DECEMBER 2020

IPC Strategic Priority Setting Consultation

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

CONTENTS

WHY DO WE NEED STRATEGIC PRIORITIES?

The trend towards increased digitization has greatly accelerated since the onset of the COVID-19 pandemic. Advances we might have expected to see over a span of several years have taken place in mere months. This shift has the potential to rapidly and profoundly change how Ontarians interact with government and how public institutions, alone or with third-party service providers, deliver public services.

This new digital reality is ushering in significant privacy and access to information issues that need to be anticipated and addressed. To meet the challenges ahead, the IPC is embarking on a strategic planning exercise to identify our office's top strategic priorities for the next five years.

The purpose of this exercise is to focus our resources and energies on advancing those key access and privacy issues:

- that matter most to Ontarians
- 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 with others
- on which the IPC is most likely to have positive and significant impact

This does not mean that we will stop doing what we are statutorily required to do, such as receiving and processing access appeals and privacy complaints. Rather, it means that we will be guided by our strategic priorities when allocating our limited resources and making discretionary choices within our mandate like what research projects to undertake, what guidelines or educational materials to develop, what issues we proactively advocate for, and so on.

In short, strategic priorities will guide the IPC's expenditure of efforts and resources and help strengthen its impact on the matters of greatest relevance and importance to Ontarians.

ABOUT THE STRATEGIC PRIORITY–SETTING PROCESS

The process of identifying potential strategic priorities began by asking IPC staff what are the most pressing concerns they hear about from members of the public and relevant stakeholders. The process was further informed by IPC's environmental scanning function and in-depth legal and policy research we regularly conduct on emerging access and privacy issues. The IPC also consulted with our newly formed external *ad hoc* **strategic advisory committee** of experts who bring diverse perspectives and serve as an independent sounding board for our office. Based on what we learned so far, we have developed a short-list of six potential strategic priorities, on which we are inviting comments and feedback through this consultation paper.

A FEW PRELIMINARY REMARKS ABOUT STRATEGIC PRIORITIES

The shortlisted strategic priorities proposed in this consultation paper are fluid and will necessarily overlap with one another. This is to be expected in our new digital reality, where boundaries have become increasingly blurred. For instance, certain new developments and technologies, such as artificial intelligence, can potentially find their way in any of the priority topics selected. Also weaving through all of the potential priorities is the growing, integrated role that private sector organizations play in the processing of personal information and the delivery of public and health services. Access and privacy issues increasingly span private and public sector privacy laws, human rights laws, and even the *Canadian Charter of Rights and Freedoms*. Part of the IPC's work will be to coordinate efforts with other regulators and relevant stakeholders at these intersections.

We also recognize that this exercise is being undertaken at a time of significant potential changes to the legal landscape in Canada. The federal government has recently introduced a new bill, the *Consumer Privacy Protection Act*, which, if passed, would replace the current *Personal Information Protection and Electronic Documents Act*. The new federal bill would apply to Ontario businesses, unless Ontario were to adopt its own substantially similar private sector privacy law.

The Ontario government recently held a public consultation about the possibility of introducing its own private sector privacy law. The IPC made a **submission** in response to this consultation setting out our thoughts on what should be included in such legislation were it to be adopted. We will continue to be an active contributor in this important public dialogue.

Given these recent developments, we recognize that we may have to eventually adapt our selected priorities in the future — particularly if a made-in-Ontario private sector privacy law is enacted and significantly alters the scope of our mandate.

NEXT STEPS

This strategic planning exercise would not be complete without hearing the valuable perspectives and insights of stakeholders like you. We are asking for your advice and insights about which priorities you believe should guide the IPC's work over the next five years.

We invite you to provide your feedback online at **https://www.ipc.on.ca/guidance-documents/forms/strategic-priority-consultation-form/**, by email to **consultation@ipc.on.ca**, or by mail to IPC Strategic Priorities, 2 Bloor Street East, Suite 1400 Toronto, ON, M4W 1A8 on or before January 15, 2021. To help with your review, we have included questions throughout this paper on which we especially welcome your input. You are free to answer any of the questions you wish and you are not required to answer all of them.

Please note: we will not be making the responses we receive public. Instead, we will publish a summary of what we have learned as part of this consultation in our final report, which will be available at **https://www.ipc.on.ca/about-us/ipc-strategic-priority-setting-consultation/** in **early 2021.**

Once the IPC has selected its priorities, we will develop an operational plan for each priority, including specific goals, objectives, and success measures, along with a roadmap of activities we could undertake over the next five years to achieve them.

ABOUT THE IPC

The IPC was created in 1987 to oversee Ontario's access and privacy laws. These laws set the rules for how Ontario's provincial and municipal governments, public organizations, health care providers, and child and family service providers may collect, use, and disclose personal information. They also provide individuals with the right to access and correct their own personal information and the public with the right to access government-held records more generally. Specifically, 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***)

In carrying out its mandate, the IPC serves both public institutions and the public by:

- resolving access to information appeals
- investigating privacy complaints
- reviewing information management practices of organizations, including prescribed entities
- promoting compliance with applicable privacy and access laws through practical guidance
- researching emerging technologies, their risks, and potential impacts on access and privacy rights
- providing comment and advice on proposed government legislation and programs
- educating the public and other stakeholders about Ontario's access and privacy laws
- responding to media requests about current issues and trends affecting access and privacy rights in Ontario.

The commissioner is an officer of the legislature who is appointed by, and reports to, the Legislative Assembly of Ontario and is independent of the government of the day.

SELECTION CRITERIA

In developing a short-list of potential strategic priorities in this paper, the IPC considered the following criteria. We invite you to keep them in mind when making your comments.

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?

