President
of the Treasury Board

Présidente
du Conseil du Trésor

Ottawa, Canada K1A 0R5

Mr. Pat Kelly
Chair, Standing Committee on Access to Information, Privacy and Ethics
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Kelly,

Pursuant to Standing Order 109 of the House of Commons, I am pleased to respond on behalf of the Government of Canada (the Government) to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics (the Committee), entitled "Collection and Use of Mobility Data by the Government of Canada and Related Issues" (the Report), tabled in the House of Commons on May 2, 2022.

I wish to sincerely thank the members of the Committee for their time spent examining the use of mobility data during the COVID-19 pandemic and Canada's personal information protection regimes, as well as to provide thoughtful recommendations on those topics. I am grateful as well to the stakeholders and individuals who appeared before the Committee to express their views and provide evidence and expert advice.

Canada takes privacy very seriously and has a strong foundation of privacy protection as evidenced by the *Privacy Act*, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and a suite of policy instruments to support Government institutions in complying with the *Privacy Act.*

The Government is actively working on modernizing both the PIPEDA and the *Privacy Act* to address the issues identified in the report, for example with regard to transparency, de-identified data, and other elements of the legislation that can be strengthened. This will help meet current and future needs of the country as it continues to evolve into a digitally and technologically enabled service model.

Bill C-27, the *Digital Charter Implementation Act, 2022*, was introduced in June 2022 and proposes to replace the PIPEDA with an entirely new law to protect personal information that is handled in the course of private sector commercial activities. The bill introduces new concepts to reflect technological realities of the digital marketplace, and fundamental changes to the enforcement regime. The Department of Justice Canada (JUS) is also developing proposals to modernize the *Privacy Act*, which would include a

.../2

framework in respect of the collection, use, disclosure, retention, and safeguarding of de-identified information commensurate with the privacy risks. Meanwhile, the Treasury Board of Canada Secretariat (TBS) reviews its policy instruments regularly or at least every five years to assess their continued effectiveness and accuracy.

It is also important to recognize that we are living in unprecedented times. During the pandemic, the Public Health Agency of Canada (PHAC) purchased and used de-identified and aggregated mobility data received from third parties to assess mobility patterns of Canadians with the objective of understanding the spread of the virus and taking informed public health decisions. The private sector companies involved confirmed that no identifiable data was provided to PHAC during the mobility program and that they used best industry standards in sharing the de-identified data. Due to the level of de-identification and aggregation of the data, the Government could not identify individuals in the datasets, so the data did not engage the *Privacy Act*. The program highlights how it is essential to strike the right balance between collecting data for the public good, while respecting privacy and security obligations.

The Government has carefully considered the Report. The Response, contained herein, addresses the 22 recommendations put forward by the Committee by grouping them into three themes reflecting the Government's holistic approach to privacy protections: 1) Mobility Program; 2) Data; 3) Legislative Reform. Through these three themes, the Government will demonstrate how it will or is addressing the recommendations.

Mobility Program
(Pertaining to recommendations 4, 5, 6, 21, and 22)

Summary of recommendations:

- Update *COVIDTrends* webpage to include where the data originates from, what data providers are providing the information and opt-out information.
- Undertake measures to inform of mobility data collection programs on an ongoing basis that includes the nature and purpose of the data collection.
- Ensure only the requesting department or agency can use the collected mobility data and that any other department or agency be specified in the tender with rationale.
- Increase public awareness and education of mobility tracking and disease surveillance initiatives.
- Develop clear guidelines regarding the use of mobility data and consult with the OPC, stakeholders and groups that may be disproportionately affected by such an initiative.

The Government acknowledges these recommendations and commits to continuing the work toward increasing public transparency and education. In the context of the acquisition of mobility data from the private sector, the Government took steps to be transparent with Canadians through a public announcement by the Prime Minister's

.../3

Office, proactive disclosure of contracts and weekly updates to the mobility indicator on the *COVIDTrends* webpage, which explained the sources of the mobility data. This page was regularly spotlighted in tweets from the Chief Public Health Officer of Canada, Dr. Tam, and other PHAC communications to the public. The Government also informed the Office of the Privacy Commissioner (OPC) about the mobility program and offered to respond to any questions the OPC might have or provide further briefings, should the OPC wish. The Government recognizes the need for more transparency, particularly in the context of mobility data.

While the Government did not collect the personal information in its acquisition of de-identified and aggregated mobility data, public perceptions of potential government overstep, and privacy concerns over government use of data, are important issues that should be considered and addressed.

