



Information and Privacy
Commissioner of Ontario

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

SEPTEMBER 2021

IPC Response to the Ontario Government's Consultation on a New Provincial Data Authority

The Information and Privacy Commissioner of Ontario (IPC) welcomes this opportunity to comment on the Ontario government's consultation on its proposal to create a provincial [Data Authority](#) as part of its overall [Digital and Data Strategy](#). The IPC is encouraged by the government's commitment to provide useful data to Ontarians and to inspire trust by protecting privacy and ensuring data security. In keeping with its mandate, the IPC offers the following high-level submissions on Themes 1, 2 and 4: ensuring privacy and transparency, increasing access to high-value government data, and promoting equity and responsibility.

Theme 1: Ensuring privacy and transparency

The effectiveness of the proposed Data Authority to ensure privacy and transparency will depend on whether its purpose, functions, and powers are aimed at addressing real gaps in the present system — rather than duplicating existing structures — and anticipating the types of protections that will be required for the future.

The strategy explains that a proposed Data Authority could be “responsible for building modern data infrastructure to support economic and social growth at scale, while ensuring that data is private, secure, anonymous, and cannot identify people individually.” This gives a sense of the general zone of the Data Authority's work. But the strategy itself does not clearly indicate the specific purposes of a Data Authority or the powers, duties, and functions it would have to meet its objectives. It is not possible from the consultation document to know whether the Data Authority would be something like a secure data trust, a technical standards-setting body for government, a public-facing service organization, a new policy, a transformation in culture, or something else aimed at promoting government's effective use and sharing of valuable data.

The IPC looks forward to reviewing more specific proposals defining the contours and content of the Data Authority currently being considered. In the meantime, however, the IPC offers the following high-level comments.

Data Authority must be subject to independent oversight

The proposed Data Authority, like all government institutions that coordinate or work directly with personal information, should be designated as an institution for the purposes of section 2 (1) of the *Freedom of Information and Protection of Privacy Act (FIPPA)*, and made subject to independent oversight by the IPC.



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

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel/Tél : (416) 326-3333
1 (800) 387-0073
TTY/ATS : (416) 325-7539
Web : www.ipc.on.ca

As an office of the Legislative Assembly, the IPC is independent from the government, which gives it the unique ability to provide impartial independent oversight of the access and privacy decisions and practices of government institutions. The IPC also oversees institutional governance of data and personal information in respect of certain designated super-structures. These entities have greater flexibility under the law to perform a special gate-keeping role in collecting, using, linking, and analyzing data from various sources, managing different datasets, and enabling access to data by other organizations or institutions subject to explicit conditions or standards. Examples of super-structures include: inter and extra ministerial data integration units under Part III.1 of *FIPPA*; the Independent Electricity System Operator (IESO) as a designated institution under *FIPPA*; prescribed entities, persons and organizations like the Institute of Clinical and Evaluative Sciences (ICES) and Ontario Health, under the *Personal Health Information Protection Act (PHIPA)*. The IPC would expect to play a similar independent oversight role in respect of any new Data Authority, including in respect of its privacy and security policies and practices, its data governance structures and processes, and its overall compliance with Ontario's privacy laws.

Enhance privacy protections commensurate with any augmented powers or authorities granted to government.

Any additional legal powers or authorities granted to government as a part of the strategy should be accompanied by a commensurate level of enhanced privacy protections for Ontarians. This includes long-overdue updates to *FIPPA* — for example, to require institutions to conduct privacy impact assessments for high-risk initiatives, and to report data breaches to Ontarians and to the IPC above a certain threshold. There are two reasons for this. First, updates to *FIPPA* would signal to Ontarians that their government institutions are evolving in a good balance — with new powers for government institutions come up-to-date protections for Ontarians. Second, making updates to the general rules in *FIPPA* instead of creating many different special-purpose privacy protection regimes would make more practical and operational sense. It would avoid confusion and unintended consequences caused by the interaction of many sets of rules in a system that should instead become more clear and efficient.

Relationship of Data Authority to existing privacy laws governing disclosure

The IPC encourages the government to consider closely the relationship of a proposed Data Authority to the existing legal provisions for disclosure of information in *FIPPA*, *PHIPA*, and Part X of the *Children and Youth Family Services Act (CYFSA)*.

The Data Authority may interact with several existing legislative schemes governing the use and disclosure of personal information and personal health information under certain statutory conditions. These include, but are not limited to:

- Rules for prescribed entities that analyze or compile statistical information for the management, evaluation, monitoring, resource allocation and planning of the health system under *PHIPA* s. 45(1);
- Rules for prescribed persons who maintain registries of personal health information under *PHIPA* s. 39(1)(c);

- Technical standards governing the work of data integration units under *FIPPA* Part III.1;
- Provisions which allow access to information for research purposes such as *PHIPA* s. 44 (1) and *FIPPA* s. 21(1) (e); and
- Provisions which allow disclosure of personal information without consent for defined purposes under *CYFSA* Part X s.292(1).