OPPORTUNITY 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 a 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?

With that context in mind, we present our six potential strategic priorities in no particular order of importance. We also propose a high-level goal that sets out what we would hope to accomplish five years from now for each potential priority. We describe what our office has done in each priority area to date, and we suggest some ideas of how the IPC might be able to build on that work in the future. (As noted above, our intention is to develop more detailed operational plans once we have selected our final slate of strategic priorities.)

POTENTIAL STRATEGIC PRIORITY: GOVERNMENT DIGITAL SERVICE DELIVERY

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.

WHY MIGHT THIS BE A STRATEGIC PRIORITY?

As government institutions shift to digital service delivery, it is critical that service improvements and efficiencies do not come at the cost of Ontarians' access and privacy rights.

COVID-19 has accelerated digital service delivery across the government. This method of delivering services is likely to continue even after the pandemic has ended. For example:

- the Ontario government has **stated its commitment** to "becoming the leading digital jurisdiction in the world in order to improve the services the people of Ontario rely on every day"
- the City of Toronto has announced its **Digital Infrastructure Plan**, noting that its approach to digital service delivery requires critical acceleration
- as part of its free wireless network across the GO Transit system, Metrolinx offers riders access to digital entertainment such as books, music, and podcasts
- the Ontario Cannabis Store sells cannabis products to Ontarians through an online sales platform
- ServiceOntario continues to increase the number of services it offers online, such as driver's licence and health card renewals and related address changes

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 and/or establish their eligibility for the desired service (e.g., they may have to prove their place of residence or age of majority). To do this, a government may choose to partner with another organization (such as a bank) with which the individual has previously established their identity, or to issue its own electronic or biometric identifier that serves as proof of identity. Each method poses its own privacy, security, and equity challenges.

Security will 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. Cybercriminals are becoming increasingly sophisticated and capable of illegally accessing information or disrupting the service altogether as a means of extorting significant ransom payments.

Some digital and online service delivery platforms are designed, built, and operated by third parties on behalf of government organizations. This often leads to additional concerns about where those third parties store the personal data of users and how they might use advanced data analytics to segment users and make certain inferences based on usage patterns, risk profiles, and other personal characteristics. The introduction of third party service providers also introduces the potential that they may re-use the personal information for their own commercial purposes.

To achieve greater efficiencies, the use of digital services is often accompanied by attempts to link data about Ontarians and share it with other government departments or organizations. Having to collect (and recollect) information for different purposes and keep it in separate information silos has long been a point of frustration for government organizations. Governments today are looking to share information across departments to streamline service delivery. People experience similar frustrations on their end. Rather than repeating the same information (such as a change of address or marital status, the birth of a child or the death of a spouse) several times to multiple government departments, they prefer to be asked only once and expect their updated information to be coordinated across different services.

However, information silos, as frustrating as they are, have traditionally served as a form of protection by creating technical or procedural barriers against the use and sharing of personal information for different and unauthorized purposes. As governments modernize their services and adopt digital identity methods to enable necessary information-sharing across silos, the protections once provided by keeping information separate must be replaced by alternative forms of checks and balances. These include access controls, limits on unrelated uses and disclosures, transparency requirements, and security protections, all within an overarching governance framework.

WHAT WORK HAS THE IPC DONE IN THIS AREA?

The IPC has been actively engaged in discussions about **Ontario's Digital Strategy** and issues such as digital identity within the public sector. Some of our early research on the subject of identity management will serve as a good foundation for resolving the digital identity questions and challenges faced by all public sector organizations in the next five years. We have also provided advice to municipalities that are looking for innovative and efficient ways to provide their services to Ontarians.

The IPC supported the Ontario government's development of the data integration framework set out in Part III.1 of *FIPPA* that will enable privacy-protective sharing and linking of data within and between data integration units for planning and analysis purposes. We are currently in the process of consulting with the Ontario Ministry of Government and Consumer Services (MGCS) on the development of data standards that will establish the rules for data integration, including: how to link and de-identify personal information, publicly report on the use of personal information, and securely retain and dispose of personal information.

HOW COULD THE IPC BUILD ON THIS WORK?

Working with MGCS, and in particular with the Information, Privacy and Archives Division, the IPC can support government's shift towards a digital service delivery model by creating practical guidance and model data governance frameworks for other providers to follow. The IPC can also play a key role in establishing security and data sharing standards for government digital platforms and digital identity systems.

With respect to our prior work on data integration, many of the measures that have been developed to ensure confidentiality, accountability, transparency, and security among data integration units could be adapted to support integrated digital service delivery across government.

The IPC could further support institutions in the shift toward online service delivery by providing guidance on privacy and security considerations when using digital platforms offered by third party providers. For example, the IPC could provide guidance on the contractual and other protections necessary to ensure seamless accountability for Ontarians' personal information processed by private sector organizations on behalf of government institutions.

The IPC could also play a key role in providing Ontarians with education and guidance to enhance digital literacy and encourage uptake of government digital services. In part, this could be done by providing them with a better understanding of the privacy risks involved, the ways they can avoid or reduce them, what information they are entitled to ask for, and how they can hold their government to account for the actions and decisions that affect them.

RESOURCES

KEY IPC RESOURCES:

- **Open Letter: IPC Comments on the Ontario Government's Better, Smarter Government Discussion Paper (2019)**

Other Key Documents:

- Government of Ontario – **Ontario Onwards: Digital Identity Project** (October 2020)
- Resolution of the Federal, Provincial, and Territorial Information and Privacy Commissioners – **Protecting and Promoting Canadians' Privacy and Access Rights in Information Sharing Initiatives** (January 2016)
- Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners – **Protect and Promote Canadians' Access and Privacy Rights in the Era of Digital Government** (October 2014)

GUIDING QUESTIONS
Would *government digital service delivery* be a priority for you? Why or why not?
If the IPC were to make *government digital service delivery* a priority, do you agree with our proposed goal statement? If not, how would you suggest changing it?
If *government digital service delivery* is selected as one of IPC's strategic priorities, what else could the IPC do to advance this priority area over the next ftive years?

