatisfied with the continuation of the stay, it could bring a motion to the court on an expedited basis. This condition was maintained, at the IPC's request, when Laurentian made subsequent requests for extensions of the stay to ensure close monitoring of the status of freedom of information requests made to Laurentian and complaints from requesters. (In January 2022, the IPC objected to a further extension of the stay and later brought a motion to have it lifted. Laurentian originally opposed the IPC's motion, but before the hearing, the parties agreed to a settlement, which resulted in the stay being lifted. Since that time, the university has been required to respond to access for information requests in accordance with the timelines set out in FIPPA).

Toronto Police Services Board MO-3960 and MO-4003-R

The divisional court dismissed a challenge to the IPC's 2020 decision and related 2021 reconsideration decision that found records requested from the Toronto police were the subject of a prior appeal before the IPC. The prior appeal was also between the requester and the Toronto police and dealt with the same issues concerning the same records, namely about the application of the personal privacy exemption and the reasonableness of the Toronto police's search for the records. Given that the IPC already made final decisions on these issues in the prior appeal, the IPC determined that it should not allow the requester to re-litigate the issues. The court held the IPC's decision was reasonable as the evidence before the IPC was that the requester had an opportunity to participate in the prior appeal, the records were the same, the issues were the same, and final decisions on those issues were made.

The court also dismissed the requester's argument that the procedure before the IPC was unfair. The requester argued that they ought to have been given notice that the appeal at the IPC might be dismissed because of the prior appeal and that they ought to have received assistance from the IPC given that he was self-represented. The court found that the requester had been given notice of the issues to be addressed, was not entitled to further assistance from the IPC, and should have raised any allegations of procedural unfairness at the IPC.



IPC'S YEAR IN SUMMARY

JAN

15 — BODY-WORN CAMERAS

Follow-up on the IPC's recommendations to the Toronto Police Service on the development of its body-worn camera (BWC) program.

28 — PRIVACY DAY

Commissioner Kosseim hosts her first Privacy Day **webinar** focusing on law enforcement and surveillance technologies.

FEB

25 — HEALTH PUBLICATION

Guidelines on privacy and security considerations for virtual health care visits are launched.

MAR

4 — LAUNCH OF PODCAST

The **Info Matters** podcast series hits the digital airwaves!

APR

22 — LAUNCH OF STRATEGIC PRIORITIES

Release of the IPC's **Strategic Priorities 2021-2025** to promote and protect the access and privacy rights of Ontarians now and into the future.

14 — BILL 283

IPC issues **recommendations** to strengthen protection of personal health information under Ontario Bill 283, *Advancing Oversight and Planning in Ontario's Health System Act, 2021*.

19 — JOINT STATEMENT ON VACCINE PASSPORTS

The IPC joins with federal, provincial, and territorial privacy commissioners to issue a **joint statement** on privacy and COVID-19 vaccine passports.

MAY

20 — EDSBY INVESTIGATION

Release of **findings** in IPC's investigation of the York District School Board's use of Edsby, a cloud-based data management service that stores and processes student attendance.

2021

JUN

JOINT RESOLUTION ON IMPACT OF COVID -19 ON ACCESS AND PRIVACY

2 The IPC and federal, provincial, and territorial commissioners call on governments to **strengthen protection** of access and privacy both during and after the pandemic.

TRUSTWORTHY ARTIFICIAL FRAMEWORK

7 Submission of 14 **recommendations** to the government's public **consultation** on the development of a **trustworthy artificial intelligence (AI) framework** for Ontario.

MODEL GOVERNANCE FRAMEWORK FOR BWC

7 Release of a **model governance framework** for the use of body-worn cameras by police services in Ontario to promote a consistent level of rights protection across the province.

JUL

DRAFT GUIDELINES FOR THE USE OF FACIAL RECOGNITION TECHNOLOGY BY POLICE.

10 Release of draft **guidelines** for the use of facial technology by police, developed in consultation with. federal, provincial, and territorial privacy counterparts.

STATEMENT ON FUNDING TO EXPAND THE COVERAGE OF CLOSED-CIRCUIT TELEVISION (CCTV) SYSTEMS ACROSS THE PROVINCE.

16 **Statement** in response to the government's investment in the expansion of closed-circuit television systems, encouraging organizations to consult with the IPC to ensure appropriate policies, procedures, and training are in place.

