Check against delivery

Keynote by Patricia Kosseim, Information and Privacy Commissioner of Ontario
International Institute of Communications Canada Conference
October 22, 2024

The IPC: Planning for Ontarians' Digital Future

Introduction

- Good morning, everyone.

- It's a pleasure to be here today and I'd like to thank the International Institute of Communications for giving me this opportunity to discuss something that impacts all of us: our digital future.

- In 1921, Nobel Peace Prize laureate, Christian Lous Lange, was addressing the rapid rise of industrial technologies and their potential to dominate society if left unchecked, when he famously stated that "Technology is a useful servant but a dangerous master."

- A century later, his words resonate more than ever.

- In fact, more recent Nobel Prize winner, Geoffrey Hinton, has stated that, "We're getting close to computers being able to improve themselves in a manner we can no longer control, which could mean the end of people."

- As technology rapidly shapes our world, the question remains: Are we still its master, or has it become ours?

- As this great existential debate about the future of humanity looms in the background, we must get a handle on the potential benefits and harms of emerging technologies, here and now.

- As more organizations modernize and new technologies transform the world around us, making our lives easier, smarter and more connected, we cannot lose sight of the single most critical factor of success — public trust.

- I believe public trust is the great leveler and equalizer that will keep us in check.

- Without it, innovation will fall short of its promise to advance technology for the good of all humanity, and instead, veer us off track into a world of greater disparity, uncertainty and potential danger, if not self-destruction.

- To gain and earn public trust requires responsible corporate behaviour that society can get behind morally and ethically — a type of social license — which, in turn, requires ultra transparency, demonstrable accountability and meaningful public engagement.

- Sometimes that engagement can be carried out directly between organizations and their consumers, or governments and their citizens.

- But more often, in a complex environment of high risk and uncertainty, public trust depends on the intermediary of an independent regulator.

- A regulator that can cut through all the complexity, look under the hood or kick the tires, so to speak, and reassure the public that all is okay.

- In this new era, where rapidly evolving digital communication and artificial intelligence have become mainstream, that's a tall order.

- Being an effective regulator in today's context requires a different kind of mindset, than even just a decade ago.

- Gone are the days of check-box compliance, case-by-case investigations of individual complaints after the fact, and enforcement of static laws that have become largely out of date, and out of touch with reality.

- As regulators, it's become increasingly difficult to opine on what is or is not compliant, when the law that stands on the books today never even anticipated the very technologies we're trying to regulate.

IPC's vision of a modern and effective regulator with real-world impact

- This is why four years ago, when I began my mandate as commissioner, I set a vision for the IPC as a modern and effective regulator with real-world impact.

- A forward-thinking organization, focused on modern, agile regulatory practices that shape and encourage responsible behaviour, and proactively support a digital future that includes, protects and benefits us all.

- It's about looking at things from the outside in, rather than the inside out.

- In other words, looking at the ultimate impact we want to have in the real world, and then fashioning our actions to bring about that outcome in a timely and relevant way, rather than going through internal machinations and processes, hoping that ultimately, they'll have the intended effect down the line.

- By building collaborative, consultative relationships with organizations out there, on the ground, we aim to promote a culture where compliance with the spirit — if not the letter of the law — becomes part of that desirable outcome, as opposed to a work-around.

- Our office's vision is to enhance Ontarians' trust that their access and privacy rights will be respected through:

    - **advocacy**, by actively advancing their rights in key strategic areas that impact their lives

    - **responsiveness**, by addressing their complaints and appeals in a fair, timely and meaningful manner, and

    - **accountability**, by maintaining Ontarians' confidence in the organizational excellence of our own office and our effectiveness as a regulator

- A lot of nice words, perhaps, but what does this mean in practice?

- Let me give you a few examples.

Examples of a modern and effective regulator with real-world impact

- When section 61.1 of *PHIPA* and an accompanying regulation [O. Reg. 329/04, s. 35] took effect on January 1, 2024, granting us power to issue administrative monetary penalties (AMP), we were very clear from the outset about what our stance would be on this.

