IPC Strategic Priority Consultation Submission

Contents

Introduction

1. The Public Interest Advocacy Centre ("PIAC") is pleased to provide comments to the Information and Privacy Commissioner of Ontario's ("IPC") Strategic Priority Setting Consultation ("Consultation"). The Consultation focuses on six strategic priorities that reflect the key access and privacy issues that Ontarians care most about and have the greatest positive impact. PIAC has long advocated for stronger privacy protections in the public and private sector. Privacy reform is more relevant than ever, as the accelerated digitization of services during the COVID-19 pandemic has intensified ongoing privacy challenges.

2. The preliminary remarks of the Consultation recognizes that if Bill C-11, the *Digital Charter Implementation Act, 2020*, is passed, it will apply to Ontario businesses unless Ontario adopts its own substantially similar law. PIAC advises restraint in looking to this new Bill, which PIAC believes significantly erodes privacy protections. Caution is also merited because of the upcoming adequacy review under the GDPR. PIAC is of the view that Canada's adequacy status, especially under Bill C-11, is uncertain, therefore it is risky to adapt principles from the Bill to the IPC's privacy strategy.

Government Digital Service Delivery

3. PIAC believes that transparency is key for government digital service delivery, both at the point of delivery and in the information made available about how digital services are developed. The

Consultation Paper provides the example of wireless access on the GO Transit system, which offers access to free books, music, and podcasts. Before accessing any digital service, whether public or private, individuals must be informed about their privacy rights and be given an opportunity to provide explicit consent if any personal information is collected. As a trusted source of independent advice, the IPC should ensure government institutions and public service providers provide such information, thus following a privacy-first approach to digital service delivery.

4. The IPC should also ensure that individuals understand how their personal information is digitized. Personal information that previously existed outside of centralized digital databases is now increasingly converted to more vulnerable storage formats. Cybercriminals are becoming more sophisticated and capable only in proportion to the combined volume and commercial value of personal information. Such value increases with each new data point, whether it be place of residence, employment status, age of majority, or immigration status. These new volumes of data are also attractive to the third parties who have commercial interests, and also design, build, and operate platforms on behalf of the government. Even de-identified data can still potentially affect individuals through the predictive data analytics used to influence targeted commercial decisions. The IPC must provide robust guidance on the contractual protections that need to be in place to ensure that industry partnerships themselves do not pose a risk to individual rights, and do not become personal information conduits to feed commercial interests.

5. Additionally, as personal information is shared between government institutions, one vulnerability potentially compromises the entire shared network of personal information. Therefore, the IPC should conduct ongoing research on the evolution of cyberattacks, and provide practical guidance to the government about how to effectively protect personal information against such threats by applying privacy principles like data minimization.

Transparency and Open Government

6. PIAC supports the IPC's goal of reducing barriers to access by promoting efficient access-to-information processes, proactive disclosures, and an overall culture of open government. However, access is meaningless without effective recourse. Even if individuals, through improved access rights, find concerns upon which to file complaints, the IPC cannot issue binding orders. The IPC has already expressed their intention to advocate for positive legislative reform, specifically to put in place more effective appeal processes, and to enhance the role of the public interest, among other recommendations. PIAC encourages these reforms at both the provincial and federal level, and would point out that Bill C-11 includes order-making powers for the federal Commissioner.

7. The IPC suggests that transparency can be enhanced by requiring more open procurement processes and proactive disclosure of government contracts. However, the IPC states that access-to-information requests about procurement processes are "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."[1] The IPC must clearly indicate to government institutions that such complexity must not be resolved in favour of the commercial goals of third parties. In fact, if contractual terms place such goals above accountability and transparency, institutions should err on the side of not contracting with the third parties at all.

8. PIAC advises the IPC to conduct a review of existing government contracting records, then formulate guidance for institutions on provisions that ensure individual privacy rights are not sacrificed for commercial interests. PIAC further suggests prioritizing proactive disclosure of third party contracts, especially with parties within the tech and communications industry. PIAC believes that a culture of proactive disclosure is critical to fostering the trust of Ontarians. Consistent with the IPC's goal of "enhancing the role of the public interest in access to information," proactive disclosure better enables consumer interest groups like PIAC to play a role in public accountability, and to help scrutinize public-private partnerships.