GOOGLE G SUITE INVESTIGATION

23 Release of findings in IPC's **investigation** of the Toronto District School Board's use of G Suite for Education, recommending changes to how the board provides notices of collection and improved oversight of security practices and contractual commitments.

AUG

NEW HEALTH GUIDANCE

4 Guidance on the **Use and Disclosure of Personal Health Information for Broader Public Health Purposes** is published.

2021

SEP

MODERNIZING PRIVACY IN ONTARIO

7 **Submission** to the government's public consultation on modernizing privacy in Ontario.

PROTECTING STUDENT PRIVACY RIGHTS WEBINAR

9 Launch of back-to-school **webinar** for Ontario's educators to assist them in navigating provincial privacy laws and protecting student privacy rights.

PROVINCIAL DATA AUTHORITY

22 Submission of **recommendations** for Ontario's proposed provincial data authority.

PRIVACY PURSUIT!

23 **Privacy Pursuit! Games and Activities for Kids** is published.

DIGITAL IDENTITY PROGRAM

23 **Submission** to the Ontario government's public consultation on the development of a policy framework for Ontario's digital identity program.

RIGHT TO KNOW WEEK

27 **Public interest disclosure** fact sheet is published as part of Right to Know Week activities.

OCT

REVIEW OF ONTARIO HEALTH AS A PRESCRIBED ORGANIZATION

1 **Report** summarizing the IPC's review of Ontario Health as a prescribed organization under the *Personal Health Information Protection Act* is published.

MANUAL FOR THE REVIEW AND APPROVAL OF PRESCRIBED ORGANIZATIONS

18 Updated **Manual for the Review and Approval of Prescribed Organizations** is published.

RESOLUTION ON CHILDREN'S DIGITAL RIGHTS

27 The Global Privacy Assembly adopts a **resolution** on children's digital rights, co-sponsored by the IPC.

NOV

SUBMISSION TO BILL 27, THE WORKING FOR WORKERS ACT

21 **Submission** to the Standing Committee on Social Policy regarding Bill 27, the *Working for Workers Act,* recommending that limits be placed on the authority to collect and use personal information.

FIRST PART X DECISION

30 **First decision** issued under Part X of the *Children, Youth and Family Services Act*, setting down important precedents related to the provision of services under the act and release of adoption records.

DEC

PROPOSED PHIPA REGULATION FOR ELECTRONIC FORMAT

3 **Review** of proposed regulation under Ontario's health privacy law relating to the right of access to records of personal information in electronic format.

TORONTO POLICE SERVICES BOARD'S DRAFT USE OF NEW ARTIFICIAL INTELLIGENCE TECHNOLOGIES POLICY

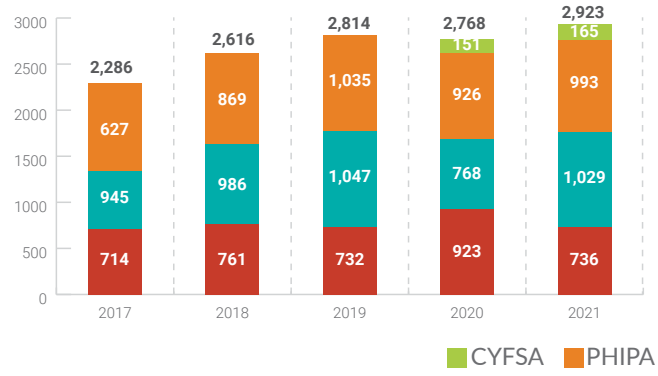
20 **Comments** on the Toronto Police Services Board's draft policy for the use of new artificial intelligence technologies.

STATISTICAL HIGHLIGHTS FROM 2021

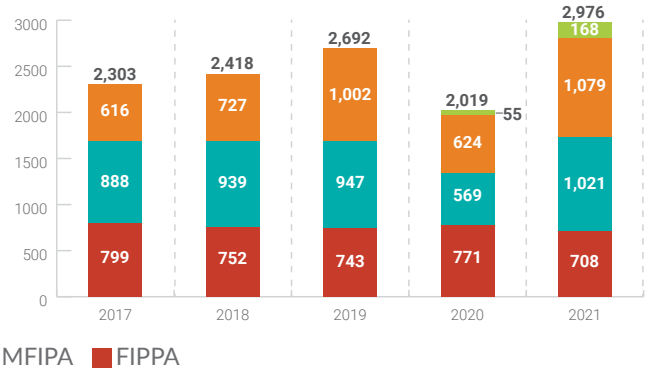
Full details are available in the IPC's **2021 Statistical Report**.