POTENTIAL STRATEGIC PRIORITY: TRANSPARENCY AND OPEN GOVERNMENT

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.

WHY MIGHT THIS BE A STRATEGIC PRIORITY?

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 for Ontarians, including:

- strengthening democracy and promoting integrity by making government more transparent and accountable for its decisions and actions, including spending
- giving the public a greater voice in what government does, and fostering government decisions and action that further the interests of all, not just a few

- empowering people and enabling them to make more informed choices and decisions
- advancing a more efficient and effective government
- improving services and finding novel ways to offer them based on past utilization data
- enhancing Ontarians' trust in their government

A culture of proactive transparency has significant benefits for government, such as reducing the person-hours and other resource expenditures involved in processing freedom of information requests.

The need for, and benefits of, transparency and open government will be more apparent as government modernizes its information systems and adopts digital service delivery models. Greater complexity in government must be met with a corresponding increase in transparency and accountability.

Many Ontario institutions have made great strides in advancing open government by proactively releasing useful datasets, making available the results of freedom of information requests (reducing the need for duplicate requests), and simplifying the process for requesting information. These strategies are an essential step towards open and transparent government. Prioritizing this issue can help accelerate these efforts and promote the increased adoption of proactive disclosure measures.

An overall culture of transparency and openness allows us to hold governments 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.

WHAT WORK HAS THE IPC DONE IN THIS AREA?

The IPC has a long history of advocating for open and transparent government. It has allocated significant resources to its internal intake and mediation functions to resolve as many access appeals as possible, as early as possible. These up-front efforts help parties to negotiate a resolution of disputes about the release of records to the satisfaction of all parties, and avoid expensive and lengthy adjudication and litigation processes. These investments in early resolution have yielded significant returns. In the IPC's 2019 annual report, we reported that 70% of all access appeals were resolved at the intake or mediation phases.

In previous years, the IPC has released several guidance documents aimed at government institutions on various matters related to putting open government practices in place. Recently, we called on the Ontario government to create a publication scheme, which requires proactive disclosure, on a routine basis, of certain broad classes of information. Such schemes can help ensure that critical information related to the government's mandate and functions is released publicly, even without an access request. In many international and Canadian jurisdictions, publication schemes are defined in freedom of information laws and help alleviate the practical and regulatory burdens of an already-overloaded access to information system.

The IPC has also recommended that Ontario institutions examine the merits of proactively disclosing information that has already been released in response to a previous access to information request. Once in the public domain, releasing these records in a privacy protective manner helps avoid repetitive access requests. Many other jurisdictions have already adopted this process, including the federal government.

The IPC's **De-Identification Guidelines for Structured Data** were developed and published specifically with a view to encouraging the responsible public release of data, while protecting personal information.

HOW COULD THE IPC BUILD ON THIS WORK?

As part of our continuing efforts to promote the proactive disclosure of information, the IPC could collaborate with relevant stakeholders in developing guidance on how to make proactive disclosure a more routine practice, and ensure that government institutions who wish to increase their disclosures have the right tools to do so. For example, the IPC can update and further build on its **De-Identification Guidelines for Structured Data** to help ensure that the data which is proactively released retains its utility for third-party users, while still protecting personal information.

Another way to ensure more transparency within government organizations is to require more open procurement processes and proactive disclosure of government contracting records. Access to information about government procurement processes represents a significant proportion of access appeals received by our office. These tend to be made more complex by the objections of commercial third parties whose expectations of confidentiality are often misaligned with expectations of taxpayers who demand an appropriate level of accountability for public spending. Our office has long called for more transparency around government spending, but there is still more work to be done in this area.

The IPC can also conduct a more detailed review of the access request process and appeal mechanisms to look for opportunities to improve their effectiveness, accessibility, timeliness, and equity — including our own internal processes at the IPC. In some cases, we can achieve these reforms through guidance that promotes process changes and ensures all the Ontario institutions we oversee are aware of, and able to meet, their obligations without requesters needing to submit an appeal to our office.

Where necessary, we will continue to advocate for legislative reform to effect positive change. For example, we have called for the modernization of our public sector access and privacy laws. Our recommendations include reducing or eliminating fees, putting in place more effective and efficient appeal processes responding to the public demand for digitization of these processes, and enhancing the role of the public interest in access to information. The IPC will continue to promote these and other improvements as part of its ongoing efforts to increase openness and transparency.

To benefit from more open and transparent government, individuals must be able to make effective use of that data. Further education efforts can be targeted to the public to enhance their understanding of the access request process and how to make use of it in an informed and practical way. The IPC could collaborate with government and community organizations to promote awareness about access to information rights and encourage initiatives that help develop the digital skills and tools needed to make use of the data that is made available.

RESOURCES

KEY IPC RESOURCES:

- **IPC Submission on Consultation Paper: Strengthening Corporate Beneficial Ownership Transparency in Canada** (March 2020)
- **IPC Comments on the Ontario Government’s Creating Economic Benefits Discussion Paper** (October 2019)
- **Open Government and Protecting Privacy** (March 2017)

- **Open Government: Key Implementation Considerations** (August 2016)
- **Open Government: Key Concepts and Benefits** (September 2016)
- **Open Contracting: Proactive Disclosure of Procurement Records** (September 2015)

OTHER KEY DOCUMENTS:

- Resolution of the Federal, Provincial, and Territorial Privacy Commissioners – **Effective privacy and access to information legislation in a data driven society** (October 2019)
- Resolution of the Federal, Provincial, and Territorial Privacy Commissioners – **Open Government** (September 2010)

GUIDING QUESTIONS
Would *transparency and open government* be a priority for you? Why or why not?
If the IPC were to make *transparency and open government* a priority, do you agree with our proposed goal statement? If not, how would you suggest changing it?
If *transparency and open government* is selected as one of IPC's strategic priorities, what else could the IPC do to advance this priority area over the next five years?

