Check against delivery

Keynote by Patricia Kosseim, Information and Privacy Commissioner of Ontario
Association of Municipal Managers, Clerks and Treasurers of Ontario (AMCTO)
Municipal Information, Access & Privacy Forum
March 28, 2024

Facing the Digital Future: Balancing Innovation and Security in Municipal Governance

Introduction

- Good morning. Thank you for inviting me here today, it's good to be back. I'm accompanied by Assistant Warren Mar, who, as many of you know, comes from the municipal sector, and understands your world very well.

- The municipal sector is the largest group of institutions our office deals with, and I always look forward to the opportunity to speak with you about the issues of the day.

- As a regulator, the IPC oversees compliance with Ontario's access and privacy laws, of course.

- But we're also here to build cooperative working relationships with public institutions and help enable what we all want: supportive communities in which Ontarians can thrive and prosper, confident that their governments are acting responsibly and respecting their rights.

- Today, I'd like to speak to you about balancing innovation, privacy, and transparency in municipal governance.

- As more public institutions modernize and innovate by adopting modern technologies, including artificial intelligence systems, we must remember that for true and sustainable success to take hold, institutions must earn and keep the public's trust.

Innovation & AI

- Steve Jobs once said, "Innovation is the ability to see change as an opportunity, not a threat."

- Many new technologies have the exciting potential to help public institutions improve their efficiency, responsiveness, and service delivery to the public.

- Think — managing wait times, delivering more timely and personalized services, responding to emergency situations, and preventing criminal activity *before* it happens.

- However, any enthusiasm we have for innovation must also be matched with an equal commitment to accountability, transparency, privacy, and security protection.

- The coexistence of all these things is not only possible, but it is absolutely necessary. We can feel excited about the potential for innovation to improve our lives, and confident about its successful outcomes, as long as the proper guardrails and governance frameworks are in place.

- Ontario's evolving Trustworthy AI Framework supports the ethical use of artificial intelligence based on three priorities:

    1. No AI in secret

    2. AI use that Ontarians can trust

    3. AI that serves all the people of Ontario

- My office made a submission as part of the government's consultation on its draft framework back in 2021. Our recommendations called for:

    - clarity of definitions and broader scope of application;

    - expanded transparency and accountability requirements;

    - more robust risk assessments;

    - continual monitoring and human supervision;

- strong independent oversight;

- and the need for a more comprehensive governance framework, including possible no-go zones.

- Two years later, and still waiting for that comprehensive governance framework, my office issued a joint statement with the Ontario Human Rights Commission urging the Ontario government to establish a more robust and granular set of *binding* rules for public sector use of AI technologies. We called for clear and effective guardrails to address safety, privacy, accountability, transparency, and human rights.

- And our offices committed to work together, and with government, to ensure AI gets developed and deployed in an ethically responsible manner that benefits all Ontarians.

- As you know, Ontario is not alone in this AI governance challenge. AI is the song that's got the whole world singing.

- And generative AI is the latest refrain that's got everyone's voices chiming in.

- In the hands of bad actors, generative AI can produce material that causes real-world harm — spreading false or misleading information that can ruin people's lives and reputations, destabilize trust in public institutions, send stock prices plummeting, and seriously undermine elections and other democratic processes.

- Last December, the IPC joined its federal, provincial, and territorial counterparts in releasing *Principles for Responsible, Trustworthy, and Privacy-Protective Generative AI Technologies.*

- These principles are designed to mitigate a host of new risks brought on by generative AI, particularly for vulnerable and historically marginalized groups, and ensure that any generative content, including text, imagery, audio or video, is clearly identified as having been created by generative AI.

- Last October, we also co-sponsored two international resolutions related to AI that were universally adopted at the 45th Global Privacy Assembly.

- One of these resolutions sets out international principles for the development, operation, and deployment of generative AI systems, reinforcing our FPT statement, and the other focuses more specifically on AI use in the context of employment.