Overall

Opened Files 2017-2021

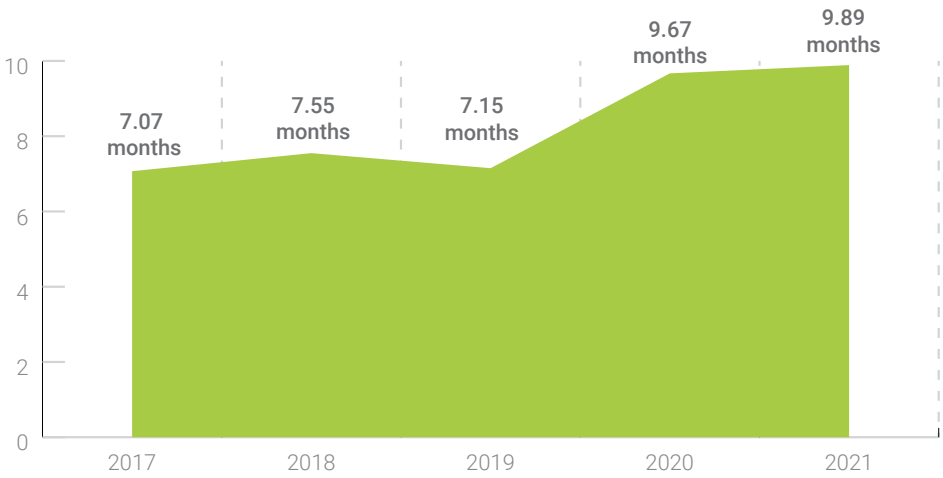


Closed Files 2017-2021



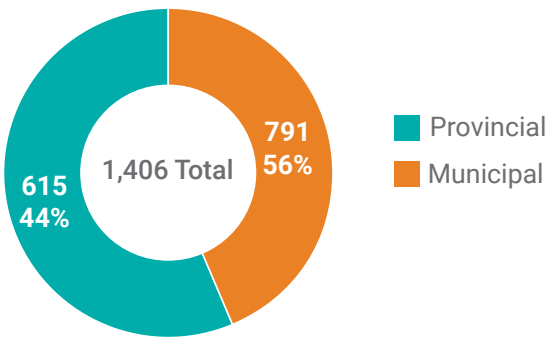
CYFSA PHIPA MFIPA FIPPA

Average Duration (in Months) to Process and Close a File 2017-2021

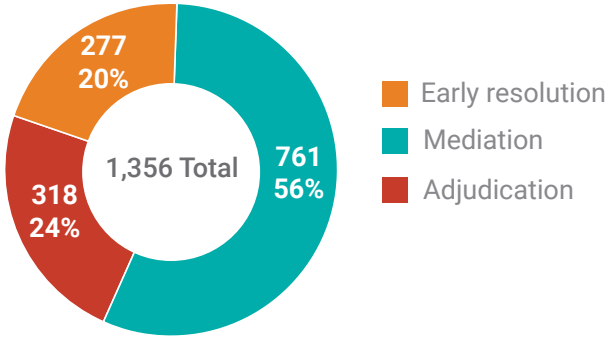


FIPPA/MFIPPA Files

Access Appeals Opened



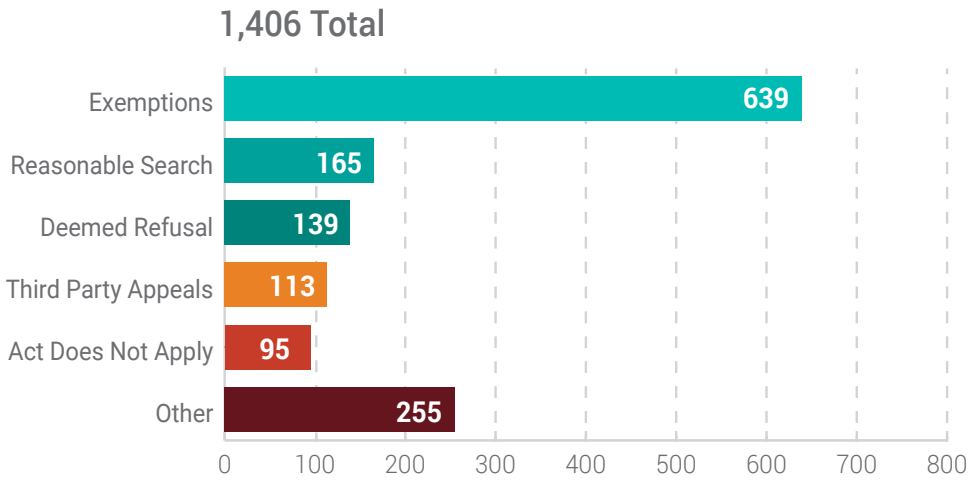
Access Appeals Resolved by Stage



