President
of the Treasury Board

Présidente
du Conseil du Trésor

Ottawa, Canada K1A 0R5

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

Dear Mr. Brassard,

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 seventh report of the Standing Committee on Access to Information, Privacy and Ethics (the Committee), entitled "Device Investigation Tools Used by the Royal Canadian Mounted Police (RCMP) And Related Issues" (the Report), tabled in the House of Commons on November 23, 2022.

I wish to sincerely thank the members of the Committee for their time reviewing the use of On Device Investigative Tools (ODITs) by the RCMP and providing thoughtful suggestions and recommendations regarding their use. I am grateful as well to the witnesses who appeared before the Committee to express their views and provide advice.

As new technologies emerge, the tools needed to identify and monitor criminal activities also need to evolve. The use of ODITs help law enforcement overcome the challenges posed by encryption used by criminals to avoid police detection. The Government recognizes that the protection of privacy is crucial. Hence, it is a priority for the Government to ensure that all its activities support transparency and are conducive to promoting public trust.

Given the potential intrusiveness of ODITs, their use by law enforcement is subject to strict measures to ensure they are used responsibly. Judicial authorization is sought and granted for investigations of listed serious offences under the *Criminal Code* when it can be demonstrated that less intrusive options were explored first.

The Government is actively working on modernizing the *Privacy Act*. Several of the proposals currently under consideration would address concerns identified in the report. For example, the Government is considering elevating to legislation the requirement to conduct Privacy Impact Assessments and granting new powers to the Privacy Commissioner to ensure that they are able to exercise their mandate effectively. The Government has also introduced Bill C-27, the *Digital Charter Implementation Act*, which would modernize the federal private sector privacy framework through the enactment of the *Consumer Privacy Protection Act*.

In addition, the RCMP has established the National Technology Onboarding Program to implement an internal, centralized system to identify, assess, and track new and emerging investigative tools and technologies before they are made operational.

The Government has carefully considered the Report. The Response, contained herein, addresses the nine recommendations put forward by the Committee. The Response is the product of a collaborative effort among implicated government institutions and their agencies: the Treasury Board of Canada Secretariat, the Department of Justice Canada, Innovation, Science and Economic Development Canada, Public Safety Canada and the RCMP, Global Affairs Canada, and the Privy Council Office.

Recommendation 1: That the Government of Canada amend the *Privacy Act* to include an explicit obligation for government institutions to conduct privacy impact assessments before using high-risk technological tools to collect personal information and to submit them to the Office of the Privacy Commissioner of Canada for assessment.

The Government recognizes the need for establishing a modern, 21st century privacy framework. Indeed, the Department of Justice Canada (JUS) is currently leading a review of the *Privacy Act* with the goal of modernizing it to ensure it meets the requirements of the digital age and the privacy expectations of individuals. Substantial policy development and engagement work has taken place in support of this initiative. In its discussion paper published in November 2020 entitled, *Respect, Accountability, Adaptability: A discussion paper on the modernization of the Privacy Act* (the Discussion Paper), JUS outlines several potential amendments. For instance, the *Privacy Act* could potentially impose an obligation on federal government institutions to conduct PIAs with respect to new programs or activities, or substantially modified programs, that involve the collection, use or disclosure of personal information for administrative purposes, for automated or manual profiling activities, where sensitive personal information is involved, or other activities involving a high risk for personal information as otherwise mandated by government policy. The modernized law could also require federal public bodies that prepare a PIA to provide a copy to the Privacy Commissioner for views and recommendations, which the Privacy Commissioner would have to provide within a mandated timeline.

Currently, under the *Directive on Privacy Impact Assessment*, government institutions are required to conduct a PIA for new or substantially modified programs or activities where the collection of personal information is for an administrative purpose. Additionally, government institutions are required to provide the completed PIA to both the OPC and the Treasury Board of Canada Secretariat (TBS). They are also expected to make public a summary of the PIA unless there are security reasons that would prevent them from doing so. The *Directive* also requires that government institutions provide the completed PIA to TBS in order to ensure that the President of the Treasury Board, as Designated Minister, can discharge their oversight role for several policy areas.

Recommendation 2: That the Government of Canada create a list of banned spyware vendors and establish clear rules on export controls over surveillance technologies.