- Speaking of AI in the employment context, as some of you may know, the government passed Bill 149 as part of its Working for Workers reforms, requiring employers to indicate in their public job postings if they are using AI in the recruitment process.

- I appeared before the legislative committee examining the bill to say that, while this is a good step, it's not nearly enough to mitigate the risks of AI throughout the entire employment relationship — not just during recruitment — and to address the risks of AI in all sectors, not just employment.

- Our Privacy Day event in January 2024 focused on the theme of artificial intelligence in the public sector. We had over 2300 attendees and another 1,300 plus views of the webcast since. For those of you who missed it, you can still find the webcast on our YouTube channel and hear all the great insights from our panel discussion that day.

- Earlier this month, my office issued a privacy investigation report that, for the first time, addressed the use of AI technologies. We investigated the use of AI-enabled proctoring software at McMaster University.

- You can read more about it in my most recent blog up on our website called AI on Campus.

- Essentially, we found significant privacy concerns arising from the use of this AI-enabled technology that collects sensitive biometric information and assesses student movements and behaviours while writing exams remotely to flag potential instances of cheating.

- The report addressed the need for guardrails on the adoption and use AI technology by universities, with some key recommendations.

- They include:

  - consulting with different communities comprising the student body, particularly vulnerable and historically disadvantaged groups who may experience systemic discrimination or bias

  - providing students with an opportunity to opt out of online proctoring and choose in-person testing

  - ensuring that the data used to feed the algorithms is obtained in compliance with relevant laws and regulations, and

  - prohibiting the use of students' personal information for product improvement, research, or algorithmic training without their consent

- In a recent cybersecurity and survey report by the Canadian Internet Registration Authority (or CIRA), **78 per cent** of MUSH organizations surveyed (i.e., municipalities, universities, schools and hospitals), expressed worry about cyber threats from generative AI. And with reason.

- I urge all municipalities that are considering, or are already using AI, to take the steps needed to ensure it respects the privacy and human rights of Ontarians, and to heed the recommendations of data protection authorities worldwide, including the IPC.

- I also urge you to participate actively in the debate about what the appropriate guardrails should be. While Ontario's evolving Trustworthy AI framework is intended for provincial government institutions, there is no principled reason why municipalities, and broader public sector, should not be subject to the same rules.

Cybersecurity

- I want to turn next to discuss cybersecurity, which has become an issue of increasing concern for Ontario's public institutions.

- Cyberattacks have dominated the headlines recently, with a rash of attacks targeting municipalities in Ontario.

- I can't speak to the specifics, as my office has several investigations in progress. But I can tell you that the number of cyberattacks reported to the IPC from municipal institutions has more than doubled in 2023, compared to last year.

- And this is in a context of voluntary breach reporting. We don't know what we don't know, but one could only imagine how many more cybersecurity incidents go unreported.

- One thing for certain: cybersecurity has become critical for municipal institutions.

- When cyberattacks threaten the integrity of public services, cybersecurity becomes more than just a compliance issue. Every attack chips away at the public's confidence in governments' ability to safeguard their information and to provide critical services.

- According CIRA's 2023 Cybersecurity Survey and Report, the MUSH sector — is at greatest risk.

- These organizations, including municipalities, are a particularly attractive target for these attacks because of the large amounts of personal information in their custody and control.

- Cybercriminals also take advantage of the fact that public institutions provide critical services that residents rely on. They extort money from these institutions on threat of paralyzing the delivery of essential public services by locking down data, not returning the data, or releasing it on the dark web.

- The CIRA report, which surveyed 500 cyber security professionals from across Canada, found that over a third (**38 per cent)** of MUSH sector organizations had experienced a cyberattack in 2023, and nearly a quarter (**22 per cent)** had experienced a ransomware attack.

- Of those, **50 per cent** ended up paying the ransom demand in these attacks.

Resource Constraints

- Whenever the issue of municipalities and cybersecurity is discussed, one of the major concerns raised is the lack of resources to address the problem.