9. In the Consultation Paper, de-identification is discussed in the context of developing de-identification guidelines "with a view to encouraging the responsible public release of data, while protecting personal information."[2] It goes without saying that datasets released to the public should not contain identifying information. PIAC believes that de-Identification is more important in discourse about how institutions may responsibly use data, discussed below.

Responsible Use of Data for Good

10. PIAC has always taken issue with the use of "innovative and socially beneficial" as buzzwords to encourage more public-private partnerships. Commercial interests can be framed as "innovative and socially beneficial." The IPC's use of these terms in its goal statement risks promoting a paternalistic culture in the development of privacy practices and partnerships with third parties. There is a difference between serving social benefits and serving individual rights. PIAC cautions the IPC not to treat the two interchangeably, and to resist allowing institutions to hold out "innovation" as justification for increasingly privacy-invasive practices.

11. Regarding the responsible use of data, PIAC applauds the IPC for asking the right questions: "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?"[3] These are questions that the federal government has apparently failed to

[1] Information and Privacy Commissioner of Ontario, "IPC Strategic Priority Setting Consultation", (Toronto: IPC, December 2020), at p. 9.
[2] Information and Privacy Commissioner of Ontario, "IPC Strategic Priority Setting Consultation", (Toronto: IPC, December 2020), at p. 8.
[3] Information and Privacy Commissioner of Ontario, "IPC Strategic Priority Setting Consultation", (Toronto: IPC, December 2020), at p. 11.

ask in drafting Bill C-11, which extensively excises individual rights to informed consent. In answering the above questions, the IPC must carefully consider input from multiple stakeholders, but also cast particular scrutiny on stakeholders who are driven by commercial interests rather than concern for individual rights.

12. Data trusts have become a pillar in the ongoing discourse about new data governance models. As with any framework that seeks to support more public-private collaborations, PIAC believes that the key consideration is to avoid rendering data trusts a source of personal information to drive commercial growth at the expense of privacy. The government of Ontario, in their recent 2020 consultation on strengthening privacy protections, defined data trusts as "a legal mechanism that enables an organization's data to be governed by a trusted third party, to ensure the transparent and accountable use of that data."[4] There are many questions that need to be answered based on this statement: What are the appropriate oversight mechanisms, access and correction rights, and retention periods in the legal framework? Will data trusts be populated according to the type of data, or the purpose for which data is used? Who can be the trusted third party, and what responsibilities should they have to uphold a high standard of transparency and accountability? The only way to answer these questions is to dedicate a comprehensive multi-stakeholder consultation process, possibly even multiple rounds of consultations, about data trust regimes.

13. Between the federal and provincial government, there have been no meaningful steps taken toward proposing concrete regulations, guidelines, principles or standards for data trusts. Current discussions are still largely nebulous, even inconsistent. For example, the Ontario government's discussion paper on private sector privacy reform states that data trusts "allow organizations to assign an individual as the custodian or steward for the data, agree on a standard set of rules for how data would be shared, and ensure that whoever has access to the trust uses the data in accordance with these results."[5] On the other hand, ISED in their 2019 paper on private sector privacy modernization explains that data trusts treat "datasets as assets that an independent third party must manage according to contractual terms designed to ensure the responsible, appropriate use of those assets."[6] Are data trusts then governed by individuals within an organization, or by an independent third party organization? PIAC believes that a workable data trust regime must be built on consistent provincial and federal interpretation, therefore the IPC must resolve inconsistencies before developing any governance guidelines.