POTENTIAL STRATEGIC PRIORITY: RESPONSIBLE USE OF DATA FOR GOOD

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.

WHY MIGHT THIS BE A STRATEGIC PRIORITY?

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.

The emerging "data for good" movement among many public institutions, not-for-profit organizations, and large multi-nationals encourages the application of artificial intelligence and machine learning systems to analyze massive data holdings in ways that are not humanly possible. Fostering innovative and entrepreneurial approaches and solutions often requires cross-sectoral sharing of information in collaborative efforts to help address the most complex humanitarian challenges in areas such as health, equity, poverty, education, and the environment.

Of course, where there is data for good, there is also "data for bad." Important conversations are needed around questions such as, What is good? Data for *whose* good? Who gets to determine (and ultimately decide) any trade-offs being made? Who is ultimately accountable for the outcomes resulting from the use of data for good? And what are the boundaries that cannot be crossed, regardless of the good that might be achieved?

Data governance frameworks have begun to emerge to support the responsible treatment of data based on concepts of fairness, accountability, transparency, and respect for privacy. These frameworks rely, in part, on methods of de-identifying data, the development of model data-sharing agreements and appropriate review and approval processes. The Ontario government's recent **discussion paper** on private sector privacy reform also put forward data trusts as a potential sharing model.

These new data governance models are emerging around the world and have been the subject of much debate in recent years. However, there is still much work to be done to identify the appropriate models for supporting data for good initiatives in Ontario. Further analyses are required to fit these new data initiatives within Ontario's existing access and privacy laws or to consider what legislative amendments might be necessary to enable them in the future. There are still many uncertainties around the public's rights and organizations' obligations regarding these data holdings, how to define the public good, how to weigh and align the risks and benefits, who gets to decide, and how to ensure efficient and effective oversight, particularly across different sectors. Removing such uncertainties would be a significant step toward ensuring responsible data innovation in Ontario.

WHAT WORK HAS THE IPC DONE IN THIS AREA?

The IPC has examined the kinds of technical and policy-based frameworks needed for privacy-respectful sharing and use of personal information for social good, through work such as our **Big Data Guidelines** and our **De-Identification Guidelines for Structured Data**. We have also set out **our vision** for what is needed to promote trust and confidence in the data economy.

The IPC has built up significant expertise in the health sector, by overseeing Ontario's health privacy law, which incorporates novel ways of entrusting data to prescribed entities for health research and planning purposes. These entities are entrusted to use data for social good, subject to appropriate regulatory oversight and review of their personal information practices and procedures by the IPC every three years. *PHIPA* also sets out the requisite privacy protections that form an integral part of the broader ethical review frameworks that must weigh and consider the attendant risks and benefits, both at the individual and societal level, when assessing researchers' requests for access to health data necessary to carry out their research projects.

The IPC played a significant role in the development of the governance regime introduced as part of the legislative changes relating to data integration units (DIUs). These DIUs are a novel way of encouraging responsible data sharing within ministries, across ministries and outside ministries, for the purpose of planning and evaluation of important government programs and services. These DIUs are subject to compliance with designated standards and oversight by the IPC.

The IPC was also involved in extensive policy debates about what might constitute an appropriate governance framework, including examination of a possible data trust model, in the context of the Sidewalk Labs smart city initiative in Toronto.

HOW COULD THE IPC BUILD ON THIS WORK?

Public institutions in Ontario are actively seeking or being presented with opportunities to share personal information and apply it in support of the public good. However, many may be hesitant to do so without clear guidance on the rules — an issue referred to as "**reticence risk**." As public institutions wait for clear guidance on the restrictions and considerations around sharing information, many data for good initiatives wait in limbo or are abandoned altogether.

The release of valuable data can be used by others to find ingenious and innovative ways of solving societal problems that governments, acting alone, cannot do. For this to work for the benefit of all, however, appropriate governance frameworks must be in place and released datasets must undergo sufficiently robust de-identification processes to protect personal information, while maintaining their utility.

As the de-identification of personal information is often a key first step toward the use of data for beneficial purposes, the IPC will continue to build on our expertise in this area, working with industry experts to identify technical measures which can facilitate or enable open data.

If responsible data innovation is adopted as a strategic priority, the IPC could focus its efforts on catalyzing the development of one or more trusted, practical, and privacy-protective data sharing mechanisms. The IPC could bring together interdisciplinary, multi-sectoral groups of stakeholders and other regulators, such as the Ontario Human Rights Commission, 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.

Similarly, the IPC could support Ontario institutions by developing model frameworks for the use of innovative, data-centric technologies such as artificial intelligence (AI) by bringing together the growing AI research community and working with research funders within Ontario. The IPC has an opportunity to advance the protection of privacy and access rights in this area, helping ensure that the use of AI-based systems in Ontario complies with current and emerging ethical best practices and standards. This would support the IPC's commitment as co-sponsor of an international **resolution** on accountability in the development and use of artificial intelligence. The resolution calls on all members of the Global Privacy Assembly to urge organizations that develop and use AI systems to adopt broader ethical principles into their accountability measures.

