April 2021

IPC Strategic Priorities 2021–2025

Information and Privacy Commissioner of Ontario

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

Contents

Commissioner Message

When I started my five-year mandate as Information and Privacy Commissioner of Ontario in July 2020, I committed to focusing on the access and privacy issues that matter most to Ontarians. As part of this commitment, my office began a strategic planning exercise to identify the priorities that will guide the IPC's work throughout my term as commissioner. The purpose of this exercise was to identify how we can better focus our energies and allocate our resources to advance those key access and privacy issues:

- that are of greatest relevance to Ontarians today and in the future
- that fall squarely within the IPC's jurisdiction
- that the IPC is well-suited to lead, given our strengths, capacity, and ability to partner and collaborate
- on which the IPC is most likely to have a positive and significant impact

The mandate of the IPC includes resolving access to information appeals, investigating privacy breaches, reviewing privacy policies and information practices, conducting research, and educating the public about access and privacy rights. In carrying out this mandate we issue decisions and reports, develop practical guidance and public education materials, publish research papers, provide advisory services and participate in speaking engagements throughout the year. Given limited resources, we often have to make difficult decisions about which activities to carry out or advance.

Succinctly put, priorities will assist us in making these tough strategic choices.

That said, we also recognize the need to stay flexible. While strategic priorities will help guide us, we cannot predict everything that will happen over the next few years and will have to remain open to the potential for priorities to shift in response to the unknown. The COVID-19 pandemic that caught the entire world off-guard and overwhelmingly altered how we work and live our day-to-day lives is a case in point. Difficult times like these can inspire change, and even growth, as long as we maintain the agility to deviate from the course originally charted, to face unexpected challenges, and find alternate ways of navigating new obstacles in our path.

Taking these factors and realities into account, and having considered the valuable feedback of stakeholders as well as our ad hoc strategic advisory committee, I am pleased to set out the IPC's strategic priorities for 2021-2025:

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

Within each of these strategic priority areas, it is important to situate the appropriate role of the IPC. To be clear, our mandate is not to champion these modernization or digitization initiatives as an end in and of itself — this is the work for others to do. Rather, our role as an independent Office of the Legislature remains essentially and fundamentally focussed on promoting and protecting Ontarians' privacy and access rights *within* each of these strategic areas. In so doing, our dual mission is to help enable *and* enforce compliance with Ontario's access and privacy laws and thereby do our part in helping build citizens' trust in the institutions and organizations that serve them.

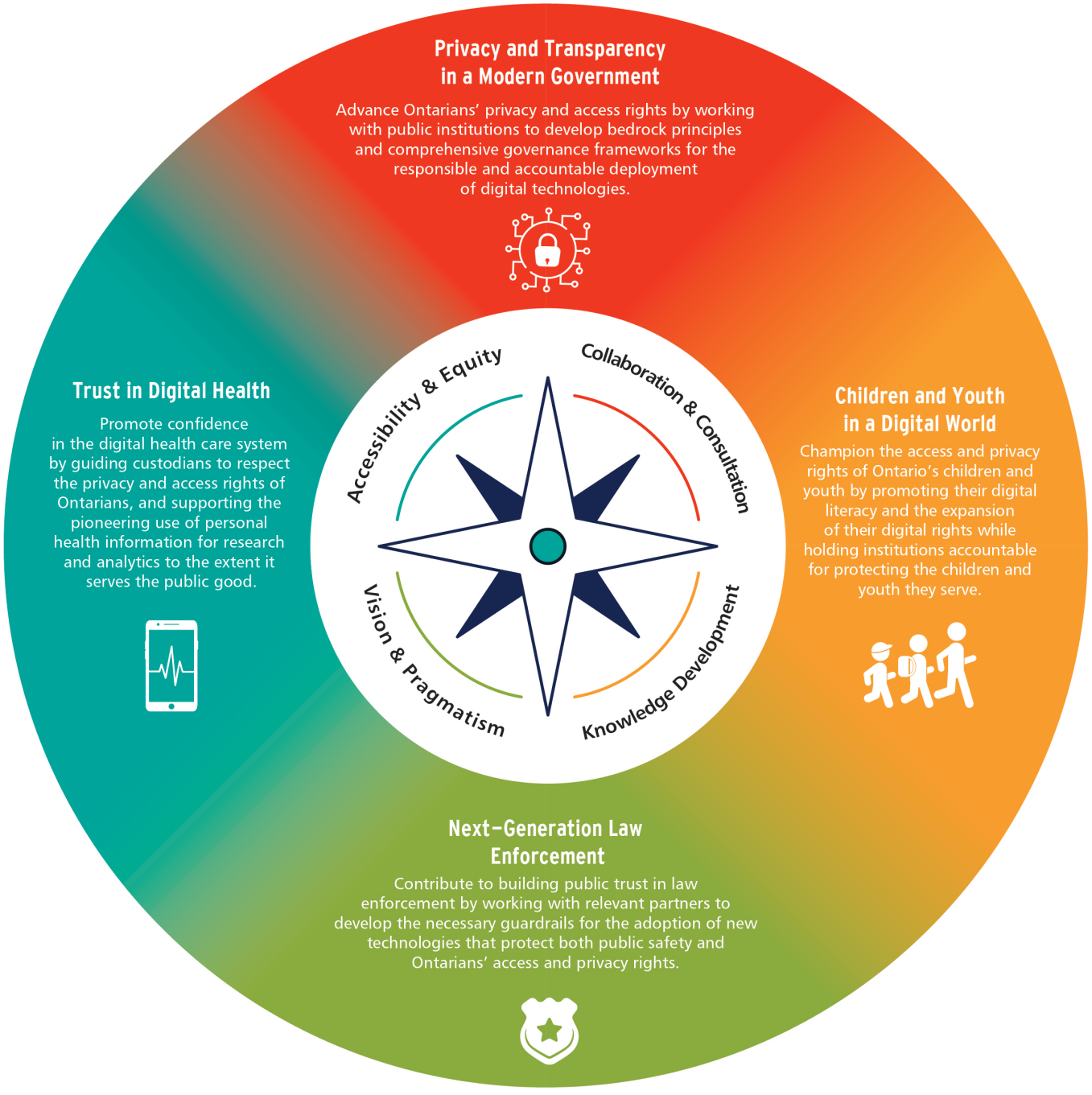
More specifically, our goals in each strategic priority area are as follows:

Privacy and Transparency in a Modern Government	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.
Children and Youth in a Digital World	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.
Next-Generation Law Enforcement	Contribute to building public trust in law enforcement by working with relevant partners to develop the necessary guardrails for the adoption of new technologies that protect both public safety and Ontarians' access and privacy rights.
Trust in Digital Health	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 have also identified four cross-cutting approaches that we will adopt across all strategic priority areas as we work to achieve our stated goals:

1. We will consider accessibility and equity issues to help reduce disparate outcomes on marginalized communities.
2. We will be bold and aspirational in our vision, but also stay grounded in pragmatism.
3. We will strive to be consultative and collaborative with relevant partners and stakeholders.
4. We will develop the knowledge, skills and capacity needed, both internally and externally, to advance these strategic priorities.

IPC Strategic Priorities 2021 - 2025



At the time of issuing this report, the IPC oversees compliance with four laws:

- ***Freedom of Information and Protection of Privacy Act (FIPPA)***
- ***Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)***
- ***Personal Health Information Protection Act (PHIPA)***
- Part X of the ***Child, Youth, and Family Services Act (CYFSA)***

It is possible that the IPC's mandate may be expanded by the introduction of an Ontario private sector privacy law. Should the government decide to move in this direction, the IPC must be able to pivot its focus to include this important priority and to operationalize and implement the new law. For this reason, we have developed a fifth provisional priority so that we are ready to hit the ground running should a new private sector privacy law be adopted:

(Provisional) Made-in-Ontario Private Sector Privacy Law	Develop the foundational building blocks and oversight mechanisms for implementing Ontario's private sector privacy law in a manner that protects privacy, supports responsible innovation, and accords with our province's unique circumstances and economic reality.

On behalf of the IPC, I would like to thank the ad hoc strategic advisory committee members for the ongoing support and sage counsel they provided throughout this process. I would also like to express our most sincere gratitude to the nearly 60 respondents who gave their precious time and made considerable effort to file submissions as part of our public consultation process. While we recognize that we did not hear from all stakeholders, we were very encouraged to see such a high level of engagement from those who participated in the process and provided thoughtful insights into what the IPC could or should do over the next few years, and offered suggestions on how we might collaborate with others. As this exercise is about selecting priorities and making tough choices, we clearly cannot onboard all of the excellent ideas we received, but we have considered them all. We will continue to do so as we move towards implementation and welcome the opportunity to work with interested stakeholders.

Listening to Ontarians

In December 2020, the IPC published a **Strategic Priority Setting Consultation Paper** and created an online form seeking public comments. We also directly contacted over 100 stakeholders encouraging them to participate in the consultation. We received 59 submissions from a wide range of stakeholders and sectors, including municipalities, universities, hospitals and health sector institutions, law enforcement agencies, Crown corporations, private sector organizations, researchers, think tanks and advocacy groups, a legal aid clinic, and private individuals.

We also created, and consulted with, an ad hoc **strategic advisory committee**, made up of 18 experts from a broad range of sectors including academia, civil society, provincial and municipal governments, health organizations, children's aid societies, and law enforcement, as well as representatives from the private sector (**see Appendix A for the composition and terms of reference of the committee**).

The process began in the summer of 2020 (**see Appendix B for a description of the process**), when the IPC identified a long list of potential strategic priorities. This long list was based on a series of internal consultations among IPC staff across all departments to canvass the most pressing concerns they hear from members of the public and relevant stakeholders in their day-to-day work. Our internal consultations were supplemented by the results of IPC's ongoing environmental scanning function and in-depth policy research into privacy and access trends in Ontario, Canada, and around the world. Following external consultations with our ad hoc strategic advisory committee and using predetermined criteria (**see Appendix C for a list of the criteria used**), we developed a shortlist of six potential strategic priorities and four cross-cutting approaches (**see Appendix D for a recap of the shortlisted priorities and cross-cutting approaches**). We presented this shortlist to the public and sought their input in our public consultation.

What We Heard

Overview

In general, submissions were very supportive of the IPC's priorities setting exercise and the consultation paper. Many respondents supported all of the identified potential priorities and did not necessarily identify their "top three." Very few excluded any priorities outright. Where a respondent disagreed with the inclusion of a particular priority, it was because they felt it was not relevant to their particular interests or mandate or that sufficient work was already underway in that area.

We were encouraged by the extent to which stakeholders described their own strategic priorities and showed themselves interested in collaborating with the IPC in advancing a specific area of interest. In particular, they expressed a willingness to work with the IPC in developing new frameworks, guidance, and resources, which will help enable broad stakeholder engagement and ensure they are practical in their implementation.

Many respondents commented on how interconnected these priorities are, recognizing the growing overlap between them due to emerging technologies and inter-sectoral initiatives that are increasingly blurring boundaries.