- In a 2023 Canadian Municipal Digital Transformation Benchmarking Report (MNP Digital), **76 per cent** of municipalities across Canada reported cybersecurity as a top focus area. When asked about the top barrier for their organization, **62 per cent** cited insufficient resources.

- Having worked with the municipal sector for some time now, I understand that many of the smaller towns and cities do not have the same level of expertise, guidance, and resources to dedicate to cybersecurity that larger institutions can.

- One potential solution may be to adopt a collective response by banding together with other organizations and forming a coalition of sorts.

- The CIRA report I mentioned earlier revealed that **41 per cent** of MUSH sector organizations surveyed said they were part of a group or partnership aimed at improving cybersecurity.

- A good example of this is Ontario Health's Provincial Cyber Security Operating Model. It is enabling health care organizations across Ontario — large and small — to work together to coordinate and manage cybersecurity challenges.

- A recent Ontario Health Annual Privacy and Security Report found that this operating model maximized participants' savings and efficiencies through service sharing and gave smaller organizations a leg up in their cyber capabilities.

- I urge you to consider building a similar coalition and coordinated approach in the municipal sector if you haven't already begun doing so.

Ransomware & Phishing IPC Fact Sheets

- To help support organizations in combatting against cyber risks, my office has a range of available resources, including our fact sheets on ransomware and phishing.

- Our factsheet on ransomware provides a useful overview for organizations covering the impacts of ransomware, and offers valuable advice on how to secure your organization, including:

    - maintaining an inventory that tracks where and how information flows

    - classifying IT assets according to sensitivity and putting safeguards in place proportionate to the sensitivity of information

    - a risk management program that establishes requirements for regular security assessments

    - ensuring personal information and sensitive records are disposed of securely

- There are also recommendations on how to respond to a cyberattack and steps for reporting breaches to our office and notifying affected individuals.

- If cyberattacks are a thief's way of stealing valuable assets, phishing is the tool they use to pick the front door lock. Our related fact sheet provides valuable insights on how to identify potential phishing attempts and protect your organization against this type of social engineering attack that remains one of the most insidious ways for criminals to get in the door.

- Phishing attempts, whether email, voice mail or text message, etc., will get even more insidious as generative AI tools produce more and more realistic traps for employees to fall into.

- Best practices to protect against phishing attacks include:

    - screening incoming emails to reduce spam and verify the authenticity of senders

    - installing software that prevents, detects, and removes malware

    - always keeping browsers and other software up to date

    - restricting administrative rights and limiting who has access to sensitive information

    - enabling encryption of documents, devices, and databases that contain sensitive information

    - training and retraining staff on how to identify suspect emails, voicemails or texts and report them immediately to your IT department.

Info Matters

- A recent episode of our *Info Matters* podcast, with Jason Besner of the Canadian Centre for Cybersecurity, also provides practical tips for organizations and individuals to protect themselves against digital threats.

- When I asked Jason what organizations could do to level the playing field with cyber criminals, his first piece of advice was to designate someone as the organization’s cybersecurity champion.

- Someone who is responsible for promoting a culture of security, awareness, education, and basic cyber hygiene practices.

- Cybersecurity is not just an issue for the IT department. It’s everyone’s responsibility in the organization.

- When it comes to individuals protecting themselves against cyber threats, he emphasized the social engineering aspect of phishing, that continues to be the leading and most reliable entry point for ransomware and cyberattacks.

- His advice was simple. Be vigilant about the communication you are receiving. Would your city clerk, HR manager, or IT department usually ask you to transfer funds, update employee details, or install a new app on your computer without proper context?

- If you receive something that sends up red flags, don’t be afraid to ask questions and investigate. Report it to your IT department and ask them to take a second look if a message looks suspicious.

Annual Report — IPC Statistics — Tribunal

- I’d like to switch gears a bit to talk about access to information.

