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

OPEN LETTER

November 28, 2019

The Hon. Lisa M. Thompson
Minister
Ministry of Government and Consumer Services
College Park, 5th Floor
777 Bay Street
Toronto, ON M7A 2J3

Dear Minister Thompson:

Re: Government of Ontario's *Better, Smarter Government* Discussion Paper

Attached please find our comments on the most recent data strategy discussion paper (Appendix A). We focused on the issue of data sharing, and did not comment on topics we covered in our previous letters (for example, procurement and training and skill development).

We look forward to working with you and the Ontario Digital Service to help the government ensure its data strategy proceeds in a manner that protects Ontarians' access and privacy rights.

As with our comments on the other two discussion papers, we are posting this letter and attachment on our website.

Sincerely,

Brian Beamish
Commissioner

cc: Dominic Roszak, Director of Operations, Stakeholder Relations and Appointments, Ministry of Government and Consumer Services

Hillary Hartley, Chief Digital and Data Officer, Deputy Minister, Cabinet Office

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
Fax/Téléc: (416) 325-9195
TTY/ATS: (416) 325-7539
Web: www.ipc.on.ca

Appendix A
IPC Comments on the Ontario Government's *Better, Smarter Government* Discussion Paper

The discussion paper outlines a number of benefits for broad data sharing such as designing better services and delivery, more effective planning and evaluation of programs and services, making interaction with government easier and less burdensome for the public, and grounding government programs and services in evidence and insight.

While acknowledging the potential benefits of data sharing for both the public and government, when it involves personal information, data sharing can raise significant privacy risks. Our comments focus on the privacy concerns that arise from sharing personal information.

Data sharing can raise the spectre of Big Brother with massive centralized databases, and create anxiety about altering the power balance between the individual and the state. Recent surveys confirm that the public is concerned over the loss of control over their own personal information held by government. For example, the Office of the Privacy Commissioner of Canada's latest privacy survey found:

- the majority of Canadians expressed discomfort with the Government of Canada sharing their personal information with foreign governments or authorities (75%), with another federal department without their consent (64%), or with another federal department for some purpose that they are not aware of (60%)

- the majority (81%) said they would be at least somewhat comfortable with the Government of Canada sharing their personal information with another department of the Government of Canada with their consent[1]

A recent American survey found that 84% of respondents think they have very little or no control over their data collected by government. The majority (78%) said they have very little or no understanding of what the government does with their data, and 64% said they are somewhat or very concerned about how the government is using their data.[2]

Use of advanced information technology and data-driven practices, combined with data sharing, create the potential for administrative efficiencies and more informed decision-making. At the same time, there is the potential for abuse and compromising individuals' existing rights.

[1] Office of the Privacy Commissioner of Canada, *2018-19 Survey of Canadians on Privacy*, Final Report, March 2019, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/#fig02.
[2] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner, Pew Research Center Internet and Technology, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, November 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

In addition to the potential loss of control over personal information, privacy risks that may arise related to data sharing include:

- use of data for purposes unrelated to the reason it was collected, or by unknown users
- decisions made using inaccurate and outdated data without the knowledge of the data subject, and to the detriment of the individual
- enhanced government profiling, surveillance and intrusion into individuals' lives
- lack of accountability for the protection of personal information
- increased risk of security and privacy breaches[3]

If the data sharing is not open and transparent, individuals will not be in a position to make informed decisions about how their information is collected, used and disclosed by governments, or have the opportunity to access or correct their personal information.

The discussion paper notes the importance of protecting privacy, including in relation to data sharing to support planning, analysis and service delivery, and in relation to open data programs. Strong and comprehensive privacy protections, discussed below, are essential to appropriately balancing individuals' rights with potential benefits, and for the public acceptance of any government data sharing initiative.

DATA SHARING FOR PLANNING, ANALYSIS AND EVALUATION

The discussion paper notes that within the Government of Ontario, data exists in silos and is not readily accessible. It also observes that program evaluation data, if effectively collected and shared, can provide valuable insights into how programs work and can be optimized for better outcomes for Ontarians. It is important to clarify that Ontario's public and health sector privacy laws currently enable data sharing for the management and allocation of resources, and planning and evaluating programs and services.

The *Freedom of Information and Protection of Privacy Act* was recently amended to include a framework for privacy protective data sharing for those purposes. The IPC is currently working with the government to develop supporting data standards. In addition, the *Personal Health Information Protection Act* permits the sharing of personal health information to the Minister of Health for funding, planning or delivering health services or allocating resources.