Several also advised of the importance for the IPC to maintain a careful balance between its dual role of enabling modernization initiatives by advising on privacy and access considerations, and overseeing institutions to hold them to account for their statutory responsibilities.

Many submissions provided detailed proposals for how the IPC could implement each priority, if it were selected. We do not summarize all of these details here. Still, these valuable proposals will be considered again at the implementation phase, as the IPC develops its action plan for operationalizing each of the selected priorities. Several submissions called on the IPC to acknowledge and address the possibility of Ontario adopting a private sector privacy law, with one stating that our "priorities should be adjusted to include recognition of the IPC's expanded role," which would likely require the dedication of significant resources.

Given the overall positive and supportive nature of the responses, we focus below on the key considerations and recommendations made by respondents that we took into account in adjusting, refining, and ultimately selecting, our strategic priorities and related goal statements to ensure their overall success.

Government Digital Service Delivery

This potential priority was broadly supported by respondents, recognizing the opportunity to promote efficiencies and equity by centralizing service delivery, while also leading in privacy-sensitive innovation. One municipality, for instance, envisioned that with IPC guidance and advice, it could become 'best-in-class' with respect to digital service delivery.

Respondents supporting the selection of this priority emphasized the need for standardization and consistency across the public service, transparency about how digital services are designed and implemented, and appropriate independent oversight, including through mandatory privacy impact assessments. Others agreed with our view that establishing and managing digital identities and developing age-appropriate gateways are foundational to this work.

Municipalities stated that they have a unique perspective on this priority and seek assurances that they will be consulted. For instance, it was noted that while the provincial government (and some municipalities) have their own information technology departments with multiple full-time staff members, smaller municipalities may rely on joint-service agreements with other municipalities for basic services. For rural and Northern communities, access to reliable and affordable broadband is also a challenge. While they understood that it is not the IPC's role to solve these challenges, they argued that the IPC should take a whole-of-service perspective to its activities, taking into account not just the perspective of the access requestor and privacy complainant, but also of municipal administrators.

Some respondents identified their own challenges with digital service delivery, such as ensuring accountability when working with third-party service providers. They expressed the desire and need to work with third parties but recommended that the IPC's priority work include an examination of the steps necessary to provide sufficient reassurance to Ontarians that use of a third party will not become "personal information conduits to feed commercial interests" and negatively impact individual privacy. To "embrace a digital future, guidance regarding agency agreements with private sector companies would be helpful,"

said one respondent, as would "an information framework for digital collection including information security content."

One submission called for a "user-centric" approach to designing digital services, while another emphasized the need for a "privacy-first" approach. Many saw the importance of ensuring transparency in government digital service delivery and holding government institutions accountable for their digital initiatives particularly due to their impact on low-income and historically marginalized populations.

Some respondents suggested expanding this priority area to integrate the unique needs of Crown corporations and the role of broader public sector institutions beyond government.

Finally, one university reminded the IPC of the importance, when providing trusted advice, that it remain a "true, third-party, autonomous and independent organization, separate from governmental influence, pressure and sway."

Transparency and Open Government

Though less than *Government Service Delivery*, there was significant support for the inclusion of *Transparency and Open Government* as an IPC priority — with one submission seeing both these priorities "as going hand in hand" on the understanding that the complexity that comes with modernizing information systems should be accompanied by greater transparency and accountability.

A submission from the municipal sector stated that openness is at the heart of how municipalities make decisions and transparency is important for building and maintaining trust. Another submission affirmed that encouraging openness supports evidence-based decision-making and "prevents ideologically driven perspectives from guiding policy." The benefits of transparency, one stated, should be accessible to all Ontarians and not only those with money and resources.

One submission suggested that the goal of "promoting" transparency and open government was rather soft and suggested being more proactive (e.g., "driving" transparency).

Though some saw this priority as the cornerstone of democracy, the limited non-support for the priority tended to be based on the view that there is already a significant amount of work that has been done towards open government, or is underway in this area.

A number of submissions encouraged the IPC to develop practical guidance in addition to policy or high-level frameworks. For instance, one submission proposed "case studies which set out the entire collection-to-openness data lifecycle (including discussions of success points or design patterns)," while others proposed toolkits and information for end-users and "resources that outline how to execute proactive transparency step-by-step, with promising practices on reducing administrative burden." Many saw building on IPC's ***De-Identification Guidelines for Structured Data*** as an important means of enabling greater transparency and open government.

Multiple submissions mentioned the need to modernize public sector laws with suggestions on reducing strain on the freedom of information system, including through proactive disclosures and the need to address frivolous, vexatious or abusive access to information requests that pose resource challenges for government institutions with little benefit to taxpayers. These submitters noted that, at a minimum, the IPC should consider the potential that bad actors will take advantage of any additional transparency or openness requirements when creating (or analysing existing) frameworks. They stated that such bad actors are not a reason to abandon transparency initiatives, but they should also be considered in the development of new processes.

A small number of stakeholders recommended that the goal statement be reframed to reference the requirement to protect commercial information in appropriate circumstances.

Finally, one public interest group pointed out that proactive disclosure better enables organizations like theirs "to play a role in public accountability."

Responsible Use of Data for Good

Responsible Use of Data for Good was among the more frequently recommended priorities. Submissions from the health sector tended to be particularly enthusiastic about this priority in combination with *Trust in Virtual Health*. One noted that access to data and artificial intelligence would foster the innovation needed to provide people the care they deserve and another noted that this priority would apply to the education and transportation sectors as well. Some respondents cautioned that "innovation" should not be seen as a justification for privacy-invasive practices while others called for a clear, neutral, and bias-free definition of "socially beneficial purposes."