RESOURCES

KEY IPC RESOURCES:

- **IPC Comments on the Ontario Government's Promoting Trust and Confidence in Ontario's Data Economy Discussion Paper** (September 2019)
- **Big Data Guidelines** (May 2017)
- **De-Identification Guidelines for Structured Data** (August 2016)

OTHER KEY DOCUMENTS:

- Resolution of the Federal, Provincial, and Territorial Privacy Commissioners – **Effective privacy and access to information legislation in a data driven society** (October 2019)
- Resolution of the Federal, Provincial, and Territorial Information and Privacy Commissioners – **Protecting and Promoting Canadians' Privacy and Access Rights in Information Sharing Initiatives** (January 2016)
- Global Privacy Assembly – **Accountability in the Development and Use of Artificial Intelligence** (October 2020)
- Global Privacy Assembly – **Ethics and Data Protection in AI** (October 2018)

GUIDING QUESTIONS
Would the *responsible use of data for good* be a priority for you? Why or why not?
If the IPC were to make the *responsible use of data for good* a priority, do you agree with our proposed goal statement? If not, how would you suggest changing it?
If the *responsible use of data for good* is selected as one of IPC's strategic priorities, what else could the IPC do to advance this priority area over the next five years?

POTENTIAL STRATEGIC PRIORITY: ACCESS, PRIVACY, AND YOUTH

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.

WHY MIGHT THIS BE A STRATEGIC PRIORITY?

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 vulnerable populations whose information privacy and access rights merit special consideration and support. Children are particularly vulnerable because they are less equipped for complex decision-making, and often cannot give informed consent or exercise the full legal privacy and access rights afforded to adults.

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. Some jurisdictions recognize the need to protect youthful experimentation and self-discovery by vesting youth with explicit powers to assert greater control over their digital personal history, including the right to request its deletion from social media platforms, such as exists in **California**.

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.

WHAT WORK HAS THE IPC DONE IN THIS AREA?

Our office has a long history of promoting youth privacy issues. In 2011, we developed resource guides for Ontario's Grade 11 and 12 teachers and in the years prior to that, we released similar resource guides for teachers of Grades 5 and 10. We collaborated with partners like MediaSmarts and other privacy regulators, in developing lesson plans for schools, along with other digital literacy resources. In 2016, the IPC was a co-sponsor of an international resolution to promote the adoption of a **Competency Framework on Privacy Education** in primary and secondary school curricula (including training opportunities for educators). In 2017, the IPC participated in an internationally led review of online educational platforms. Following the review, the IPC co-authored a 2018 international data protection commissioners' **resolution** on e-learning platforms. It included 24 recommendations and extensive guidance for educational authorities on how to put them into practice. The resolution called on privacy authorities worldwide to raise awareness of the privacy risks of e-learning platforms and to develop additional guidelines to support educational leaders and e-learning platform developers.

The IPC has also undertaken outreach efforts with ministry officials, teachers' unions, educational associations, academics, and others to engage them in an ongoing dialogue about current privacy and access issues affecting youth, and to help establish privacy best practices. These efforts include offering panels and workshops at education technology events, carrying out primary research on online educational services, and developing tools and publications for teachers, parents and students tso use. We are also well-engaged with access to information issues concerning youth, having developed wide-ranging guidance on **access to personal information and privacy in schools**.

Beginning in 2018, the IPC worked extensively to prepare for the implementation of Part X of Ontario's *Child, Youth and Family Services Act* (*CYFSA*) that sets out new privacy protection and access to information rules for children and youth in the context of child and family services. This involved outreach with multiple service providers, participation in implementation working groups, delivery of training programs to professionals in the sector, and the development of written **guidance**.

HOW COULD THE IPC BUILD ON THIS WORK?

The IPC has positioned itself as a leader in youth privacy 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.

As a first step, the IPC could work with the Ministry of Education and provincial school boards to gain a better understanding of the digital platforms and tools being used in Ontario schools, and identify where our efforts might best be targeted. Frameworks to support the review and evaluation of these tools would help the Ministry of Education and school boards adapt to the challenges associated with the exponential growth in remote learning.

The IPC could also seize the opportunity to continue to collaborate with relevant partners in strengthening the foundation of tools to promote digital literacy. We could expand our efforts to develop awareness-raising tools about the risks and impacts of using social media and other online platforms as part of the learning experience. Given the new teaching methods and learning modules, including self-learning and home-schooling, that will likely exist beyond the pandemic, these privacy and access tools could form a vital part of the province's permanent digital education curriculum and school board policy.

With new responsibilities administering Part X of the *CYFSA*, the IPC will gain additional experience handling complaints and appeals in this sector. We will continue to guide, and work with, service providers to make sure that they protect the privacy of young people entrusted in their care through their daily practices and enable the youth they serve to exercise access and correction rights, in a timely way. We will be able to gain further insights from the annual statistics that child and family service providers must report to our office. This will allow us to issue additional guidance and positively influence the information management practices and culture of this sector, with particular focus on the most marginalized communities.

We might also consider bringing together a broad range of partners to work towards the creation of a children's access and privacy code for Ontario. The first of its kind in Canada, this comprehensive privacy code could set out a framework for guiding all initiatives that impact the access and privacy rights of children and youth in the province, building on the research we have done to date.