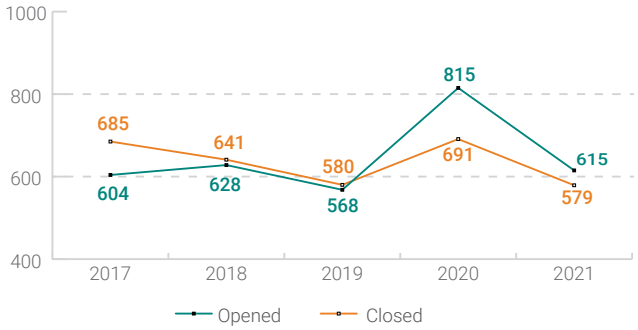
STATISTICAL HIGHLIGHTS FROM 2021

FIPPA/MFIPPA Files cont'd

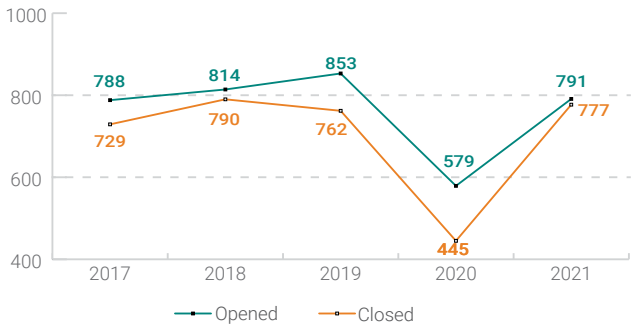
Issues in Access Appeals Opened in 2021



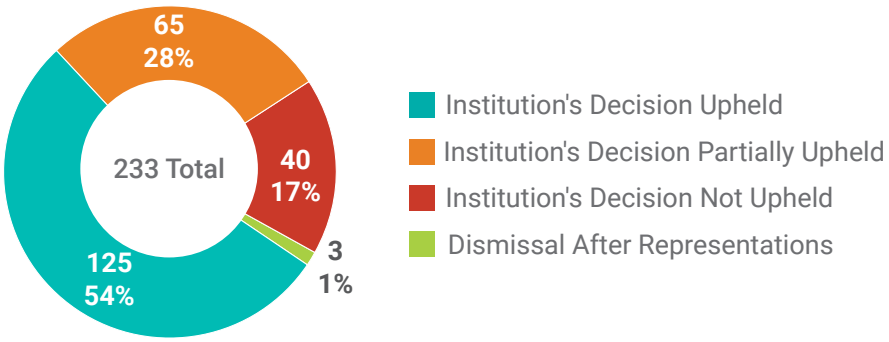
Provincial Access Appeals Opened/Closed 2017 – 2021



Municipal Access Appeals Opened/Closed 2017 – 2021



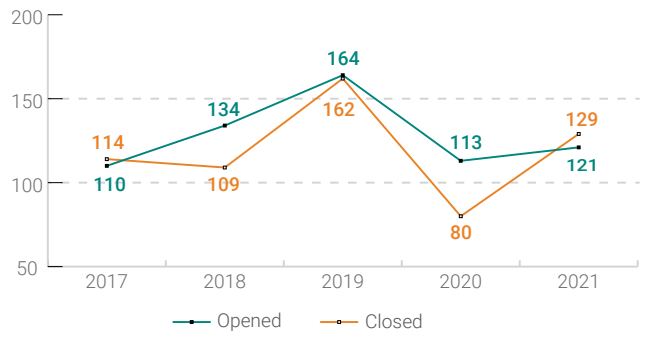
Outcome of Access Appeals Closed by Order in 2021*