If any new rules or legal authorities are created to support the strategy, the IPC recommends that they be drafted in a way that leaves no confusion about whether the new provisions are meant to supplement, be subject to, or override provisions that are already set out in laws or regulations.

The government's strategy to secure Ontarians' privacy rights in our digital economy and society requires an integrated, cross-sectoral approach to privacy protection.

The strategy consultation document states that the government is committed to making Ontario a world leader in data and privacy rights. The IPC applauds the government's intention to move Ontario ahead by making sure that Ontarians are safe to "interact or do business online." But one thing is certain: Ontario cannot fully meet this goal without a provincial privacy law that applies to the private sector in a manner which is integrated with its public, health and child and youth sector privacy laws. If the objective of the strategy is to make high-value government data available to third parties, including private sector organizations, those recipient organizations must be held equally accountable for upholding the privacy and security of that data. Even if the federal government legislates the best possible updates to federal privacy laws, important parts of life and business in Ontario are beyond its constitutional reach. Among the critical gaps that remain and are in need of a more coherent provincial approach include employees of provincially regulated businesses and non-commercial activities of not for profit organizations, professional associations and political parties. For these and other reasons set out in the [IPC's response](#) to the government's consultation about a provincial private sector privacy law, Ontario will not be able to fully meet the goals in its Digital and Data Strategy until it has its own best-in-class provincial law.

Theme 2: Increasing access to high-value government data

Proactively giving Ontarians access to useful data held by government supports not only economic goals of promoting innovation and investments in the province, but also fundamental goals of transparency, accountability and civic engagement in a healthy democracy.

The IPC commends the approach in the strategy that focuses on generating the greatest societal benefits from government's data — not only using or disclosing the collections and formats of information that are closest at hand. High quality data, as well as tools to interpret and use it, could help Ontarians spot challenges and seize opportunities in their digital society and economy. This could support Ontarians' life choices, community involvement, participation in democratic processes, as well as decisions about their businesses, education, employment, and environmental impact.

A new Data Authority could help advance the common data disclosure challenges and opportunities facing government.

Among other things, the proposed Data Authority could significantly advance the government's openness objectives by helping to address the same fundamental challenges that many ministries face as they consider disclosing data to third parties. These include:

- How to effectively and efficiently de-identify information and exploit other privacy-enhancing technologies to make the benefits of data available to Ontarians without violating their privacy rights;
- How to determine whether to accept or deny data access requests, in accordance with a robust review, assessment and governance process that weighs the societal risks and benefits, ensures transparency to Ontarians and takes accountability for decision-making;
- How to coordinate and track the flows of information that was gathered by government for a particular purpose and subsequently used for another, and be publicly transparent about these data flows; and
- How to help Ontarians — and even the government itself — better understand the spaces where data collections could occur as well as the types of data and information being collected.

The proactive disclosure of data held by government should improve the efficiency and timeliness of the existing rights to request and access government information.

Proactive disclosure of government data sets will never eliminate the need for the existing freedom of information regime under *FIPPA* and other laws that enable access to government-held data, including one's own personal information. That said, well-designed data disclosures and open government practices could help reduce delays and administrative burdens when Ontarians seek information. As the strategy is put in place, the IPC urges the government to consider proactive disclosure of information that is in high demand through *FIPPA* requests, as well as disclosure of data that has already been disclosed in response to a request. Moreover, the IPC recommends that any information practices or technology put in place to support the strategy are also specifically designed to make the government's information holdings easier to search and process when responding to an access request.

Theme 4: Promoting equity and responsibility

Making data more accessible and inclusive

Extending the benefits of open data to all Ontarians will require careful attention to our diverse accessibility requirements when the methods and formats of data are being considered. Plain language explanations will help, as will open-source tools and formats to allow Ontarians to build and use applications to make sense of data.

The proposed Data Authority could help ensure equity and responsibility by, among other things:

- Assessing and mitigating equity concerns — including the potential for bias and discriminatory use — relating to data sets, algorithms, and automated systems that use or are trained on data;
- Ensuring that disclosure of information advances the interests of all Ontarians and does not increase vulnerabilities; and
- Working with Indigenous partners when the data being considered arises from, or could be valuable to, Indigenous individuals and communities, as well as Indigenous governments, cultures, or lands.

Conclusion

An iterative approach for a Data Authority

The IPC recognizes that it is not a simple task to design a Data Authority that would address both present and potential future problems, while fitting well into the existing laws and government systems. For this reason, the IPC supports the iterative approach to the design of the Data Authority described in the strategy. Further use cases and other planning activities could help build a proposal that includes details about the Data Authority's planned purpose, powers, duties, functions, and governance. This more detailed explanation should be provided to Ontarians and to interested stakeholders, including the IPC, for further consultation before any steps are taken to create any new permanent structure and/or any new legal authorities. The IPC welcomes continued dialogue on this and other aspects of the province's Digital and Data and Strategy.