---

[4] Ontario, Ministry of Government and Consumer Services, "Ontario Launches Consultations to Strengthen Privacy Protections of Personal Data", (13 August, 2020), online: https://news.ontario.ca/en/release/57985/ontario-launches-consultations-to-strengthen-privacy-protections-of-personal-data

[5] Ministry of Government and Consumer Services, "Ontario Private Sector Private Reform: Improving private sector privacy for Ontarians in a digital age, Discussion Paper", (13 August 2020), online: https://www.ontariocanada.com/registry/showAttachment.do?postingId=33967&attachmentId=45716

[6] Canada, Innovation, Science and Economic Development, "Strengthening Privacy for the Digital Age: Proposals to modernize the *Personal Information Protection and Electronic Documents Act",* (21 May 2019), online: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

14. PIAC notes that Bill C-11 introduces de-identification as a tool to expand the potential uses of personal data while supposedly protecting privacy interests. The Consultation Paper engages with de-identification in the context of protecting personal information in publicly-released datasets, and in the context of using data for so-called "beneficial purposes." While these purposes merit discussion, the greater issue with de-identification is how such a process can be abused to exploit massive volumes of personal information for commercial interests, without the consent or knowledge of individuals. The IPC's existing "De-Identification Guidelines for Structured Data" ("Guidelines") is a good preliminary approach to practice guidelines, but it largely applies only to publicly-released datasets.

15. The Guidelines do not meaningfully address any principles and practical rules for de-identification for the internal use of personal information by public or private organizations. Perfunctorily, the Guidelines mention that "[n]on-public data releases provide the least availability but can provide a higher amount of protection, requiring a smaller amount of de-identification."[7] Reference to a sliding scale of de-identification implies that the usefulness of personal data decreases as more identifiers are stripped away, therefore organizations are inevitably incentivized to preserve as many identifiers as possible for their own data analyses.

16. PIAC agrees with the IPC that it is critical to protect de-identified data from re-identification, but it is equally important to protect individuals from the consequences of data analyses carried out by public and private parties without individuals' knowledge or consent. This is where the bulk of the research and policy work should be focused, to ensure any use of de-identification is subject to a governance framework that is, as the IPC states, "fair, accountable, and transparent, in accordance with Ontarians' values and realities."[8]

Access, Privacy and Youth

17. Today's children and youth have increasingly easy access to Internet-enabled devices, and therefore access to social media platforms that generally provide very little privacy protections for young users. The IPC has stated it has developed resources for teachers of grades 5 to 12, but PIAC recommends developing guidelines and lessons for digital literacy in earlier grades, as even very young children may already have a digital footprint due to early access to the Internet, and due to parents posting pictures and information about their children on social media. PIAC believes that digital literacy campaigns should also reach out to parents, who play a major role as the initial "gatekeepers" of Internet access for their children.

[7] Information and Privacy Commissioner of Ontario, "De-identification Guidelines for Structured Data", (Toronto: June 2016), at p. 4, online: https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf

[8] Information and Privacy Commissioner of Ontario, "IPC Strategic Priority Setting Consultation", (Toronto: IPC, December 2020), at p. 12.

18. The IPC has stated that a first step in this strategic area is to work with the Ministry of Education and provincial school boards to better understand the virtual tools and platforms used in schools. In light of recent heavy reliance on distance learning platforms like Zoom, Brightspace, and Google Classroom, a good first step would be to review how such platforms collect and use the personal information of young users. To maximize the relevance and effectiveness of guidelines and campaigns, the IPC should also conduct a comprehensive survey of how children and youth use social media, and how they relate to their own digital rights. It is one thing to study privacy policies themselves, but another thing altogether to understand the reality of digital literacy in today's children and youth.