RESOURCES

KEY IPC RESOURCES:

- **Providing access under the *CYFSA*** (November 2019)
- **A Guide to Privacy and Access in Ontario Schools** (January 2019)
- **New Lesson Plans for Educators: Privacy Rights, Digital Literacy and Online Safety** (June 2018)
- **Joint Letter to the Council of Ministers of Education on the Importance of Privacy Education** (November 2017)
- **Report on Online Educational Services** (as part of the Global Privacy Enforcement Network Sweep) (October 2017)

OTHER KEY DOCUMENTS:

- ICDPPC – **Resolution on the Privacy and Data Protection Challenges Arising in the Context of the COVID-19 Pandemic** (October 2020)
- International Conference of Data Protection and Privacy Commissioners (ICDPPC) – **Resolution on E-Learning Platforms** (co-authored by IPC Ontario) (October 2018)
- ICDPPC – **Resolution for the Adoption of an International Competency Framework on Privacy Education for School Students on Data Protection and Privacy** (Framework linked **here**) (October 2016)

GUIDING QUESTIONS
Would *access, privacy, and youth* be a priority for you? Why or why not?
If the IPC were to make *access, privacy, and youth* a priority, do you agree with our proposed goal statement? If not, how would you suggest changing it?
If *access, privacy, and youth* is selected as one of IPC's strategic priorities, what else could the IPC do to advance this priority area over the next five years?

POTENTIAL STRATEGIC PRIORITY: NEXT–GENERATION LAW ENFORCEMENT

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.

WHY MIGHT THIS BE A STRATEGIC PRIORITY?

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.

Law enforcement agencies collect and hold large volumes of personal information about Ontarians. Some of this collection occurs through hidden means with, and in some cases without, specific judicial authority. The practices of these agencies can have a significant impact on the private lives of all Ontarians.

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 as law enforcement agencies increasingly turn to surveillance technologies as a tool for enhancing public safety and improving operational efficiencies. **Ontario's $6M grant program for CCTV installation** announced in August 2020, the use of **backdoor keys** to unlock iPhones, **the use of facial recognition technologies** and the planned use of **body-worn cameras** by several police services across Ontario are but a few examples.

The use of artificial intelligence by law enforcement agencies is raising important new questions. In its **September 2020 report,** the Citizen Lab analyzes the human rights implications of algorithmic policing practices in Canada, including technologies that seek to predict crime before it occurs.

The overall increase in the amount of data collected about individuals by internet service providers, makers of household devices and body sensors connected to the internet, retail surveillance cameras and other forms of third party collection, are also worthy of consideration. While they might be installed outside the law enforcement context, they *may become available to law enforcement*.

Recently, and for the first time in Ontario, police used DNA samples shared by individuals interested in learning about their ancestry through a U.S. recreational genealogy website to solve a **cold case murder**. Through partial matching and the use of genetic linkages, forensic DNA experts were able to reconstruct a family tree and narrow down potential suspects which eventually led to identification of the actual murderer. Although individual genealogy enthusiasts may have consented to share their DNA sample with law enforcement, their distant relatives who were caught up in the investigation did not.

While technological advances in information collection and processing can lead to faster, better, and more efficient policing outcomes, they can also have significant negative effect on privacy and access rights if not used in an appropriate and privacy protective manner. There is a need to examine issues such as necessity, proportionality, transparency, and accountability when engaging in technology-assisted policing, and to establish effective oversight and control mechanisms tailored to the unique features of each technology, its proposed use, and context.

A consistent and principles-based approach to the use of surveillance technologies by law enforcement — developed in consultation with privacy and access, human rights, civil liberties, and criminal law experts — will help ensure that privacy, access, and other fundamental rights will be given their fullest consideration in communities across Ontario, including marginalized communities. Greater transparency in the use of such technologies, including data about their differing impacts, can help advance discussions about the appropriate protection of rights and how policing services are delivered.

WHAT WORK HAS THE IPC DONE IN THIS AREA?

The IPC has long been engaged in examining the use of new technologies by law enforcement. This includes providing advice to law enforcement agencies on the use of algorithmic surveillance technologies, such as **automated licence plate recognition** and facial recognition, cautioning against the risks of false positives and inherent biases that may have negative impacts on marginalized populations.

We made recommendations to better define the types of information and the situations in which personal information could or should be uploaded to the Canadian Police Information Centre (CPIC) database. We have also provided advice to Ontario police services on the necessary privacy protections to support their collection, use, and retention of race-based data.

In the recent past, we have been heavily engaged in the development of frameworks to support the privacy protective and transparent use of body worn cameras, including by the **Toronto Police Service**. And, we are currently working actively with our federal, provincial and territorial counterparts to develop guidance on the use of facial recognition technologies in the context of law enforcement.

HOW COULD THE IPC BUILD ON THIS WORK?

As the Citizen Lab states in its **September 2020 report**, "it is not too late for Canada to get it right and implement the necessary legal and policy frameworks, oversight mechanisms, and best practices" to ensure that technology-assisted policing is used in a way that is less likely to threaten human rights, including privacy.

The IPC has built strong capacity in overseeing the data management practices of police services and already has well-established working relationships in the law enforcement sector. Building on this foundation, the IPC can prioritize its role in this area, working 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. The IPC can encourage police services to integrate privacy and security protections up front, guide them in designing effective governance frameworks that will support their public safety objectives, while holding them to account for respecting the access rights, privacy rights and dignity of the communities they serve.

Lastly, the IPC can participate in constructive dialogue with other relevant stakeholders to help bridge the gap between legal access and privacy compliance, and broader rights protected by the *Canadian Charter of Rights and Freedoms*. While the IPC can raise issues and provide thought leadership with respect to the collection and use of data for law enforcement under *FIPPA* and *MFIPPA*, the ultimate judge of what is compliant with charter rights will be the courts. In that regard, and where appropriate, the IPC can participate in proceedings as a friend of the court, bringing forward its privacy expertise in the context of Section 8 challenges against the activities of law enforcement for unreasonable search and seizure.