- Organizations subject to MFIPPA are required to submit their annual statistics to our office, including the numbers of access requests they receive, and the time it takes to complete them.

- Thank you to everyone who got their reports in on time. If you haven’t yet, you still have a couple of days to get your statistical reports in before the end of the month.

- We have answers to frequently asked questions about statistical reporting on our website and webinars to help you understand the process for submitting annual statistics to our office.

- We will analyze the reports we received for 2023 and publish the data in our annual statistical report in June.

- In the meantime, I can give you a little sneak peak at some of the numbers coming out of our own office, that will be published in our upcoming annual report.

- In 2023, the IPC opened **1,121** MFIPPA files, which is the highest number of files we've seen from this sector in at least five years. Of those, **868** were municipal access appeals.

- In terms of our tribunal operations, I'm happy to report that the average time to process and close access appeals decreased by almost **15 per cent** from 2022, and by almost **18 per cent** when you account for all jurisdictions, stages, and file types.

- More than **85 per cent** of all files have been resolved through early resolution and mediation, a success rate we've managed to maintain for three consecutive years in a row.

- Our backlog in 2023 — was down **20 per cent** from two years earlier, with mediation backlogs cut by half compared to 2021.

- Our mediation pilot project for one-day mediations was highly successful with a **90 per cent** resolution rate for simplified files, closing them in an average of 42 days — four months under the overall average.

Frivolous and Vexatious & Orders of Note

- Managing time delays, and backlogs, requires making tough decisions sometimes. While the right of access is fundamental, we have a responsibility of ensuring everyone has fair access to that right.

- Generally, we process appeals on a first-come-first-serve basis. However, sometimes we have to impose limits on the number of active appeals a requester can have open with our office at any one time. We ask the requester to indicate which appeals they would like us to proceed with first and put the rest temporarily on hold. We do this as a measure of last resort, particularly with large queues waiting, to ensure fair allocation of resources to all Ontarians.

- Currently, **5 per cent** of all active files are on hold due to file processing limitations.

- When we do impose file limitations, it's so that we can balance the needs of all users of our services and prevent the system from being overwhelmed by a single party who otherwise consumes a disproportionately high amount of our resources.

- Managing scarce resources and guarding against abuse of the system also requires calling out frivolous and vexatious requests, when we see them, while also ensuring not to deny people's fundamental rights.

- These are very tough calls to make, but the law allows for this in very specific circumstances. For insights into factors for determining whether an access to information request is frivolous or vexatious, I encourage you to take a look at our Interpretation Bulletin and our fact sheet on this topic. They're both available on our website.

- As part of his series on Secret Canada, Tom Cardoso of the Globe and Mail wrote about frivolous and vexatious requests, sounding the alarm for requesters not to be unreasonable: "If a public institution has begun to warn you it considers your requests to be frivolous or vexatious, don't take that warning lightly."

IPC Orders of Note

- I'd like to go over some orders that relate to frivolous and vexatious which I think you might find interesting. You can find our orders and decisions on our website in the decisions section.

- **Order MO-4241** involved eight appeals from two requests made by a lawyer acting for plaintiffs in a class action lawsuit against the town. Requests were made for records relating to the Saw-Whet Subdivision Development Proposal, Review and Approval process.

- The Town of Oakville refused access on the basis the requests were frivolous or vexatious.

- The IPC upheld the town’s claim that the requests were frivolous or vexatious because the appellant’s requests were part of a pattern of conduct that amounted to an abuse of the right of access. It also appeared that the number of requests showed no signs of decreasing over time.

- Approximately **16 per cent** of the requests received by the town were from the appellant, or another appellant, who were involved in the same class action, and appeared to be working together.

- For the next year, the IPC limited the appellant to one active request, with limited number of parts, and one active appeal involving the town at any given time.

- **Order MO-4300** dealt with three appeals from three requests made by a business owner in Brantford.