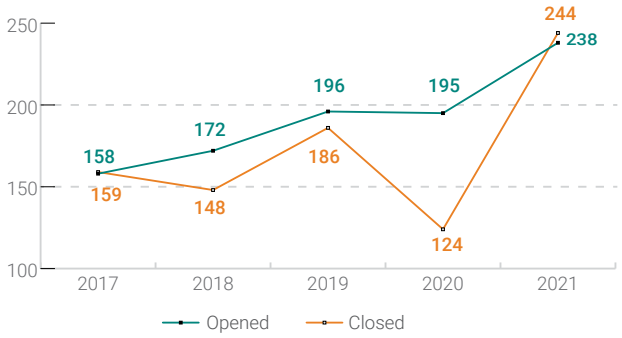
* Does not include files that were resolved, abandoned, withdrawn or dismissed without an inquiry during adjudication

FIPPA/MFIPPA Files cont'd

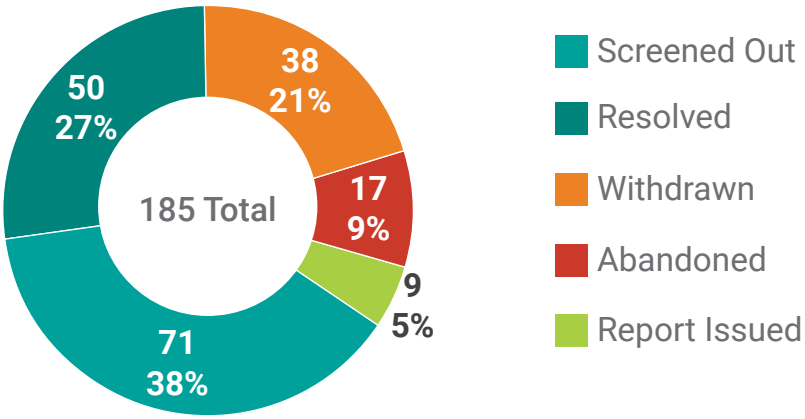
Provincial Privacy Complaints & Self-Reported Breaches Opened/Closed 2017 – 2021



Municipal Privacy Complaints & Self-Reported Breaches Opened/Closed 2017 – 2021



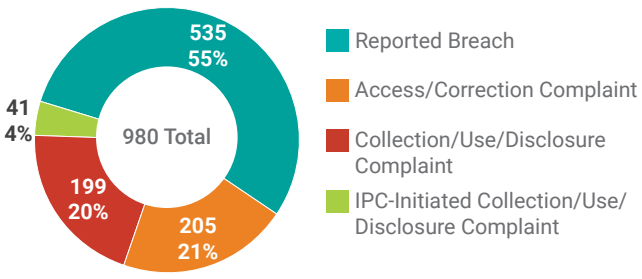
Privacy Complaints* Closed by Type of Resolution



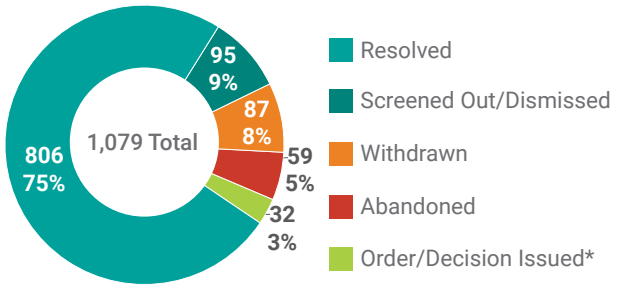
*** Self-Reported Breaches were processed separately. There was a total of 188 self-reported breaches closed, with 187 "Resolved" and 1 "Report Issued"**