- While there is certainly a place for AMPs in egregious cases, we will continue to prioritize education, guidance, and advice, by proactively guiding institutions on how to ensure compliance with Ontario's access and privacy laws.

- We will continue to focus on early resolution and mediation — coaching them to rectify mistakes or omissions, and act swiftly on lessons learned, rather than sitting back, waiting 'til they get it wrong, and slapping them with a fine for it after the fact.

- As another example, we've taken a bold step in updating our *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* under the *Personal Health Information Protection Act*, or PHIPA.

- We modernized the manual by taking into consideration the evolving security risks and cyber threats that institutions face, to ensure they aren't just compliant but resilient in today's evolving landscape.

- The manual takes a much more risk-based approach that involves a more focused and in-depth review of key high-risk areas rather than employing a superficial, soup to nuts, kind of checklist approach to compliance.

- To enhance our ability to respond to complaints in a timely and meaningful manner, we've made some important changes to our code of procedure for processing FOI appeals under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and its counterpart,

the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) that came into effect on **September 9**.

- One of these changes was to introduce an expedited appeal process to streamline and resolve straightforward cases, significantly reducing processing times.

- Other changes involve firming up timelines, setting file processing limits and closing abandoned files.

- These updates are part of our commitment to being more pragmatic and relevant, and providing Ontarians with timely consideration of appeals and giving parties the answers they want and need to get on with their lives and make informed decisions accordingly.

- It's about gaining efficiencies, being fair to all those who seek out our services, holding ourselves accountable to Ontarians, and making sustainable use of our limited resources in an increasingly data driven world, all the while respecting rules of procedural fairness and being transparent about our appeal procedures.

- The Superior Court of Justice, in a decision of just a couple weeks ago, re-emphasized the longstanding principle that it will not intervene in administrative proceedings unless there are exceptional circumstances.

- The court recognized that the IPC, like all administrative tribunals, has limited resources, and should be able to fashion its general administrative practices and procedures accordingly.

- Early this year, in February, we issued our second Transparency Challenge, calling on Ontario's public institutions to share creative examples of projects of open data and transparency.

- Our virtual 3D gallery spotlights many of these innovative projects that support government transparency and demonstrate the benefits of open data for Ontarians.

- We want to show positive examples from Ontario's public institutions and inspire others towards greater transparency.

- It's a way, as a regulator, we can celebrate the good work public institutions are doing, rather than just pointing out the bad.

- Part of our mandate is to offer comment on the privacy protection implications of proposed legislative schemes or government programs, or comment on the actual or proposed information practices of data custodians.

- Organizations are welcome to approach my office for policy consultations and seek our feedback on new programs, projects, technologies, or processes with regards to the privacy and transparency implications.

- To formalize this process, we issued consultation guidelines a couple of years ago that made explicit the rules of engagement around the process, to set out expectations, clarify the scope of confidentiality undertakings, and need for impartiality.

- We are hoping to eventually evolve this policy consultation process into a kind of regulatory sandbox, that we are exploring.

- This leads me to our *Info Matters* podcast, that's about having in-depth conversations with people from all walks of life on matters of access and privacy, covering a wide range of topics.

- It's about meeting people where they're at, making conversations accessible to a broad public audience, in a different kind of format.

- And, as a regulator, it's about having the humility to ask questions, being open to hearing different perspectives, listening and learning, along with everyone else, on the same playing field.

Strategic priorities

- Another key attribute of a modern and effective regulator is to stay laser focussed on strategic priorities, rather than trying to cover everything and diluting our efforts in the process.

- The work of the IPC is guided by four strategic priorities.

- In developing these priorities and related goals, we gathered input from our stakeholders, the institutions we oversee, and the public we serve, focusing on areas where we are most likely to have the greatest positive impact for Ontarians.

- The priorities are as follows.

- ***Privacy and Transparency in a Modern Government***. Our goal here 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, including AI.