The data sharing provisions in *FIPPA* and *PHIPA* illustrate that Ontario's privacy laws do not create barriers to data sharing necessary for planning, analysis and evaluation. Rather, they enable

[3] Stephanie Perrin, Jennifer Barrigar and Robert Gellman, *Government Information Sharing: Is Data Going Out of the Silos, Into the Mines?*, An Independent Research Report Commissioned by the Office of the Information and Privacy Commissioner of Alberta, January 2015, https://www.oipc.ab.ca/media/389571/Report_Government_Information_Sharing_Jan2015.pdf, pp. 9, 10 and 12.

the government to design better, smarter and more efficient programs and services, while protecting privacy.

DATA SHARING FOR SERVICE DELIVERY

We challenge the assertion in the discussion paper that Ontario's privacy laws restrict the government's "ability to develop modern policies and deliver services that Ontarians expect from a government in 2019." Too often, privacy is erroneously touted as a barrier to modernization.

The discussion paper states that the province's privacy legislation enables the government to collect, use and disclose personal information for "legitimate, limited and specific purposes." Data sharing can and should operate within those parameters.

For the province to share personal information for purposes beyond what is allowable under *FIPPA*, it must have the legal authority to do so. If legislative amendments are required, we would be pleased to work with the government to ensure that appropriate privacy protective measures are included.

Broadly speaking, any data sharing legislation should define comprehensive requirements for all entities involved, and ensure transparency and accountability for all data sharing activities. Specifically, the legislative framework should:

- define the purposes for which personal information may be lawfully shared and when it is prohibited
- define the organizations that have the legal authority to collect, use and disclose personal information (that is, data providers and users)
- define when disclosure of personal information requires the data subject's consent, and when it may be done without consent
- require data minimization and appropriate de-identification in defined circumstances
- require justification and effective controls by participating parties (for example, completion of business cases, data sharing agreements and privacy impact assessments prior to data sharing)
- define transparency and access measures
- establish appropriate integrity, accountability, oversight and enforcement controls
- define complaint process and remedies
- define breach notification requirements

The discussion paper states that protecting privacy is of "paramount importance." For any data sharing scheme to be successful, the government must have the legal authority and privacy

protection must be embraced. This has been essential to public acceptance in other jurisdictions that have implemented, or are contemplating, data sharing schemes.

Data Minimization

Data minimization should be a central requirement in any data sharing legislation. The government needs to define legal requirements to minimize the amount of personal information involved in data sharing, including that public organizations must not collect, use or disclose:

- personal information if other information will meet the purpose, and
- more personal information than is reasonably necessary to meet that purpose

Such requirements are not new to Ontario's public organizations. Clear data minimization provisions are set out in *PHIPA*, the *FIPPA* data integration amendments described above, Part X of the *Child, Youth and Family Services Act*, and the *Anti-Racism Act*.

Consent and Data Subject Control

As noted above, any data sharing scheme involving personal information raises significant privacy concerns about individuals' lack of control over their own information.

A key issue to be addressed in data sharing legislation should be if, or when, data subjects' consent for disclosure of their personal information will be required, and the appropriate manner of that consent (for example, express or implied, opt-in or opt-out).

In certain circumstances, consent may be the most appropriate basis upon which to disclose personal information (for example, one-off or unique instances of data sharing). However, there may be circumstances where consent is not a suitable or viable option for enabling data sharing (for example, law enforcement). For the latter situations, the legislative framework must define the authority to share personal information.

We recommend the government engage the public in extensive consultation about the issue of consent and data sharing. We also encourage the government to look for legal, procedural and technical measures to maximize the individuals' control over their personal information, and their ability to monitor how their personal information is used and disclosed, and to report any transgressions to an appropriate oversight body.

Data Quality

Any legislation that enables the sharing of personal information to support service delivery should include clear requirements to verify the accuracy, completeness and timeliness of the information before it is used and disclosed. This requirement is essential when personal information is shared on a large scale, linked or matched with other personal information, or used to make decisions that might adversely affect individuals' rights and entitlements to government benefits and services.

Poor quality personal information increases the risks to privacy and decreases the ability of the government to deliver user-centric services. Ontario's privacy laws, as well as a number of the laws noted above, already require organizations to take reasonable steps to ensure data is as accurate as is necessary for the purpose before it is used.