PHIPA Files

Types of Health Files Opened



Outcome of Health Files Closed

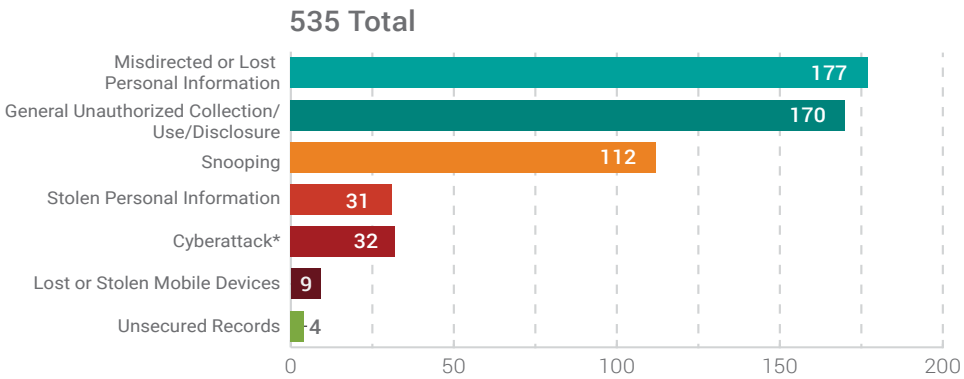


*** 1 out of 32 order/decision issued was an interim order**

STATISTICAL HIGHLIGHTS FROM 2021

PHIPA Files cont'd

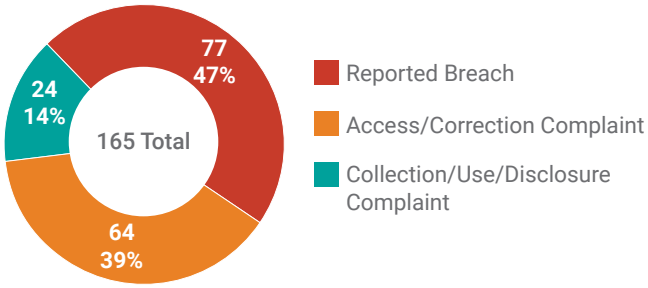
Self-Reported Health Privacy Breaches by Cause



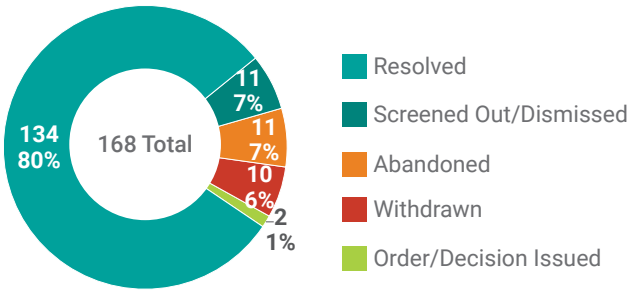
* 8 out of 32 cyberattacks involved ransomware