A small number of submissions stated that they did not consider this to be a priority area in itself, but rather a consideration underlying other strategic priorities.

Many respondents recommended that the IPC focus on practical guidance (such as case studies and lessons learned), rather than theoretical frameworks (which they viewed as already the subject of significant work in Canada and internationally). One pointed to the need to address what they viewed as the cumbersome processes around data sharing agreements. Other areas identified as being in need of practical guidance included explainability of artificial intelligence systems, responsible use of personal data in training artificial intelligence systems, de-identification, the intersection between privacy and ethics, clarity around concepts such as data trusts and group privacy, and governance frameworks to address the increasing role of commercial actors in the public sphere.

With respect to the goal, multiple submissions argued that it should be revised to explicitly reference "… while also protecting the personal information of individuals." Though this may be implied in the reference to the "responsible" use of data, they stated that it would be beneficial for this balance to be made explicit. Some also suggested expanding the goal beyond "frameworks" to include "resources," and adding a dimension of "public engagement" or "public awareness."

A provincial ministry viewed Data for Good as "the principle that the use of data should improve equity and that data should be leveraged to benefit Ontarians, Canadians and the world, in a manner that supersedes the biases introduced by corporate priorities or institutionalized practices." It suggested that the IPC continue to support guidelines and mechanisms to advance this principle, and address some of the challenges.

One municipality suggested that clear guidance on de-identification standards, and appropriate levels of technical controls would greatly assist in "cutting down on reticence risk," while another submission emphasized the need to protect individuals (and groups) from the consequences of analyzing even de-identified data.

One submission recommended that "Data for Good" be replaced with "Data for Social Value" which has more significant meaning based on input of individuals and communities, whereas public good tends to be unilaterally defined.

Lastly, one submission spoke of the possible establishment of data-trust-like entities called central data facilities over which the IPC might have a key supervisory role comparable to the one it already has in respect of prescribed entities under Ontario's health privacy law (PHIPA). When it comes to data trusts, another submission agreed with the various questions raised in IPC's consultation paper, and called for a comprehensive multi-stakeholder consultation process to begin to address them.

Access, Privacy, and Youth

Access, Privacy, and Youth was also a widely supported potential priority. However, some differences of opinion emerged with respect to the IPC's goal and proposed approach.

For instance, one submission considered access and privacy for children and youth as a cross-cutting theme, instead of a discrete priority.

Some respondents supported the goal as-is. One submission noted that the phrase "… helping youth exercise their independence …" implies ongoing assistance from the IPC, whereas a term such as "empowering" or "enabling" would better capture the ultimate goal of youth being able to make privacy decisions independently. To do this, they recommended that the IPC focus its goal on getting an appropriate curriculum into Ontario classrooms (including science, technology, engineering, and mathematics or STEM courses), and teaching students about issues like online safety and encryption. Others recommended that the IPC develop guidelines and lesson plans for digital literacy among children in much earlier grades.

Some saw the goal statement as minimizing the role of parents or guardians. They stated that parents or guardians should also be empowered to support, or act in place of, the children in their care, particularly given the critical role they play as "initial 'gatekeepers' of Internet access for their children." Respondents suggested IPC could help support parents by educating them about privacy concerns of children and increasing their awareness of available IPC resources, educational curriculum, and digital literacy campaigns.

A third approach argued that the IPC is focusing on the wrong side of the equation. Instead of considering whether youth are adequately equipped, the IPC should focus on whether institutions are meeting their obligations with respect to protecting, and enabling access to, youth information and creating environments that promote their autonomy. For some, this meant increased scrutiny of, or engagement with, those who work with youth such as schools and children's aid societies. Others pointed to the need to protect youth from private sector digital services, apps, consumer devices and social media. Multiple submissions also raised the need to improve the vetting of free software tools deployed in classrooms.

Respondents urged that when developing youth-related policy, it is important to recognize the diversity of youth and the circumstances in which they interact with government, health care, and service providers in the child welfare sector. The IPC was cautioned against a one-size-fits-all approach, noting that with youth — as with privacy in general — the notion of an 'informed choice' will differ across various situations, and requires flexibility. One called for the need to balance "parents' right-of-access with mature minors' right to self-determination," while another stated, "guidance on age of majority for making decisions about personal health information would be helpful for healthcare professionals, youth and their family members."

Several submissions pointed out that while children and youth are vulnerable, those in low-income or historically marginalized populations are even more so. Open data and proactive disclosures by relevant stakeholders should likewise be promoted to identify and address these social inequities.

Next-Generation Law Enforcement

The *Next-Generation Law Enforcement* priority received the least number of overall comments and top three priority rankings. However, those respondents who did explore this issue generally considered it to be of great importance, particularly concerning marginalized communities. Algorithmic policing was noted as having real and substantial impacts on the lives of Ontarians.

Submissions generally focused on the need for transparency and oversight. One submission noted that Ontario — as the largest province in one of the leading liberal democracies in the world — should take the lead on these issues. This could include a more proactive oversight role for the IPC, and collaboration across police services and municipal, provincial, and federal government agencies on any necessary and appropriate access and privacy frameworks. Regardless of the mechanism, it was generally felt that Ontarians should know how and when police and law enforcement agencies were collecting information about them and have confidence these activities take place with appropriate oversight.

In the event this priority was selected, the IPC was encouraged to work with the Ontario Human Rights Commission and explicitly include promoting transparency in the associated goal statement.