The Government will take actions in line with these recommendations by including proactive transparency efforts on existing and future data products to increase public trust, especially as it relates to mobility data. These actions include:

- providing more information and more regular updates on *COVIDTrends*;
- creating a public facing dashboard that highlights public health trends such as mobility data, along with information on data sources, opting out, and frequently asked questions;
- continue to contract lawfully and in line with information sharing and contracting requirements with robust safeguards, including embedding in contracts options to opt-out of the third-party operators' data collection programs and that only the departments and agencies specified have access to the mobility data;
- strengthening proactive communication with Canadians through social media campaigns and public announcements, as well as public engagement with broader stakeholders and community groups; and,
- establishing an external review panel of experts in privacy, data, de-identification and Indigenous data sovereignty to work with and inform the Government's ongoing work to improve data in public health.

Data
(Pertaining to recommendations 1, 2, 15, 16, and 20)

Summary of recommendations:

- Stipulate in all future requests for proposals for collecting data that Canadians have the option to opt out of the data collection, and that the method for opting out be easily understood, communicated and publicly available.
- Meaningfully consult with the Privacy Commissioner before engaging in a data collection program and continue to do so for the duration of the program.
- Require that companies that generate, manage, sell or use data to comply with a framework additional to self-regulation.

.../4

- Conduct audits on the source of the data and meaningful consent, collection, transmission and use of data.
- Increase investment in digital literacy initiatives, including the risks associated with the collection and use of big data.

The Government acknowledges these recommendations and will give due consideration to them in future policy and legislative amendments, where appropriate.

Reliable, timely, and relevant data are crucial to inform policy and decision-making in public health emergencies and to improve long-term public health outcomes for Canadians. The Government uses data to inform policies, to make evidence-based decisions, and to provide quality services to Canadians. Data is created and used in every government domain from fisheries and farming to border control and immigration, as well as broad applications in research and statistical analyses such as epidemiological studies and modelling. While data is crucial for decision-making in all domains of government, the Government also recognizes the need to protect it. The Government will codify the need to take steps to ensure contractors provide appropriate privacy protections around the information involved in the contract. The Government puts trust and privacy at the center of the transition to a more digital government that will improve service delivery to Canadians.

Some of the data that the Government uses is about individuals and falls within the definition of personal information as defined in section 3 of the *Privacy Act*. Because a purely consent-based privacy model is not feasible in the public sector, the Government requires that personal information must be directly related to an operating program or activity before it is collected, which puts an onus of responsibility onto the Government to manage this personal information with strict adherence to law and policy. There are opportunities for improvement as the Committee has highlighted, such as improving the consent and opting-out framework for those initiatives where consent is possible, and the Government is actively working on strengthening the legislative frameworks for personal information protection.

Currently, the Government has strong frameworks in place to ensure any collection, transmission and use of personal information and data is appropriate. This includes policy requirements to assess privacy risk prior to beginning a new, or substantially modifying, a program. The Government leverages risk-based audit strategies and will continue to do so to ensure those frameworks are effective in protecting privacy.

Complementing the public-sector framework for personal information protection, Bill C-27 and the *Consumer Privacy Protection Act* (CPPA) would replace the private-sector privacy law PIPEDA with a modernized privacy law that includes a framework for use of personal information that has been de-identified, in certain circumstances, with appropriate protections. By complying with this framework, organizations would be able to use de-identified information without an individual's knowledge or consent

for internal research, analysis and development, or to voluntarily disclose it without consent at the request of government institutions that have the legal authority to obtain the information or for socially beneficial purposes. Organizations would have to ensure that technical and administrative controls are proportionate and would not be able to use de-identified information to identify and individual.

In addition to de-identified information, Bill C-27 proposes to define anonymization, and specifically carves it out of the scope of the CPPA. This is intended to provide some clarity around how information can be managed or disposed of once it is outside the protection of privacy law. The *Artificial Intelligence and Data Act* (AIDA) also proposes to require the adoption of standards related to anonymized data for the development of Artificial Intelligence (AI).

Under TBS policy, government institutions are required to notify the OPC about new or substantially modified personal information collection and acquisition programs, notably as part of the formal privacy impact assessment process. Throughout the pandemic and despite the fact that the use of de-identified and aggregate mobility data did not engage the *Privacy Act*, PHAC had weekly, and later bi-weekly meetings with the OPC to keep them apprised of all pandemic initiatives, and to answer the OPC's questions. While insightful, consulting the OPC on all data collections and acquisitions, even when the data has been de-identified, and continuing throughout the program may impede the efficient delivery of government services. Therefore, notification is only required for new or substantially modified programs that involve personal information.

The OPC plays an important oversight role in the federal government privacy framework as an arm's length champion of the privacy rights of Canadians. When it comes to information that has been de-identified to such an extent that an individual can no longer reasonably be identified from the information, engagement with the OPC may be appropriate in some circumstances. However, in light of the Commissioner's role and mandate, the degree of consultation with the OPC should be aligned with how identifiable individuals can be from a data set, if at all. It is important to ensure that the de-identification methods used are adequate to provide the appropriate standard of privacy protection. Statistics Canada is key in supporting government institutions and the OPC with expert advice on statistical standards, methods and procedures.