The Government recognizes the need to have clear rules to ensure control over surveillance technology. Rules currently exist with respect to items controlled on Canada's Export Control List, including for surveillance technology. All permit applications for the export of controlled items are reviewed on a case-by-case basis under Canada's robust risk assessment framework, including against the *Arms Trade Treaty* criteria that are enshrined in Canada's *Export and Import Permits Act* (EIPA). Under the EIPA, controlled goods and technology will not be exported from Canada where there is a substantial risk that they could be used to commit or to facilitate serious violations of international humanitarian law, international human rights law, or serious acts of gender-based violence or violence against women and children, amongst other criteria. Subject matter experts assess export permit applications against each of the mandatory criteria, as well as to ensure consistency with Canada's laws and regulations, international obligations, foreign and defence policies, as well as security interests.

Canada has also joined the Export Controls and Human Rights Initiative launched at the December 10, 2021, Summit for Democracy and is working with like-minded countries to develop a voluntary written Code of Conduct intended to guide the application of human rights criteria to export licensing policy and practice.

Recommendation 3: That the Government of Canada review Part VI of the *Criminal Code* to ensure that it is fit for the digital age.

The Government continues to enhance the ability of the law to keep pace with technological change by, for example, drafting legislation that creates or amends laws, including the *Criminal Code*, to be technology neutral. This means, for example, avoiding using terminology tied to a particular technology, and using more general concepts that will be less vulnerable to being quickly outdated. In

the *Criminal Code* specifically, a framework for the lawful use of certain investigative techniques for the purpose of criminal investigations is established, ensuring their use is limited and constrained to minimize privacy intrusions and respect the *Canadian Charter of Rights and Freedoms* (*Charter*). The Government is receptive to further potential reforms to be identified through ongoing review. The Government is conscious such reforms may be required to ensure the law keeps pace with technology and continues to be effective in providing for appropriate judicial oversight and protections for privacy in the context of the lawful use of investigative techniques such as ODITs.

Part VI of the *Criminal Code* establishes a comprehensive regime to govern the use of the investigative technique of intercepting private communications. Part VI only permits the use of this technique if its stringent conditions are met. There are different authorities in Part VI for different situations, and there are some exceptional authorities, for example to address emergency situations. Conditions set out in Part VI can apply to: limit its use to the investigations of specified offences; require prior judicial authorization; require that interception is clearly the only remaining investigative option (i.e., that other investigative procedures have been tried and failed or that it appears they are unlikely to succeed, or that given the urgency of the matter it would be impractical to carry out the investigation of the offence using only other investigative procedures); require specific and focused collection; and to impose strict time limitations. Part VI also imposes requirements for notifications to the person who was the object of the interception, and for the publication of annual reports. The regime in Part VI has been repeatedly upheld by Canadian courts as being consistent with the requirements of the *Charter,* including section 8 which provides protection against unreasonable search and seizure. The use of ODITs would need to meet the stringent requirements of Part VI, and criminal investigators may also need additional specific authorities from the courts, such as general warrants, to ensure that all the activities contemplated by law enforcement in deploying ODITs are receiving appropriate judicial scrutiny prior to their use. In addition to the requirements set out in Part VI and other parts of the *Criminal Code* for specific thresholds to be met prior to use of investigative techniques, there are also criminal offences that apply to protect people from privacy intrusions, for example through interception of private communications or computer hacking, such as the offence of intercepting private communications in s.184(1), and the offences of unauthorized use of computers (s.342.1), mischief in relation to data (s.430(1.1)) and possession of devices (which includes computer viruses) to obtain unauthorized use of computers or commit mischief (s.342.2).

The Government remains committed to ensuring that our laws continue to keep pace with modern technology to ensure that they are fit for the digital age, while acknowledging that given the pace of technology, this is a challenge. This will be done while respecting privacy as protected under the *Charter*.

Recommendation 4: That the Government of Canada amend the preamble to the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* to indicate that privacy is a fundamental right.

The Government recognizes the fundamental importance of protecting individuals' personal information and, hence, its ongoing efforts to modernize the federal privacy framework. In its Discussion Paper, JUS explores several potential changes in a modernized *Privacy Act*, including updating the purpose clause. A modernized purpose clause could provide better guidance for interpretation by clearly stating the important underlying objectives of federal public sector privacy legislation. Such objectives could include the protection of individuals' human dignity, personal autonomy, and self-determination; enhancing public trust and confidence in government; and promoting effective and accountable public governance.