It is worth noting that the submission received from a law enforcement agency was also supportive of this priority, recognizing the mutual interest in responsible use, proper oversight, and appropriate protection of personal information, as well as the overall need to increase police-public trust. Given the rapid pace of evolving technology and constraints on resources, it was noted that rather than police services across Ontario each separately undertaking privacy impact assessments of a new process or technology, it would be more efficient to be guided by a common set of provincial guidelines developed by, or in consultation with, the IPC. These guidelines could also include features for customization on a case-by-case basis. It was also suggested that the IPC convene a provincial working group with broad, cross-sectoral representation from police, first responders, investigators, privacy and legal experts, with further engagement of Crown counsel, defence counsel, civil libertarians, human rights advocates, and those with lived experiences from marginalized communities.

Trust in Virtual Health

Trust in Virtual Health was one of the areas most often identified as a top three priority in submissions. As one submission stated: "Canada has an opportunity to be a world leader in the development and implementation of digital health technologies, including the adoption of artificial intelligence and machine learning for health." Another pointed to the "tremendous opportunity in virtual health to bring practical, scalable methods into common use" and "integrate concepts of privacy engineering into innovative solutions for health care delivery and health tech more broadly."

Some suggested the need to support individuals as they gain greater control over their health information through personal health portals, digital health apps and body sensors, and the need to support health organizations with respect to information security issues, such as managing cybersecurity threats.

The overlap between this priority and *Responsible Use of Data for Good* was highlighted by many respondents, with multiple submissions noting the potential benefits for Ontarians by enabling artificial intelligence in health research. Similarly, overlaps with *Government Digital Service Provision* were highlighted, noting that as occurred with government services, the rapid uptake of digital services in the health sector accelerated by COVID-19 did not necessarily allow for consistent and adequate scrutiny of platforms.

One group recommended the IPC consider evaluating the changes that have come about in response to COVID with "an eye to addressing health care delivery outside of an emergency" and how personal health information should continue to be managed once the threat of COVID-19 has subsided. Another identified the need to help institutions reset by providing clear guidance to those that may have quickly adopted virtual solutions to ensure prompt delivery of health care, outweighing privacy and security concerns at the time. A third recommended the IPC continue to keep a watchful eye on new categories of personal health information (such as COVID-19 test results or vaccination status) to protect individuals from potential privacy and discrimination risks, particularly in insurance or employment contexts. A fourth identified the importance of "modernizing and future-

proofing policy and legislation" to reflect changes brought on by the pandemic in a manner that reflects the views of Ontarians.

A respondent recommended that should this priority be selected, explicit reference should be made to principles of trust, dignity, fairness, participation, and security, bearing in mind that the elderly are the most frequent users of Ontario's health system and yet "may not always have the same level of digital literacy as the rest of the population."

One submission made the point that, as drafted, this priority appears to focus entirely on physical health, to the possible exclusion of mental health. Given the rapid expansion of services such as online therapy, they suggested that this priority area should specifically include mental health.

One respondent thought that the goal description was too broad, noting that the health analytics involved a different toolbox than virtual health while recognizing some overlap. Another recommended separate goal statements in respect of virtual health and health data analytics. Yet others recommended that this priority, if adopted, be renamed *Trust in Digital Health* to reflect that it speaks to more than the virtual provision of healthcare.

Lastly, the overlap between health, law enforcement, and child protection was identified as an area where more guidance is needed.

Cross-Cutting Approaches

Respondents were generally satisfied with the proposed cross-cutting approaches, and few comments were submitted except to acknowledge the particular importance of the proposed focus on equity and accessibility. Privacy is a fundamental human right, it was noted, and one that enables the exercise of other rights. Scrutiny of activities under Ontario's privacy laws, it was argued, should include or be based on the recognition of this.

One submission recommended that, within the *Equity and Accessibility approach*, the term "vulnerable and marginalized people" be replaced with more person-centred language such as "people experiencing structural vulnerabilities or marginalization."

Other respondents put forward other potential cross-cutting approaches. These included: enabling innovation, engagement with other Ontario regulators, ensuring privacy compliance through a human rights framework, re-envisioning data protection for genomics, and lessening the overall burden on individuals with a focus on accountability.

One recommended adding standardization as a cross-cutting approach can support the implementation of all strategic priorities, facilitate their management over time, and facilitate IPC's interaction with other organizations.

Others urged the IPC to consider the increasing "blurring of strict distinctions between the public and private sectors" and the need to respond to the realities of an innovative public-private sector economy within a broader human rights framework.

What We Decided and Why

Following extensive analysis of the nearly 60 submissions received and having carefully considered the advice of our ad hoc strategic advisory committee, we have decided to:

- *Merge the two government-centric priorities (Government Digital Service Delivery and Transparency and Open Government):* We agree with the observation that privacy protection and transparency must go hand-in-hand when modern government systems are introduced, with the understanding that the latter (transparency) must include, but is not limited to, a robust access to information regime. As two sides of the same coin, we have combined them to create our new priority: *Privacy and Transparency in a Modern Government*. To ensure we remain focussed on what could otherwise become a vast and unwieldy priority area, we will hone our efforts to develop the fundamental access and privacy building blocks for governments to use when introducing any new digital technology or system. Taking a comprehensive meta-level approach, rather than attempting to advise on each application, we will work to develop the bedrock principles, common tools, and governance frameworks that will ground such digitization efforts in values of privacy, accountability, fairness, and transparency. For example, this might include working with others to develop templates for algorithmic impact assessments, designing governance frameworks for managing public-private partnerships, securing approaches for validating and authenticating digital identity, and updating our de-identification guidelines to take into account new forms of privacy enhancing technologies.