- The city claimed the appellant made 145 access requests for correspondence between city staff. The city responded to many of the requests, until the city eventually denied access on the basis that the requests were frivolous or vexatious.

- The IPC found that many of the requests were duplicative, excessively broad, and unusually detailed. There was evidence that the appellant was trying to burden the system with his requests.

- The IPC limited the appellant to one access request to the city, with limited number of parts, and one appeal before the IPC for one year.

- **Order MO-4468** involved a lawyer representing plaintiffs in a class action lawsuit who made a multi-part access request to the conservation authority.

- The conservation authority claimed that it had become overburdened by the number of requests submitted by the class action legal team.

- The IPC found that the appellant made recurring or similar requests, related to the class action, and that the multi-part access request formed part of a pattern of conduct, amounting to 37 requests in total.

- While the IPC did not find that the appellant was trying to burden the system, the impact of their actions still culminated in the abuse of the right of access.

- **Order** **MO-4493** involved the Township of Oro-Medonte. The township received a three-part request from an appellant who is part of a group suing the township over certain user fees for the water system and ownership of the water system.

- The township denied access on the basis that the requests were frivolous or vexatious, claiming that the appellant had filed 35 access requests, each resulting in an appeal, all relating to the same issue.

- Even though the appellant had a genuine interest in the information, the request was viewed as part of an overall pattern of conduct intended to overburden the township when they were already dealing with related access requests and litigation.

- The appeal was dismissed.

- I describe these orders not to open the floodgates for institutions to deny the access requests of legitimate requesters on grounds that they are being frivolous or vexatious. Frivolous or vexatious does not mean merely annoying, inconvenient or resource intensive.

- Rather, I cite these recent orders to show that this exception exists in the law for a reason, and that the IPC will recognize its application in appropriate circumstances, where the requisite conditions are met.

IPC Guidance

- Before I conclude, I'd like to take a moment to tell you about some our latest guidance and other resources.

Third Party Guidance Document

- I'm excited to tell you about a new IPC guidance document, *Privacy and Access in Public Sector Contracting with Third Party Providers.*

- We are still putting the finishing touches on the guidance with a view to releasing it in the coming weeks. I am grateful to the AMCTO for their helpful input on an earlier draft of this guidance document.

- You may have heard me say this before, but I'll say it again. You can outsource services, but you can't outsource accountability.

- This guidance document provides valuable support for Ontario's public sector in identifying access and privacy considerations that need to be built into outsourcing arrangements with third parties.

- You'll find recommendations that span across all phases of the procurement process, including planning, tendering, contracting, vendor management, and terminating the contact or agreement.

- It will soon be made available on our website and I encourage you to take a look at it once it's up, and share it with your networks.

Revised M/FIPPA Code of Procedure

- Another project my office is currently working on is revising the code of procedure for appeals under FIPPA and MFIPPA. The code last underwent a review back in 2004.

- We felt this review was necessary to:

    - reflect the IPC's current operations for processing appeals, including e-appeals

    - improve timeliness for the processing of appeals

    - maintain the fair and just consideration of appeals

    - provide greater transparency and understanding of the IPC's procedures when considering appeals

- We held a public consultation inviting feedback from public institutions and other interested parties. We received a lot of valuable feedback for which we thank you. We are currently taking into consideration what we've heard as we finalize the updated Code of Procedure.

- Please keep an eye out for the revised code of procedure which will be posted on our website soon.

Interpretation Bulletins

- Something else I think you will really find useful is a new series of Interpretation Bulletins we've created to provide insight into how the IPC and the courts interpret certain provisions of FIPPA and MFIPPA when reviewing appeals.

- These Interpretation Bulletins can help organizations make better informed access decisions right up front at the request stage, and assist parties involved in an appeal with our office so they know what to expect and how they can improve the quality of their submissions.