Regarding the private sector privacy framework, the Government agrees with the Committee that the protection of privacy is crucial to ensure individuals can exercise their fundamental rights and freedoms. That is why the Government introduced Bill C-27, the *Digital Charter Implementation Act, 2022*. The bill would replace the current private sector privacy law, the *Personal Information Protection and Electronic Documents Act*, with a modernized law entitled, the *Consumer Privacy Protection Act* (CPPA). The bill would also introduce the *Personal Information and Data Protection Tribunal Act*, which would establish an administrative tribunal to hear appeals of certain decisions made by the Privacy Commissioner under the CPPA and to impose penalties for the contravention of certain provisions of that Act.

The CPPA's purpose clause explicitly recognizes individuals' right of privacy with respect to their personal information and reforms under the new law will ensure individuals have greater control of their privacy. Further, the preamble to Bill C-27 explicitly affirms that the protection of privacy rights is important for ensuring that individuals can exercise individual autonomy and dignity, and fully enjoy other fundamental rights and freedoms.

This legislation represents a significant step forward to deliver on the Government's commitment to ensure confidence in the digital marketplace and to create the conditions for responsible innovation. The CPPA would significantly increase the powers for the OPC to oversee and enforce the law; thereby creating a strong incentive for organizations to engage in practices that respect individuals' privacy rights.

Recommendation 5: That the Government of Canada regularly remind former elected or appointed members or any individuals who have previously worked for a national security agency of their lifetime obligations under the *Security of Information Act* and obtain acknowledgment of their understanding of these obligations.

The Government takes the security of its information, facilities and assets seriously and agrees with the spirit of this recommendation, which is captured in the *Security of Information Act* (SoIA) and given precision via the Government's *Operational Standard* for the SoIA. As per the Standard, when an individual "permanently bound to secrecy" ceases to be employed with a department or agency, they are required to undergo an exit interview conducted by a security official, or an equivalent appropriate security exit procedure and formal sign off. In addition, individuals shall be reminded of their ongoing obligations under the SoIA and the consequences of any violations. The exit interview and formal sign-off reinforce the consequences of failure to comply with their obligations under this law.

Additionally, the Government provides a security briefing to newly appointed Cabinet members, including a high-level summary of the Ministerial Security Reference Book (MSRB) which is designed to support Ministers over the course of their mandate. The MSRB outlines a range of security measures that exist to protect people, information, facilities and assets in Canada and around the world. Governor-in-Council appointees also receive security briefings from their respective departments.

Recommendation 6: That the Government of Canada grant the Office of the Privacy Commissioner of Canada the power to make recommendations and issue orders in both the public and private sectors when it finds violations of the laws for which it is responsible.

The Government respects the important oversight role of the Privacy Commissioner. At present, the *Privacy Act* empowers the Privacy Commissioner with broad investigative powers, including the power to issue reports of findings containing any recommendations that the Commissioner considers appropriate, and proposed actions to be taken by government institutions.

Regarding possible amendments to the *Privacy Act*, in its Discussion Paper, JUS explores several potential changes that would strengthen the Act's oversight regime. For instance, a modernized Act could provide the Privacy Commissioner with greater powers, including the power to audit the personal information practices of federal public bodies, to enter into binding agreements with federal public bodies and to issue orders similar to those issued by the Information Commissioner.

Existing TBS policy instruments create opportunities for engagement between government institutions and the OPC to discuss the potential privacy risks associated with a program or activity and to develop appropriate mitigation measures based on the OPC's recommendations. Current government policy requires institutions to notify the Privacy Commissioner of any initiatives that could relate to the *Privacy Act* or to any of its provisions, or that may have an impact on the privacy of individuals. This notification allows the Commissioner to be seized with any upcoming initiatives where there may be an impact on privacy. Similarly, the PIA process provides an opportunity for government institutions to engage with the OPC to help appropriately identify and mitigate privacy risks at the onset of a program or activity.