In today's digital world, individuals expect efficient, effective, and streamlined programs and services. To rise to those expectations, the Government is working to facilitate the sharing of information between institutions and de-identifying or anonymizing information is one tool the Government can use. The Government is working on legislative and policy updates to ensure that the appropriate privacy protections and processes, as well as sound information management, data stewardship, and transparency practices, are in place.

The Government's Digital Charter outlines what Canadians can expect from the Government in relation to the digital landscape. The 10 principles set out in the Charter provide the framework for continued Canadian leadership in the digital and data-driven economy. This principled approach will not only protect Canadians' privacy and personal data but also leverage Canada's unique talents and strengths in order to harness the power of digital and data transformation. The Digital Charter is one example of a public education initiative to inform Canadians about how the Government handles their data.

Legislative Reform
(Pertaining to recommendations 3, 7, 8, 9, 10, 11, 12, 13, 14, 17, 18, and 19)

Summary of recommendations:

- Add explicit transparency requirements to the *Privacy Act.*
- Amend the *Privacy Act* and the PIPEDA to include definitions of 'legitimate commercial interest' and 'public good' in the handling of personal data and that the OPC be given the power to investigate breaches of the ethical guidelines.
- Amend federal privacy legislation to render it applicable to the collection, use and disclosure of de-identified and aggregated data.
- Add a standard for de-identification to federal privacy legislation or the ability for the Privacy Commissioner to certify a code of practice for de-identification.
- Add a prohibition on re-identification of de-identified data to federal privacy legislation.
- Give the Privacy Commissioner the authority to proactively audit the practices of third-party mobile data providers to ensure compliance with PIPEDA when the data is to be used by a federal institution.
- Amend the *Privacy Act* and the PIPEDA to regulate the activities of private companies in the handling of mobility data and that the Government ensure private companies have obtained meaningful consent from their customers to collect that data.
- Strengthen the powers of the OPC with order-making powers and the ability to impose penalties under both the *Privacy Act* and the PIPEDA.
- Amend the PIPEDA to require that service providers display a message offering the user the option to opt-out of data collection, to continue using the service without accepting the terms and conditions, or to decline all terms and conditions and cookies.
- Add a public education and research mandate to the *Privacy Act.*
- Amend the *Privacy Act* to include necessity and proportionality criteria for the use, collection and disclosure of personal information.
- Add a privacy by design standard to federal privacy legislation.

The Government acknowledges the recommendations and has committed to reform of the *Privacy Act* and the PIPEDA. The introduction of Bill C-27 in June 2022 is an important first step in meeting these commitments. As evidenced by the introduction of Bill C-27 and consultations on reform of the *Privacy Act,* reforms are intended to incorporate Canadians' modern expectations of privacy in the digital age, to ensure interoperability with the data protection laws at home and with our international partners, and to support innovation through responsible uses of information and data in both the private and public sectors. The reforms to both privacy laws are intended to recognize that data about individuals is essential to businesses and to providing efficient and effective government services. Updated privacy laws will also entrench the importance of educating and informing the public about privacy-related topics and will include explicit transparency requirements.

Privacy Act

The Government of Canada recognizes that the *Privacy Act* needs to be modernized. Canadians' expectations of privacy have changed since the Act became law nearly four decades ago, as have their expectations of how their government serves and protects them. My colleague Minister Lametti is currently leading a thorough review of the *Privacy Act.*

Substantial policy development and engagement work has taken place in support of this initiative. In its discussion paper entitled *Respect, Accountability, Adaptability: A discussion paper on the modernization of the Privacy Act*, JUS proposed a number of potential changes to the *Privacy Act* which align with issues raised by the Committee's recommendations. This paper was published in support of public consultation from November 2020 to February 2021. Many of these proposals speak to the recommendations made by the Committee, including:

- limiting the collection of personal information to that which is reasonably required for a federal public body's functions, with proportionality being a key consideration;
- recognizing the need for a framework under the Act regarding de-identified information, including defining what de-identified information is and is not;
- requiring federal public bodies, in the early stages of the development and implementation of an initiative, program or activity, to embed privacy protections, thereby entrenching what is already an obligation under government policy (to require institutions to design with privacy in mind);
- creating a specific offence for re-identifying personal information that has been de-identified; and,
- providing the Privacy Commissioner with greater powers, including the power to audit the personal information practices of federal public bodies, to enter into binding compliance agreements with federal public bodies and to issue orders similar to those issued by the Information Commissioner.