RESOURCES

KEY IPC RESOURCES:

- **Letter from Commissioner Kosseim to Toronto Police Service Board Regarding Approval of Body-Worn Camera Contract Award and Project Implementation** (August 2020)
- Blog Post: **Good Governance will be the Key to Delivering on the Promise of Body-Worn Cameras** (August 2020)
- **Release of Personal Information to the Police: Your Privacy Rights** (August 2019)
- **Best Practices for Automated Licence Plate Recognition (ALPR) Technologies** (September 2016)

- **IPC Submission to the Ministry of Community Safety and Correctional Services on its Strategy for a Safer Ontario** (April 2016)
- **Crossing the Line: The Indiscriminate Disclosure of Attempted Suicide Information to U.S. Border Officials via CPIC — Special Investigation Report** (April 2014)

OTHER KEY DOCUMENTS:

- International Conference of Data Protection and Privacy Commissioners – **Resolution on Facial Recognition Technology** (October 2020)
- **Guidance on the use of body-worn cameras by law enforcement authorities** (February 2015) (Privacy Commissioner of Canada; jointly with provincial and territorial offices)

GUIDING QUESTIONS
Would *next-generation law enforcement* be a priority for you? Why or why not?
If the IPC were to make *next-generation law enforcement* a priority, do you agree with our proposed goal statement? If not, how would you suggest changing it?
If *next-generation law enforcement* is selected as one of IPC's strategic priorities, what else could the IPC do to advance this priority area over the next five years?

POTENTIAL STRATEGIC PRIORITY: TRUST IN VIRTUAL HEALTH

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.

WHY MIGHT THIS BE A STRATEGIC PRIORITY?

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 among different custodians have expanded the volume and breadth of organizations involved in delivering health services to Ontarians.

For instance, private sector companies now increasingly collect data from **wearable health devices and body sensors** (such as heart rate, temperature or blood pressure monitors, pedometers, body positioning or balance sensors, etc.). Private sector actors also process health data through virtual care platforms and provide individuals with patient portals and digital health apps for accessing their health information. Given the number of potential service providers handling health information and the many methods of sharing it, there is a need for clear and seamless accountability throughout these increasingly complex data flows, both within and beyond the bounds of the *PHIPA*, Ontario's health privacy law.

The COVID-19 pandemic has increased the role of health information in helping navigate everyday life, expanding the range of parties who may be able to access that information. Some employees are required to submit daily wellness checks to their employers, many of whom are not subject to any privacy rules in Ontario. An **emergency order** granted first responders access to COVID-19 status. We have also seen COVID-related trends and statistics reveal pre-existing health inequities among populations more vulnerable to the virus due to socioeconomic factors. The emergence of these stark inequalities during the pandemic has reignited the interest in collecting aggregate statistics and combining health information with other information potential determinants of health to paint a more complete picture of overall health and wellness.

The digitization of health information allows for greater data sharing and supports important health research. For example, a recent temporary **change** to Ontario's health privacy law allows ICES (formerly known as the Institute for Clinical Evaluative Sciences) and Ontario Health to provide health information to the Ministry of Health's **Ontario Health Data Platform**, which is used for researching and responding to COVID-19 and its effects. Otherwise, however, researchers may find that navigating diverse and rigid rules that may no longer fit the reality of what they are trying to do and limit the sharing of health information, posing challenges to their work.

The **expanded application of machine learning** and other artificial intelligence techniques can potentially improve both individual health outcomes and the overall efficiency of the health care system, but also raise other concerns, such as the risks of false positives and potential discrimination.

WHAT WORK HAS THE IPC DONE IN THIS AREA?

The regulation of health information has been an area of particular strength and focus for the IPC. We have long been champions of finding the appropriate balance between enabling better health outcomes through data availability and the protection of individuals' health information. For example, working with its federal counterpart, the IPC quickly turned its focus to enabling the privacy-protective deployment of the COVID-19 exposure notification app in Ontario.

The IPC has written extensive guidance aimed at providers (e.g., about how to safeguard personal health information, including when it is in digital form) and the public (e.g., about individuals' rights of access to, and correction of, their personal health information).

The mandatory breach reporting requirement under *PHIPA* has given the IPC significant insights into the extent and causes of data breaches in the health sector, and has helped us gain understanding into some of the greatest vulnerabilities of custodians' privacy and security measures and how to help reduce them.

PHIPA allows prescribed entities and persons to collect personal health information from custodians for purposes specified in the legislation, subject to IPC oversight and approval. Every three years, the IPC reviews their detailed information practices and procedures and issues recommendations as needed.

Part V.1 of *PHIPA*, which came into force in 2020, sets out Ontario Health's responsibility for maintaining and administering the "electronic health record," which is a single core health record for each Ontarian. As the prescribed organization under Part V.1, Ontario Health's information practices and procedures will also be subject to expert review and oversight by the IPC every three years.

Recent changes to *PHIPA* will further expand the IPC's mandate with respect to consumer electronic service providers (e.g., health apps), individuals' access to records in electronic format, and the requirement for custodians to maintain an electronic audit log. *PHIPA* sets out a new framework for Ontario Health to develop interoperability requirements for digital health assets, subject to consultation with the IPC, to the extent these requirements relate to privacy or to individuals' rights of access and correction. Another significant amendment has introduced an administrative penalty scheme — a first of its kind in Canada — empowering the IPC to enforce compliance with *PHIPA* and issue fines against offending organizations.

HOW COULD THE IPC BUILD ON THIS WORK?

Building on our past experience and expertise, and Ontario's strong health privacy law, there is a significant opportunity for the IPC to be a leader in developing 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 the use of health data for research and population-wide interventions, and setting appropriate guidelines for the use of health information in training artificial intelligence systems.