- To support our ***Children and Youth in a Digital World*** priority, we're championing the access and privacy rights of children and youth by promoting their digital literacy and expansion of their digital rights while holding institutions accountable for protecting the children and youth they serve.

- As part of the ***Next-Generation Law Enforcement*** priority, we're contributing to building public trust in law enforcement by working with partners to develop guardrails for the adoption of new technologies and community-based approaches that protect both public safety and access and privacy rights.

- And through the ***Trust in Digital Health*** priority, we're promoting confidence in the digital health care system by guiding health information 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.

- All four of these, as you can see, are about enabling important societal benefits — be it government services, public education, health or public safety — by working with others to proactively establish appropriate guardrails and governance frameworks that help guide institutions to responsibly deploy technologies in a manner that's transparent and accountable to the public, and that fundamentally respects access and privacy rights.

- A common refrain across all four of these strategic priorities has been the need for law reform and modernization.

- Last May, the government of Ontario responded with Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act*.

- Schedule 1 establishes system requirements for public sector entities in the areas of cyber security and AI and sets out rules for the use of digital technologies affecting children and youth under eighteen.

- Schedule 2 amends the *Freedom of Information and Protection of Privacy Act* to introduce stronger privacy protections and oversight.

- While this bill is directly on point with the issues of the day, and represents a promising first step, there is clearly room for improvement.

- My office submitted our recommendations to the legislative assembly on how the bill can be further strengthened.

- If you'd like to read the full submission, it's available on our website at ipc.on.ca.

- One key aspect of the bill is to build a cyber security governance regime.

- Cyberattacks are sadly now a regular feature of the news, and public sector institutions are increasingly becoming the targets, particularly of ransomware attacks.

- The City of Hamilton was hit with a ransomware attack that shut down almost all city phone lines, paralyzed city council, and impacted dozens of services.

- The city has spent millions of dollars to restore its systems and intends to spend close another $34 million between 2025 to 2033 to strengthen the city's cyber security posture.

- Last spring, a ransomware attack targeting five southwestern Ontario hospitals took their systems offline for weeks and forced people to postpone or reschedule surgeries and appointments.

- It was reported that it cost the hospitals approximately $7.5 million to recover and upgrade their systems.

- The Canadian Internet Registration Authority's 2024 CIRA Cybersecurity Survey, revealed some startling statistics about municipalities, universities, schools and hospitals — or the MUSH sector.

- The report, which surveyed 500 cyber security decision-makers across Canada, found that more than half (**55 per cent**) of MUSH sector organizations had experienced a cyberattack in 2024, compared to **38 per cent** in 2023.

- Of these attacks on MUSH sector organizations in 2024, **29 per cent** were successful, compared to **22 per cent** in 2023.

- Cybercriminals know that public institutions process large amounts of personal information and that they simply cannot shut down when faced with a cyberattack.

- They must continue to operate and provide essential services, which makes them particularly vulnerable to ransom attacks.

- While I support the government's intention in Schedule 1 to build a cyber security governance regime, more needs to be done to protect the privacy and security of Ontarians.

- Among my recommendations regarding cyber security:
    - core elements of a cyber security program should be set out explicitly in statute and ensure that any regulations governing those cyber security programs require the inclusion of certain core elements
    - these core elements include the identification and management of organizational cyber security risks, and procedures to minimize the impact of cyber security incidents when they happen
- I also recommend that the IPC be notified of cyber security incidents affecting personal information as part of the mandatory requirement to report cyber incidents to the Minister of Public and Business Service Delivery and Procurement.
- Schedule 1 of the bill also seeks to regulate the use of AI by public sector entities by addressing transparency, accountability, risk management, technical standards, and oversight, as well as certain prohibited uses to be drafted in future regulation.
- We recommended, first and foremost, that the law should enshrine clear statutory guardrails around the use of AI technologies and not leave such fundamental matters to regulation.
- In our submission, we included a set of principles for public sector organizations that are developing or deploying AI systems, namely:
    - before AI technologies are adopted, they should have to meet independent testing standards to ensure they are ***valid and reliable*** and work as intended.
    - AI systems should be ***safe*** and designed for the physical and mental health of people, our economic security, the environment, and be monitored throughout their lifespan.