Poor quality of data may:

- impact the usefulness of sharing, which can contribute to reluctance to support sharing
- increase the pressure to use identifiable data to improve the quality
- lead to organizations not wanting to accept data offered[4]

Digital Services

A key privacy challenge with data sharing related to online service delivery is how to design a reliable and privacy protective scheme for authenticating the identity of individuals. An effective and secure digital identity is a necessary enabler for the provisions of online services.

While a digital identity would be necessary for processes designed to create conveniences and cost savings, it also could facilitate the linking of disparate personal information across government. Public acceptability of a digital identity will depend, in large part, on establishing the proper balance between the legitimate information needs of government and individuals' right to privacy.

Robust privacy and security measures, transparency, as well as strong governance, oversight and enforcement will be required. These measures are also necessary to restrict the function creep that could occur with a digital identity and associated unique identifying number, symbol or other particular assigned to the individual.

To avoid function creep, we recommend legislative restrictions on the collection, use and disclosure of any identity number. In addition to advancing transparency and accountability, this would also help limit the potential for privacy-invasive profiling and surveillance. The limits in the *Personal Health Information Protection Act* for the use of the health number provide a good example. They have prevented the health card from becoming a universal identifier used for unrelated purposes.

[4] United Kingdom Law Commission, *Data Sharing between Public Bodies: A Scoping Report*, July 2014, https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2015/03/lc351_data-sharing.pdf, pp. 115-116.

PUBLIC ENGAGEMENT

The government is aware that, in Canada and other jurisdictions, major initiatives designed to modernize government have failed, in part, because of adverse public reaction and lack of broad consultation. Due to this, other governments have undertaken extensive public engagement about data sharing in order to educate and get feedback from the public, and to be transparent about their proposals, actions and decisions (for example, Australia and the United Kingdom).

For any data sharing initiative to succeed, the province must engage the public to foster the necessary trust, confidence and acceptance – sometimes known as social licence. Effectively addressing the potential privacy issues is essential to obtaining public support.

Justification

To develop social licence for data sharing, the province needs to provide the public with more detailed information about its justification, costs and benefits, as well as the proposed scope of the initiative and rationale (for example, whether data sharing would cover just ministries, all of the Ontario Public Sector, the broader public sector, or private sector as well). Broad assertions or assumptions about the potential benefits are not sufficient. Before the government proceeds, Ontarians require substantive information to make evidence-based decisions about the merits of data sharing, and whether their rights are appropriately protected.

Public engagement and justification must not be just a one-time undertaking. In a number of other jurisdictions, prior to specific data sharing occurrences, the involved entities must justify the need and define the tangible benefits expected from the sharing, who will receive those benefits, and how they will be measured.[5] For example, in the United Kingdom, the requirement for the parties to complete business cases and data sharing agreements, which are then published, drives this analysis and accountability.

Transparency

The discussion paper states that "Ontarians must feel confident that their personal information is being managed by government in ethical and lawful ways." That confidence is a prerequisite for the success of any data sharing scheme. It is predicated on full transparency regarding the development, implementation, ongoing operation, and evaluation of the government's activities. As noted above, any legislative framework for data sharing should define appropriate transparency measures.

For example, Australia is currently developing its data sharing initiative. The Australian government is marketing transparency as "a key pillar underpinning the Data Sharing and Release

[5] United Kingdom Cabinet Office, *Digital Economy Bill: Digital Government (Part 5), Introduction to Data Sharing Codes of Practice*, October 19, 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567319/2016-10-20_Digital_government_codes_of_practice.pdf, p. 19.

legislation to build public trust and confidence."[6] Similar to the United Kingdom's transparency requirements, the Australian National Data Commissioner will be required to publish registers of data sharing agreements, and accredited users and data service providers. The public registers are designed to increase transparency about what, why and how data is being shared, including who is accessing the data. The Commissioner will also publish an annual report on the operation and integrity of the data sharing system.[7]

[6] Australian Government, Department of the Prime Minister and Cabinet, *Data Sharing and Release: Legislative Reforms Discussion Paper*, September 2019, https://www.datacommissioner.gov.au/sites/default/files/2019-09/Data Sharing and Release Legislative Reforms Discussion Paper - Accessibility.pdf, p. 35.
[7] Ibid., pp. 35 and 37.