- *Clarify the scope of the Trust in Digital Health priority:* We agree with feedback indicating that this priority should encompass not only the access and privacy aspects of delivering virtual health, but also the digitization of health information. This includes associated opportunities and risks of data analytics, research, and use of artificial intelligence and machine learning tools to evaluate health systems and improve population health. To reflect both of these dimensions, we will use the term digital health rather than virtual health. This will allow us to integrate within this strategic priority several elements of the previously proposed *Responsible Data for Good* priority to which many stakeholders responded very favorably and enthusiastically. When speaking to this priority, we will be clear that health includes both mental and physical health.

- *Refine the various goal statements:* Goal statements are a critical component of this priority setting exercise, as they serve to clarify the scope of the work we will carry out under each priority, and establish a standard against which our progress can be measured. We have carefully reconsidered and further refined each of our goal statements in light of feedback received during the consultation process to ensure they are specific, measurable, and actionable. This required some balancing to consider our dual responsibilities as trusted advisor to help enable transparent and privacy-respectful treatment of data, and as independent regulator holding institutions to account for their decisions and actions. We also took care to ensure our goal

statements were sufficiently broad to cover off critical aspects of the priority area, while not being so broad as to become a catch-all or so generic as to be unclear and meaningless as a priority.

- *Acknowledge the potential adoption of a private sector privacy law:* We agree with several respondents who advised us to be prepared should the government introduce a made-in-Ontario private sector privacy law. If such a law comes to pass, it would likely have a significant impact on our work and require extensive effort to prepare for its coming into force and implementation. In other words, it would inevitably become an additional priority of ours. Acknowledging that the Ontario government has not yet made its decision on this matter, we nonetheless believe it would be prudent for us to be well prepared to respond to such an eventuality. For this reason, we have articulated a fifth, provisional priority, a *Made-in-Ontario Private Sector Privacy Law*, and drafted a related goal statement to allow us to quickly pivot as needed and be ready to deliver on our expanded mandate and related expectations.

What's Next

With our strategic priorities identified, it is time for us to implement them. Our immediate next step will be to develop short- and long-term action plans for operationalizing each priority, as well as criteria for measuring and evaluating our work and reporting on our progress over time. In so doing, many of the excellent ideas we received during the consultation process about what the IPC could, or should do, in each priority area will be considered as we make and communicate our plans.

We look forward to ongoing collaboration and consultations with various stakeholders on how best to achieve our stated goals and to hearing more from Ontarians about their access and privacy concerns. Together, we will strive to think creatively and act proactively to advance Ontarian's privacy and access rights in these strategic priority areas over the next few years.

Appendix A: The Ad Hoc Strategic Advisory Committee

Membership

Matthew Anderson, President and CEO, Ontario Health

Lisa Austin, Chair in Law and Technology, Faculty of Law, University of Toronto

Vass Bednar, Executive Director, Master of Public Policy in Digital Society, McMaster University

Nicole Bonnie, Chief Executive Officer, Ontario Association of Children's Aid Societies

Rodney Burns, CIO, Alliance for Healthier Communities

Robert Fay, Managing Director, Centre for International Governance Innovation

Rebecca Finlay, Vice President, Engagement and Public Policy, Canadian Institute for the Advancement of Research (CIFAR); Acting Executive Director, Partnership on AI

Charles Finley, Vice Chair of Waterfront DSAP/CXO, Futurpreneur Canada

Matthew Johnson, Director of Education, MediaSmarts

Satyamoorthy Kabilan, Executive Partner, Gartner Inc.

Vivek Krishnamurthy, Executive Director, The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), University of Ottawa

Eric Labelle, City Clerk and Solicitor, City of Greater Sudbury

Micheal Miller, Executive Director, Association of Native Child and Family Service Agencies of Ontario

Christopher Parsons, Senior Research Associate, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

John Roberts, Chief Privacy Officer and Archivist of Ontario, Ministry of Government and Consumer Services

Teresa Scassa, Canada Research Chair in Information Law and Policy, University of Ottawa

Colin Stairs, Chief Information Officer, Toronto Police Service

Laura Tribe, Executive Director, OpenMedia

Terms of Reference

Approved: October 28, 2020

Purpose

The purpose of the IPC *Ad Hoc* Strategic Advisory Committee is to provide independent, expert advice to help ensure a broader range of interests and perspectives are considered and applied throughout the IPC's strategic priority-setting process.

Mandate

The role of committee members is advisory in nature. More specifically, the mandate of the committee is to advise on:

- IPC's priority-setting planning process and stakeholder engagement
- potential strategic access and privacy priorities for 2020-2025, and
- public communications about the process and the strategic priorities.

Meetings

The Committee will hold a minimum of three virtual meetings to be held in October 2020, November 2020 and January 2021. Teleconferences and email consultations may take place in between meetings, on an as-needed basis.

Membership

Members of the Committee have been selected for their visionary leadership and knowledge in their respective fields. Members are invited to participate as individual experts, informed by their current roles, but not as representatives of their respective organizations. Membership on the committee does not imply endorsement by the IPC of a particular organization, company, product or service.

Meetings are chaired by the Commissioner, and in their absence, one of the Assistant Commissioners.

Term

The term of membership will run from October 15, 2020 until February 28, 2021.

Confidentiality

All written materials provided to participants to inform the Committee's deliberations should be treated confidentially, unless otherwise stated. Roundtable discussions will be held under the Chatham House Rule. Participants are free to use the information received as part of the Committee discussions, but may not identify the name or affiliation of the speaker(s) or the views of individual participants.