    - AI technologies should be ***privacy protective*** and developed using a privacy by design approach that anticipates and mitigates privacy risks to individuals and groups.

    - ***transparent*** policies and practices should be adopted that inform people when they are interacting with AI and explain when and how decisions have been made about them using AI.

    - an ***accountable*** governance structure is necessary so that individuals can challenge the accuracy of decisions made about them and seek recourse.

    - most importantly, AI technologies should be ***human rights affirming*** by being fair and equitable for all individuals and communities.

- This last point is especially important when considering historical discrimination and bias against marginalized communities. All the more reason then, to meaningfully engage them in the development and deployment of AI systems and the rules necessary to regulate them.

- My other major recommendation was the need for independent oversight and enforcement. Public sector organizations should be subject to review by an independent oversight body with authority to enforce these principles. Otherwise, it'd be largely an empty shell of government overseeing itself.

- These recommendations are consistent with the joint statement we issued last year with the Ontario Human Rights Commission, urging the provincial government to develop and implement effective guardrails for the use of AI technology in the public sector, addressing safety, privacy, accountability, transparency, and human rights.

- They're also consistent with the principles established together with our federal, provincial, and territorial counterparts addressing responsible, trustworthy, and privacy-protective generative AI technologies, recalling many of these similar principles to mitigate privacy risks and promote the safe development of AI technologies.

- And likewise, consistent with two unanimous resolutions adopted internationally at the 45th Global Privacy Assembly, comprised of more than 130 data protection authorities around the world — one on generative artificial intelligence systems and the other on artificial intelligence and employment.

- Schedule 1 also proposes to regulate, through ministerial directives and regulations, digital technologies aimed at children and youth under 18 years.

- We stressed the need to create and implement standards for digital technologies that respect the rights of children and youth and are consistent with the values of personal autonomy, dignity, and individual self-determination.

- Among our other recommendations would be to remove certain sections from the bill prescribing how school boards and children's aid societies shall collect, use, retain and disclose digital information, that risk creating regulatory redundancy with existing privacy laws and may result in inconsistent requirements.

- Instead, we call for strengthening privacy protections of children and youth in already existing privacy laws, to ensure a more consistent, coherent, and seamless privacy regulatory regime.

- Concretely, this should include deeming personal information of children to be sensitive information — that has to be taken into consideration when developing PIAs, for example, or establishing reasonable safeguards.

- And again, we strongly recommended providing for independent oversight and enforcement.

- Bill 194 introduces mandatory breach notification, an explicit requirement to conduct privacy impact assessments, a new privacy complaint and investigative regime, with order-making powers

- While strongly in favor of this reform, we nonetheless recommended expanding the grounds for individual complaints, and broadening the

commissioner's investigative powers to allow onsite examination of technical systems.

- Finally, recommended that MFIPPA be reformed as soon as possible to mirror the same changes as in FIPPA. For decades, these two sister pieces of legislation have operated in tandem to ensure equivalent protection of citizens' privacy in both provincial and municipal institutions.

- To strengthen one, but not the other, would be to introduce significant divergence in the privacy requirements in the provincial and municipal sectors which, from the perspective of the average Ontarian, would make zero sense.

Conclusion

- We are standing at a pivotal moment. Change is happening fast, but with that comes the incredible opportunity to shape a digital future that works for all of us.

- If the federal bill, C-27, does not go through as planned, Bill 194 might be the only game in town.

- It's a chance for Ontario to show digital leadership through robust laws and regulations that protect privacy, support innovation, and reflect our province's unique circumstances and economic reality.

- It's all the more reason then, to get it right.

- As we enter a new digital era, both the public and private sector have to prioritize transparency and accountability upstream to ensure privacy and human rights are protected downstream.

- These are the keys to securing the public's trust in the responsible adoption of technologies and innovative approaches that will shape a digital future that benefits of us all and leaves no one behind.

- Thank you.