Next-Generation Law Enforcement

19. PIAC notes that the IPC, in their goal statement for this strategic area, emphasizes the enforcement of "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."[9] However, even in the past year, the IPC has repeatedly fallen short of enforcing this standard. For example, the IPC admitted that it did not know that the Toronto Police Service had been using Clearview AI's facial recognition technology until the IPC was notified by the Service.[10] The IPC must determine how this was allowed to happen despite "providing advice to law enforcement agencies on the use of algorithmic surveillance technologies, such as automated licence plate recognition and facial recognition."[11]

20. The IPC again demonstrated its blindness when the Canadian Constitution Foundation, through an access-to-information request, revealed that Ontario police had been unlawfully accessing a database of Ontarians who tested positive for COVID-19.[12] Despite the shutdown of this portal after a legal challenge from several human rights organizations, and despite reports demonstrating misuse of personal health information, the IPC took the view that the police "took appropriate steps to ensure personal information was used in accordance with Ontario's privacy laws."[13] Test centres did not even obtain the knowledge and consent of individuals to use their personal health information for this purpose. Regarding the ongoing investigation on police access to the COVID-19 database, the IPC has expressed that "[i]f any reports are

---

[9] Information and Privacy Commissioner of Ontario, "IPC Strategic Priority Setting Consultation", (Toronto: IPC, December 2020), at p. 16.

[10] Information and Privacy Commissioner of Ontario, News Release, "Information and Privacy Commissioner of Ontario Statement on Toronto Police Service Use of Clearview AI Technology", (14 February 2020), online: https://www.ipc.on.ca/information-and-privacy-commissioner-of-ontario-statement-on-toronto-police-service-use-of-clearview-ai-technology/

[11] Information and Privacy Commissioner of Ontario, "IPC Strategic Priority Setting Consultation", (Toronto: IPC, December 2020), at p. 17.

[12] The Canadian Press, "Ontario police used COVID-19 database illegally, civil rights groups find", *CBC News* (30 September 2020), online: https://www.cbc.ca/news/canada/toronto/covid-police-database-1.5745481

[13] Information and Privacy Commissioner of Ontario, News Release, 'Police use of COVID19 First Responder Portal", (21 December 2020), online: https://www.ipc.on.ca/newsrelease/police-use-of-covid19-first-responder-portal/

produced at the conclusion of our investigation into this matter, they will be made available to the public at that time."[14] PIAC advises that the public release of a report should not be a matter of *if* such a report is produced, but *when*.

21. The IPC noted in the Consultation Paper that the increase of information collection by law enforcement is "likely to continue as law enforcement agencies increasingly turn to surveillance technologies as a tool for enhancing public safety and improving operational efficiencies."[15] In light of this prediction, the IPC must ensure that privacy violations do not increase in proportion to the use of technology-assisted policing, and furthermore that the IPC does not continue its pattern of being caught unaware of privacy-invasive police conduct.

Trust in Virtual Health

22. PIAC has illustrated above the importance of privacy in the intersection of policing and health during the pandemic. More generally, the pandemic has created new categories of personal health information that could potentially be misused. Information like vaccination status, or information relating to COVID-19 testing, or the severity of an individual's illness or long-term effects are all data upon which institutions and organizations may seek to make decisions about individuals. The IPC must anticipate these potential risks, and accordingly develop guidelines to protect COVID-related personal information from being used to discriminate against individuals in the future (ie. in insurance or employment contexts).

Conclusion

23. At both the provincial and federal level, privacy rights currently stand at a critical precipice of change, and within the last two years, reform discussions and consultations have escalated for both public and private sector privacy. The balancing of individual rights and commercial interests is a common tension point among these recent proceedings. PIAC advocates strongly in favour of the former, and believes the IPC should also prioritize individual rights within each of the six strategic priority areas laid out in this Consultation. In Bill C-11, the federal government has already demonstrated its intention to enable significantly greater collection, use, and disclosure of personal information for so-called "business purposes," at the expense of individual knowledge and consent rights. PIAC advises the IPC to avoid the federal government's approach, and to keep transparency, accountability, and individual privacy rights at the forefront in developing future guidelines, particularly for novel governance models and tools like data trusts and de-identification.

[14] Information and Privacy Commissioner of Ontario, News Release, 'Police use of COVID19 First Responder Portal", (21 December 2020), online: https://www.ipc.on.ca/newsrelease/police-use-of-covid19-first-responder-portal/
[15] Information and Privacy Commissioner of Ontario, "IPC Strategic Priority Setting Consultation", (Toronto: IPC, December 2020), at p. 17.