Media Comment

Committee members will not undertake media activities in connection with the work of the Committee, unless given prior approval by the Commissioner.

Procedures

Members will make every effort to participate in all meetings. If a member is not able to attend, they must advise the Administrative Coordinator of their absence in advance, and may not send alternate representation in their stead.

Any documentation, including the agenda, will be sent to members by the Administrative Coordinator at least three business days prior to the meeting.

Decisions

As Chair, the Commissioner will seek out and take into consideration the views of all Committee members, individually and as a group. However, the Commissioner and Assistant Commissioners will make the final decision(s) with respect to the consultation process and the selection of the IPC's strategic priorities for 2020-2025.

Remuneration

Members of the Committee serve without remuneration and will be reimbursed by the IPC for any pre-approved expenses related to carrying out their duties, in accordance with the IPC's Finance and Procurement Policies.

Effective Date

These terms will come into force on October 28, 2020 as approved by the Committee.

Appendix B: A Description of the Process

DEVELOPMENT OF PROPOSED STRATEGIC PRIORITIES

September to November 2020

- Consulted with all IPC staff on top issues resonating with Ontarians (through complaints, appeals, inquiries, media requests, etc.)
- Researched and analyzed trends emerging from IPC's daily environmental scanning function
- Developed a long list of potential strategic priorities, narrowed down to a short list of six (6) using defined criteria in consultation with IPC's Senior Management Committee

CONSULTATION ON PROPOSED STRATEGIC PRIORITIES

December 2020 to January 2021

- Consulted with external, ad hoc strategic advisory committee
- Drafted the external consultation paper to gather input from general public and key stakeholders
- Released IPC's public consultation paper and launched public consultation process
- Initiated targeted outreach to over 100 key stakeholders

CONSIDERATION OF PUBLIC AND STAKEHOLDER INPUT

January to March 2021

- Considered responses received through the public consultation process
- Reconvened the ad hoc strategic advisory committee to discuss and deliberate on the public input received
- Selected IPC's final slate of strategic priorities for 2021-2025

RELEASE OF IPC STRATEGIC PRIORITIES 2021–2025

April 2021

- Published final report announcing IPC's strategic priorities for 2021 – 2025
- Began the strategic implementation process and development of action plans in dialogue with key stakeholders

Appendix C: Criteria Used to Shortlist our Potential Priorities

Relevance to Ontarians

- Is the proposed priority of pressing importance to Ontarians and will it continue to be as significant over the next five years?
- Does the proposed priority pose risks of negative impact on Ontarians? Is there an opportunity to help reduce or eliminate such risks?
- Do the risks and impacts affect certain people or groups more than others?

Potential for Impact

- Will addressing the proposed priority advance the purposes of access and privacy laws in Ontario?
- Is there a realistic opportunity to make significant improvements in this priority area within the next five years?
- Is there a leadership gap the IPC can fill in this priority area?
- Are there partners the IPC can collaborate with to achieve greater impact?

IPC Capacity

- Does the proposed priority fall within the IPC's mandate?
- Is the proposed priority well-aligned with the IPC's strengths (including any past work done on the issue)?
- Can the IPC reasonably address this proposed priority area with its current level of resources?

Appendix D: Recap of Potential Priorities and Cross-Cutting Approaches

The six potential strategic priorities that were shortlisted for broader public consultation were:

Government Digital Service Delivery

Proposed Goal: The IPC will be a trusted source of independent advice to government institutions seeking to digitize their services, while holding them accountable for respecting the privacy and access rights of individuals who use such services.

As government institutions shift to digital service delivery, particularly accelerated by COVID-19, it is critical that service improvements and efficiencies do not come at the cost of Ontarians' access and privacy rights. Digital service delivery is not a simple one-to-one conversion of a paper-based process. While the transition to digital service delivery supports greater efficiency, it also gives rise to new privacy considerations. For example, when accessing new digital services, people may need additional tools to securely identify and authenticate themselves. Governments are increasingly looking to link data and share information across departments to streamline and improve services. Security will also be an important consideration, as the shift to online government services makes the digital service platforms and the information they house especially vulnerable to cyberattacks. As well, some digital and online service delivery platforms are designed, built, and operated by third parties on behalf of government organizations, potentially leading to concerns about where those third parties store the personal data of users and how they might use it. Building on its past work in this area, the IPC could support institutions in the shift toward online service delivery by contributing to the development of data sharing standards, providing model data governance frameworks, and developing guidance on privacy and security considerations when using digital platforms.

Transparency and Open Government

Proposed Goal: The IPC will reduce barriers to access government-held information by promoting efficient access-to-information processes, proactive disclosures, and an overall culture of open government, while also protecting the personal information of individuals.

It is critical that people be given access to the non-identifiable information they need to be able to hold their governments to account, express views, and make decisions and choices that form the cornerstone of our democracy. An open-by-default approach to government-held information offers many important social benefits. An overall culture of transparency and openness allows Ontarians to hold their government to account for the

actions and decisions they take in the name of the citizens they serve. Open government supports informed policy debates and enables the freedom of choice needed to uphold the integrity of our public institutions and the pillars of our democracy. Proactive transparency also allows government to gain efficiencies, reduce resource expenditures on processing freedom of information requests, enhance Ontarians' trust in government and accelerate citizen adoption of new programs and initiatives. The IPC has a long history of resolving access to information appeals through mediation and advocating for open and transparent government. The IPC can further build on this work by finding greater process efficiencies in the access to information regime, promoting greater proactive disclosures, and calling for modernized legislative reforms.