CYFSA Files

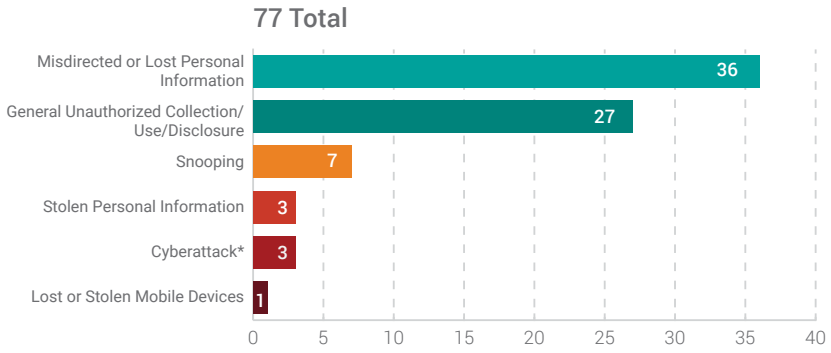
CYFSA Files Opened by Issue



Outcome of CYFSA Files Closed

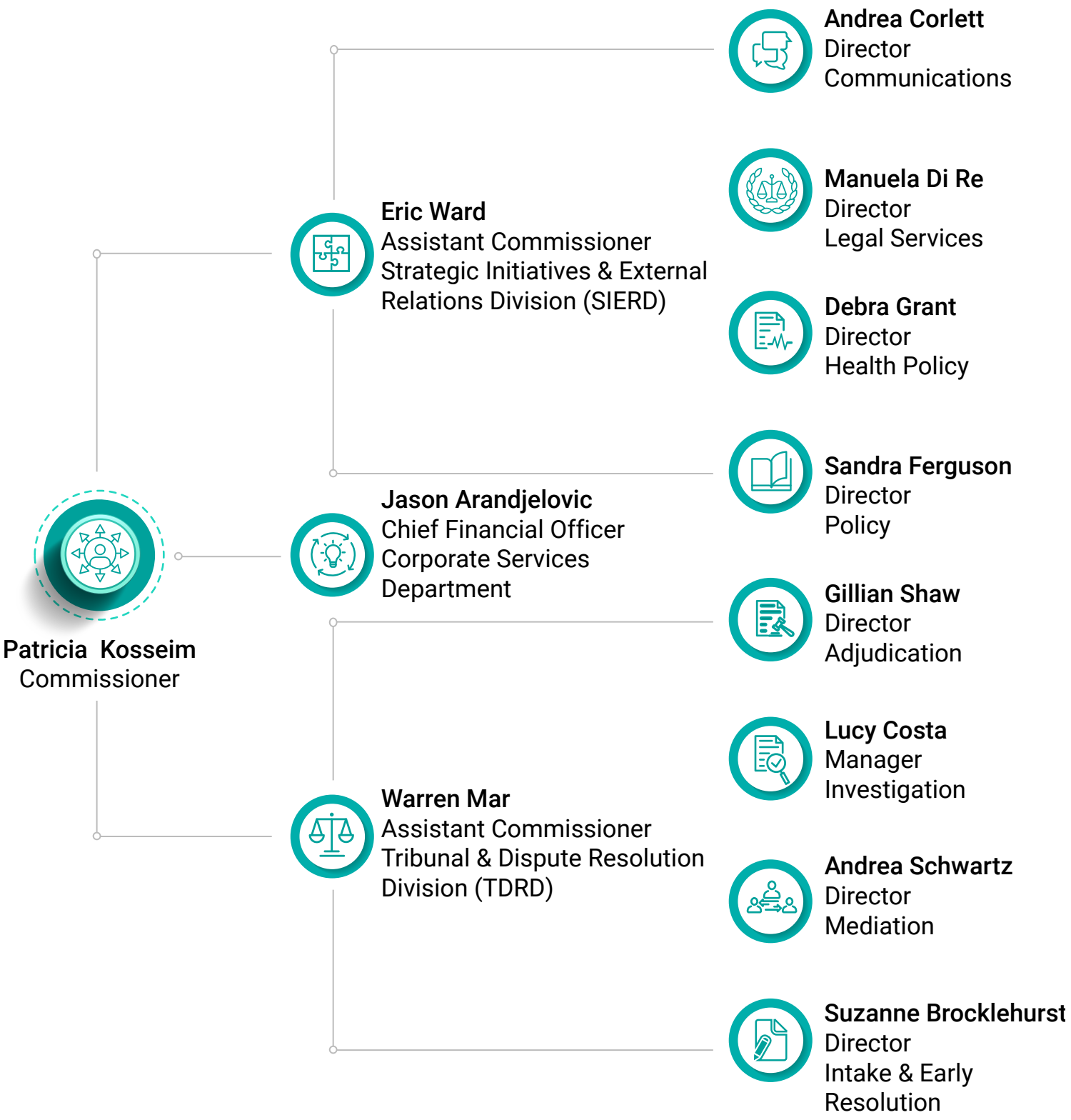


Self-Reported CYFSA Privacy Breaches by Cause



* 1 out of 3 cyberattacks involved ransomware

IPC ORGANIZATIONAL CHART



In 2021, the IPC had a staff of 130 full time equivalents (FTEs).

FINANCIAL STATEMENT

	2021-2022 ESTIMATE (UNAUDITED) $	2020-2021 ESTIMATE (UNAUDITED) $	2020-2021 ACTUAL (UNAUDITED) $
Salaries and Wages	14,433,300	13,885,500	13,531,705
Employee Benefits	4,138,200	3,682,500	3,268,132
Transportation and Communications	132,900	286,700	123,254
Services	3,125,700	2,475,900	3,000,591
Supplies and Equipment	122,500	322,000	203,575
Total	**21,952,600**	**20,652,600**	**20,127,257**

Note: The IPC's fiscal year begins April 1 and ends March 31.

2021 APPEALS FEES DEPOSIT

(CALENDAR YEAR)

GENERAL INFORMATION	PERSONAL INFORMATION	TOTAL
$19,469	$3,020	$22,489

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.

Access and Privacy:
Cornerstones of a Digital Ontario

2021 ANNUAL REPORT

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

416-326-3333
www.ipc.on.ca
info@ipc.on.ca