Regarding the private sector privacy framework, the Government agrees with the Committee on the need to strengthen the enforcement and oversight role of the Privacy Commissioner. The proposed CPPA would empower the Privacy Commissioner with authority to order non-compliant organizations to take any action or cease any action that would be required to bring them into compliance. Under the CPPA, the Privacy Commissioner would also be able to recommend penalties for contraventions of key provisions of the law. A new Personal Information and Data Protection Tribunal would be authorized to levy penalties and would serve as a recourse mechanism for individuals and organizations affected by OPC actions. Maximum penalties under the CPPA would be among the highest of any privacy law in the world and the Privacy Commissioner would continue to provide guidance and recommendations to organizations to ensure that their activities comply with the law.

Recommendation 7: That the Government of Canada amend the *Privacy Act* to include the concept of privacy by design and an obligation for government institutions subject to the Act to meet this standard when developing and using new technologies.

The Government recognizes the importance of identifying privacy risks at the onset of a program or activity and developing appropriate mitigation measures to lessen these risks. Undertaking a PIA in the early stages of a program or activity, in consultation with departmental privacy officials as well as TBS and OPC, is an important measure to ensure privacy risks are identified and appropriately managed. Elevating the requirement to conduct a PIA to legislation, as considered in an updated *Privacy Act*, would help ensure programs and activities are designed with privacy in mind.

Regarding potential amendments to the *Privacy Act*, JUS's previously mentioned Discussion Paper explores several potential changes that would strengthen the Act's accountability regime. For instance, a modernized Act could bring into the law the concept of "privacy by design," which would require that government institutions integrate considerations of how to protect personal information into the early stages of the development and implementation of an initiative, such as a new program or service offered by a

government institution.

Recommendation 8: That the Government of Canada establish an independent advisory body composed of relevant stakeholders from the legal community, government, police and national security, civil society, and relevant regulatory bodies, like the Office of the Privacy Commissioner of Canada, to review new technologies used by law enforcement and to establish national standards for their use.

The Government believes in the importance of ensuring appropriate oversight of government programs and activities, including those related to law enforcement. There has been substantial work by the RCMP in recent years to create an advisory body to review its new technologies and propose national standards for their use. The RCMP has established the National Technology Onboarding Program (NTOP) to implement an internal, centralized system to identify, assess, and track new and emerging investigative tools and technologies before they are made operational. NTOP's assessment process evaluates the privacy, legal, ethical, Gender-based Analysis Plus and security considerations of new technologies to ensure compliance with RCMP policies, as well as Canadian legislation and standards. The RCMP is supportive of regular engagement with the OPC, the National Security Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians to ensure relevant oversight bodies are actively informed as to which new technologies are being contemplated and how they will be used. Additionally, the RCMP is exploring how to advance proactive disclosure to the public of the types of tools and technologies that have been assessed by NTOP and policies related to those technologies.

Furthermore, NTOP has proposed the development of a new working group that would comprise members from policing agencies across the country, with the objective of standardizing the NTOP assessment process across all levels of Canadian law enforcement. The RCMP has engaged in preliminary discussions with its partners and has received positive feedback on the proposal.

Recommendation 9: That the Government of Canada amend the *Privacy Act* to include explicit transparency requirements for government institutions, except where confidentiality is necessary to protect the methods used by law enforcement authorities and ensure the integrity of their investigations.

The Government commits to continuing to work toward increasing public transparency. At present, the *Privacy Act* requires government institutions to, among other things, collect personal information directly from the individual to whom it relates and to inform this individual of the purpose of the collection, where appropriate. It also requires the creation and publication of personal information banks, accessible to every person. In addition, the Act provides any individual with a right to request access to his or her personal information, and

request that corrections be made to that information.

Regarding potential amendments to the *Privacy Act*, JUS explores several potential changes in its Discussion Paper that would modernize the transparency practices of government institutions. These include a possible obligation for government institutions to publish online key information on their activities involving personal information, in an accessible and searchable personal information registry. A modernized Act could also impose new proactive publication requirements, including as they relate to information-sharing agreements. This framework could account for necessary exceptions, where the publication of sensitive operational information would be inappropriate, such as in respect of law enforcement investigations, intelligence gathering and national security activities.

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 individuals 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, promote privacy by design and modernize legislation and policies with the ultimate end of protecting personal information in a trustworthy and respectful manner.

Sincerely,

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