Responsible Use of Data for Good

Proposed Goal: The IPC will convene, and work with, relevant partners to develop governance frameworks that support the responsible use of data for innovative and socially beneficial purposes.

To unleash the full potential of data needed to help solve some of society's most pressing problems, it is vital that appropriate governance frameworks be in place to ensure their responsible use. Fostering innovative and entrepreneurial approaches and solutions often requires cross-sectoral sharing of information in collaborative efforts to help address the most complex, challenges in areas such as health, equity, poverty, education, and the environment. Data governance frameworks have begun to emerge to support the responsible treatment of data. The IPC could build on these by focusing its efforts on catalyzing the development of one or more trusted, practical, and privacy-protective data sharing mechanisms. IPC could bring together interdisciplinary, multi-sectoral groups of stakeholders, and draw on their experience to date to develop appropriate data governance frameworks that are fair, accountable, and transparent, in accordance with Ontarians' values and realities.

Access, Privacy, and Youth

Proposed Goal: The IPC will champion the access and privacy rights of Ontario's children and youth, helping them to exercise their independence, protect themselves and make informed choices about their personal information.

It is imperative that the privacy rights of youth are appropriately protected, that they are able to understand how to control the use of their personal information in different contexts, and that they are empowered to learn, grow and develop safely. Jurisdictions worldwide are recognizing that children and youth are a vulnerable group whose information access and privacy rights require special considerations and supports. Strengthening youth privacy and access rights means applying fair information principles such as consent, data minimization, retention, and accountability in age — and culturally — appropriate ways. This includes identifying

and addressing any systemic challenges to access and privacy rights and disparate impacts experienced by children, youth, and their families in marginalized populations. The IPC has positioned itself as a leader in youth privacy and digital literacy issues. Continuing to focus on this strategic area would allow us to further build on our strengths by addressing the many new issues brought about by e-learning and the special considerations arising in vulnerable populations. The IPC could convene a broad range of relevant partners to work towards the creation of a children's access and privacy code for Ontario.

Next-Generation Law Enforcement

Proposed Goal: The IPC will develop and enforce the necessary boundaries to ensure that law enforcement's adoption of new technologies in order to protect public safety, also respects Ontarians' access and privacy rights.

In order to establish and maintain trust between Ontarians and law enforcement agencies, it is crucial that police services and other organizations be transparent and held accountable for the personal information they collect, use and disclose as part of the technologies they deploy and the powers they wield in the name of public safety. Information collection has always been a central function of law enforcement. Still, the extent of collection, and the digitization and automation of this process, have been increasing in recent years, made easier by the use of technology. This trend is likely to continue at an exponential rate, particularly through lawful access to information collected by third parties operating in the private sector. While technological advances may bring efficiencies to police work, they can also have a significant impact on access and privacy rights, if not used in an appropriate and privacy protective manner. The IPC has built strong capacity in overseeing the data management practices of police services and can continue to build on this work in collaboration with police oversight boards, human rights commissions and civil society groups. Given the current spotlight on law enforcement in Ontario and across the country, the IPC has an opportunity to continue to promote a culture of enhanced transparency, accountability, and proportionality in policing by actively consulting on the use of next-generation surveillance technologies before their use.

Trust in Virtual Health

Proposed Goal: The IPC will help support a virtual health care system which respects Ontarians' privacy and access rights and is founded on human dignity and trust.

Trust in how our personal health data are processed is critical for increasing adoption of digital health technologies and ultimately improving health care outcomes for individuals and across populations. The increased digitization of health information, the accelerated move towards virtual health services, and the heightened emphasis on the interoperability of Ontario's digital

health assets have expanded the volume and breadth of organizations involved in delivering health services to Ontarians (including private sector). The expanded application of machine learning and other artificial intelligence techniques can potentially improve individual health outcomes and the overall efficiency of the health care system, but also raise concerns such as risks of false positive and potential discrimination. There is a need for clear and seamless accountability throughout the complex data flows, both within and beyond what is covered by *PHIPA*. The IPC has long been a leader in health privacy issues. Building on our past experience and expertise, and on Ontario's strong health privacy law, the IPC could develop new frameworks in the digital health space, particularly at the intersections between public, private and health sectors. This could include access and privacy guidance for delivering virtual health, promoting use of health data for research and artificial intelligence systems, and enabling Ontarians to safely access, manage and store their own personal information through personal health portals, digital health apps and body sensors.

Cross-Cutting Approaches

In addition to identifying the shortlist of potential strategic priorities, the IPC also reflected on how it could work to advance each priority. We identified four cross-cutting approaches that could be applied across all the priorities to further enhance the impact of our work.

Accessibility and Equity

Applying the dual lens of accessibility and equity to its evaluation of programs and technologies related to its priorities, as well the IPC's own services and processes.

Capacity Building

- Developing IPC's internal capacity by enhancing staff training and gathering knowledge through engagement with diverse stakeholders
- Educating organizations on how they can practically comply with their privacy and access obligations
- Supporting research into privacy-enhancing technologies and other advances in access and privacy
- Empowering individuals to exercise their access and privacy rights

Visionary but Pragmatic

Ensuring IPC's work on strategic priorities is visionary with an eye to the future, while not losing sight of today's challenges and the need for practical advice and guidance.

Collaboration and Consultation

- Consulting, and collaborating with, a range of relevant stakeholders to ensure a holistic approach that reflects multiple perspectives
- Coordinating our efforts with those of other regulatory bodies

IPC Strategic Priorities 2021–2025

Information and Privacy Commissioner of Ontario

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

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

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

April 2021