Many of these proposals received positive feedback, including from the Privacy Commissioner of Canada. My colleague Minister Lametti's December 2021 mandate letter commits to building on these previous engagement efforts and continuing the substantive review of the *Privacy Act*. The views of stakeholders and partners, including those of this Committee, the Privacy Commissioner, data experts and Indigenous partners, will be taken into account in the development of proposals to bring the *Privacy Act* into the 21st century.

Private Sector Privacy Legislation

In the years since the PIPEDA came into force in 2004, technology, information and its role regarding privacy and the economy have evolved significantly. In an effort to address this changing environment, the Government launched the Digital Charter in 2019 as blueprint for digital transformation of the economy. A key pillar of the Digital Charter was the modernization of Canada's private sector privacy law, the PIPEDA.

To this end, on June 16, 2022, Bill C-27, the *Digital Charter Implementation Act*, 2022, was introduced in the House of Commons. Among the pieces of legislation proposed under Bill C-27 is the CPPA, which builds on reforms to the PIPEDA in the previous Parliament under former Bill C-11, *Digital Charter Implementation Act, 2020*. The CPPA reflects the extensive consultations undertaken, as well as stakeholder input and Privacy Commissioner recommendations on the former Bill C-11. It proposes, among other things, provisions to substantially reform privacy protections found in the PIPEDA. Furthermore, it would address new challenges posed by a data-driven, digital, and global economy by enhancing control for Canadians, enabling responsible data innovation and strengthening oversight and enforcement. Bill C-27 also introduces AIDA which proposes to regulate AI systems in order to promote responsible development and deployment, including the adoption of measures related to anonymized data in that context. Furthermore, AIDA would criminalize the use of unlawfully obtained data for AI development as well as the deployment of AI systems in a manner that is reckless, fraudulent, or deliberately seeks to cause harm.

If passed, the CPPA would address many of the points raised by this Committee's recommendations. The Act proposes a comprehensive framework for privacy protection. In particular, the CPPA would codify the following:

- A new exception to consent covering specified business activities that an individual would reasonably expect in the circumstances. It would also permit organizations to collect or use personal information under the rubric of "legitimate interests," provided the business has assessed and mitigated the risks to the individual; and makes these assessments available to the OPC upon request.

- Additional exceptions to consent relating to socially beneficial activities that would permit organizations to disclose personal information that has been de-identified to public institutions to enable participation in initiatives led by the public sector that support the public good.
- A framework for use of personal information that has been de-identified in certain circumstances with appropriate protections. Unauthorized re-identification would be prohibited by the CPPA.
- The OPC would be able to approve a particular code of practice as a means of complying with a part or all of the CPPA.
- A broad audit power where the Privacy Commissioner could conduct an audit if they believe that Part 1 of the CPPA has been, is being, or is likely to be contravened. Additionally, the Privacy Commissioner would continue to have the power to initiate an investigation if they have reasonable grounds.
- A new right for individuals to request that their personal information be transferred to another organization in accordance with data mobility requirements specified in regulations. The CPPA provides for the regulations that would establish technical and procedural mechanisms for the secure and practicable transfer of personal information between organizations.
- A series of new order making powers for the Privacy Commissioner. The CPPA would empower the Privacy Commissioner to compel respondents to comply with the Act, to cease activities that violate the CPPA, to enter into compliance agreements with respondents that are binding and to recommend administrative monetary penalties for specific contraventions.
- A clear set of provisions that require organizations to stop collecting, using, or disclosing personal information if an individual notifies an organization that they withdraw their consent. Individuals would be able to withdraw their consent in relation to some or all of the personal information being handled by the organization.
- A requirement for organizations to put in place policies, procedures and practices to give effect to requirements under the law.

Of note, under current privacy laws, neither of the terms "de-identified," nor "anonymized" are defined and are used in a variety of contexts with different meanings. This has led to confusion regarding how they apply in the context of privacy protections and law. Bill C-27 proposes that "de-identify" would mean "to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains." Various privacy protections would continue to apply to such data, given the risks of re-identification. Meanwhile, "anonymize" would mean "to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means." Privacy protections would not apply to such data as it would no longer be considered personal information. Similar definitions may be proposed in a modernized *Privacy Act* to create a seamless code

between the private and public sectors, where possible. Were these definitions in place at the outset of the Mobility Data Program, the privacy obligations may have been clearer to the public.

I wish to thank the Committee and stakeholders once again on completing the Report and issuing the thoughtful and timely recommendations. The Government is committed to protecting the privacy of Canadians as is demonstrated by the solid legislative and policy framework already in place. The Government is equally committed to building on that solid foundation to improve transparency, derive value from the data it holds, and modernize the legislation and policies with the ultimate end of protecting personal information and personal data in a trustworthy and respectful manner.

Yours sincerely,

The Honourable Mona Fortier, P.C., M.P.