The IPC may also be able to collaborate with cybersecurity experts to provide guidance to hospitals and other health service providers with respect to the growing issue of data breaches and, in particular, ransomware attacks.

Ontarians are increasingly gaining access to their own health information through personal health portals and digital health apps and body sensors. The IPC could play a leadership role in this area, ensuring that people know how to manage and store this information while minimizing unnecessary risks.

The IPC can also work with relevant stakeholders in the evaluation of impacts and effectiveness of the data collection and policy changes that have occurred because of the pandemic, with an eye to creating a framework to address future similar emergency situations.

Health information is generally considered to be among the most sensitive categories of information about an individual. However, as a responsible data regulator, the IPC would also need to ensure that any governance mechanisms designed to protect privacy are well-measured and do not unduly impact the value and utility of the data for public good — a challenging task, but one of great importance for the people of Ontario.

RESOURCES

KEY IPC RESOURCES:

- **Comments of the IPC on Proposed Interoperability Regulations under *PHIPA*** (July 2020)
- **Comments of the IPC on Proposed Regulation under *PHIPA* with Respect to the Health Data Platform** (July 2020)
- **IPC Recommendations on COVID Alert** (July 2020)
- **Comments of the IPC on Proposed Regulations Under Part V.1 of *PHIPA*** (June 2020)
- **Comments of the IPC on Bill 138** (December 2019)

Other Key Documents:

- **Joint Statement by Federal, Provincial and Territorial Privacy Commissioners on Privacy Principles for Contact Tracing and Similar Apps** (May 2020)

GUIDING QUESTIONS
Would *trust in virtual health* be a priority for you? Why or why not?
If the IPC were to make *trust in virtual health* a priority, do you agree with our proposed goal statement? If not, how would you suggest changing it?
If *trust in virtual health* is selected as one of IPC's strategic priorities, what else could the IPC do to advance this priority area over the next five years?

CROSS–CUTTING APPROACHES

In addition to identifying potential strategic priorities and steps the IPC might take to advance them, the IPC has also reflected on how it might do so. The IPC has identified four cross-cutting approaches that could be applied across *all* strategic priorities to further enhance the impact of our work.

ACCESSIBILITY AND EQUITY

Vulnerable and marginalized people will often experience the greatest impacts — both positive and negative — from information-driven government processes and procedures. At the same time, these individuals may not be equally served by government access to information services, digital programs, or digital service delivery models — or even the IPC's own services and processes.

To address this, the IPC will:

- apply the dual lens of accessibility and equity to its evaluation of programs and technologies related to its priorities, as well to its own services and processes

CAPACITY BUILDING (INTERNAL AND EXTERNAL)

Capacity is an on-going challenge in an area as broad and ever-changing as privacy and access to information. Therefore, in support of its strategic priorities, the IPC will:

- continue to develop its **internal** capacity by enhancing staff training and gathering knowledge through engagement with diverse stakeholders
- continue to educate organizations on how they can practically comply with their privacy and access obligations
- support research into privacy-enhancing technologies and other advances in access and privacy, including by creating pathways for researchers to show the practical impacts of their work
- continue to empower individuals to exercise control over their own information and demand greater transparency with respect to information held and used by governments

VISIONARY BUT PRAGMATIC

The IPC recognizes that a strategic priority must have an eye to the future, while not losing sight of today's challenges.

In support of its strategic priorities, the IPC will:

- ensure that its work on strategic priorities is visionary, considering the full range of potential future paths
- draw from the experiences of other jurisdictions and evolving international data privacy norms for new technologies
- identify intermediate steps along those paths at which practical advice and guidance can be created

COLLABORATION AND CONSULTATION

The IPC cannot, and should not, seek to advance significant access and privacy priorities in a vacuum. We must continue to develop strong, trusted relationships with stakeholders, including organizations we regulate, academics specializing in the areas of access, privacy and technology, journalists, and civil society groups who represent the interests of individuals, communities and groups. These relationships support the mutual sharing of knowledge and perspectives, and the leveraging of resources and strategies. We are also aware that in many instances, our strategic priorities will be affected by multinational organizations or international data flows and require cross-border cooperation and coordination.

In support of its strategic priorities, the IPC will:

- commit to seek out collaborations with relevant stakeholders across sectors when advancing our strategic priorities
- coordinate our efforts with other regulatory bodies, including data commissioners and human rights regulators
- consult with a range of stakeholders to ensure a holistic approach that reflects multiple perspectives and advances the IPC's work, in the interest of all Ontarians

GUIDING QUESTION

What other cross-cutting approaches should the IPC consider taking in respect to its strategic priorities?

CONCLUSION

A primary goal of the IPC's strategic priority-setting exercise is to ensure that we are able to channel our discretionary efforts and allocate our limited resources towards issues of greatest relevance and value to Ontarians. To do that, we need to hear from you.

You are invited to provide your feedback by **January 15, 2021,** online at **https://www.ipc.on.ca/guidance-documents/forms/strategic-priority-consultation-form/**, by email to **consultation@ipc.on.ca**, or by mail to IPC Strategic Priorities, 2 Bloor Street East, Suite 1400 Toronto, ON, M4W 1A8.

We leave you with the following concluding questions, and look forward to hearing from you.

CONCLUDING QUESTIONS

If you could only select three strategic priorities for the IPC to focus on over the next five years, which would they be?

Are there any other potential strategic priorities you think we should consider? If so, please describe them and tell us what you think the IPC's role should be in addressing them.

How would you describe yourself?

- a member of the general public
- a public-sector organization
- a member of the health care sector
- law enforcement
- private sector organization
- child and family services sector
- academic
- other

Any other closing comments?

IPC Strategic
Priority
Setting
Consultation

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

December 2020