- Current IBs cover topics such as:

    - Custody or Control
    - Fees and Fee Waivers
    - Personal Information
    - Reasonable Search
    - Frivolous and vexatious requests

- New interpretation bulletins are being posted on an ongoing basis. We've just released a new batch on:

    - Advice or recommendations
    - Public Interest Override
    - Third Party Information
    - Economic interests

- Let us know if you have any questions about the bulletins or suggestions for future topics.

Transparency Challenge

- One more thing before I conclude — the IPC has launched its second Transparency Challenge!

- I was recently interviewed by Municipal World Magazine about this initiative and spoke about how the Transparency Challenge was part of my office's ongoing efforts to build a culture of transparency among government institutions.

- Transparency and access to information are vital to our democracy. They allow the public to hold their governments accountable, help counter misinformation, foster civic engagement, and build public trust.

- In this year's Transparency Challenge, we are once again calling on public institutions to share their innovative approaches to open data and government transparency.

- We've also added a new twist this year, asking institutions to show us the unique ways they are being transparent about how they collect, use, or disclose personal data.

- We hope to bring out the competitive spirit of public institutions to take up this year's challenge!

- We will select among this year's submissions to be displayed in a new gallery of our Transparency Showcase to be unveiled in September 2024.

- To give you a taste of what's currently in our exhibit, I'd like to share with you a few of the great submissions we received from municipalities last year.

City of Barrie

- The City of Barrie's initiative features a mobile app that gives residents access to information about popular city services.

- The app allows for quick and easy access to information about city events, roadwork, municipal elections, council meetings, transit and parking, public notices, access to information requests, and the list goes on.

- I also really like that the app gives people control by allowing them to customize and opt in or out of notices.

City of Brampton

- The City of Brampton publishes information about their access requests online, showing what records have been released under access laws.

- When the city receives an access to information request, an index is created that includes a summary of the request, a breakdown of responsive records by page number, details on the applicable sections of the law, the type of access granted, and any additional comments.

- The city publishes these indexes online, together with details about how the city responds to each access to information request it receives under MFIPPA.

- This gives the public a clear window into the access requests the city receives and how each one is treated.

Town of Whitby

- The Town of Whitby created an online tool for the 2022 municipal election to help candidates share their platforms and give electors much easier access to information to support their voting decisions.

- This is a great example of how open data can have a direct and positive impact on civic engagement.

- This new tool also allows electors to easily access their own status on the voters' list and voting location.

- A survey found that **96 per cent** of voters were satisfied with the tool and **70 per cent** said that having easy access to candidate information was the most helpful feature.

City of Guelph

- The City of Guelph's GeoDataHub uses geographic information systems technology to provide information about what is going on around the city.

- It offers easy online access to the city's open datasets to provide information about the location of snowplows, parks, bus stops, parking lots, and more.

- Residents can also add information about events and activities in their community.

- This is a great resource that encourages community engagement and allows residents to combine datasets and perform their own custom analyses with maps and charts.

- I hope you enjoy visiting these and other great examples in our virtual gallery and feel inspired to make a submission of your own this year. It's a great opportunity for your organization to demonstrate your commitment to open government and transparency.

- The deadline is **May 31, 2024**, so you still have lots of time to make a submission.

Conclusion

- In closing, I would like to say that both Assistant Commissioner, Warren Mar and I, place great importance on the IPC's relationship with the municipal sector based on open lines of communication, collaboration, and cooperation.

- We aspire to be modern and effective regulator with real-world impact. To achieve that vision, we need to hear and understand the perspective of those of you who on the front lines who serve

Ontarians at the local, community level, and who see and feel — first-hand — the real-world impact on their privacy and access rights.

- I was heartened to read in the AMCTO's Proactive Submission to Modernize the *Municipal Freedom of Information and Protection of Privacy Act* that "Municipalities consider transparency an important tool for building and maintaining public trust and recognize the importance of continuously improving."

- On that, we are completely aligned.

- And so, in the spirit of mutual collaboration and continuous learning, Warren and I would be happy to open the floor to hear your questions and comments.

- Thank you.