Minister of Innovation, Science and Industry
Ministre de l'Innovation, des Sciences et de l'Industrie
Ottawa, Canada K1A 0H5

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

john.brassard@parl.gc.ca

Dear Mr. Brassard:

I am pleased to provide you with a copy, in both official languages, of the Government Response to the recommendations of the Standing Committee on Access to Information, Privacy and Ethics (the Committee) contained within the report entitled: *Facial Recognition Technology and the Growing Power of Artificial Intelligence*.

The Government expresses its appreciation to the members of the Committee for their dedication and valuable work in examining and providing suggestions and recommendations to improve the federal legislative frameworks and policies that apply to facial recognition technology (FRT) and artificial intelligence (AI).

The Government also extends its gratitude to the many witnesses, including representatives of law enforcement, advocacy groups, experts, the Privacy Commissioner, and others who appeared before the Committee. The Committee's analysis, supported by the witnesses' insights, provides an informed perspective and will help shape the future policy towards FRT and AI in Canada.

Given the rise in the use of FRT and AI, as well as the many potential applications of these technologies, it is important that federal legislative frameworks and policies remain fit-for-purpose with respect to providing effective protections for personal information, transparency, and supporting trust in Government and the marketplace. Ensuring the responsible deployment and use of new data and digital technologies is one of the priorities of the Government.

That is why the Government has introduced Bill C-27, the *Digital Charter Implementation Act, 2022* (DCIA). The DCIA would modernize the federal private sector privacy framework through the enactment of a new *Consumer Privacy Protection Act* (CPPA) and would create an entirely new framework for the regulation of AI entitled the *Artificial Intelligence and Data Act* (AIDA). The DCIA

…2

also enacts the *Personal Information and Data Protection Tribunal Act*, which establishes 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. This legislation represents a significant step forward to deliver the Government's commitment to ensure confidence in the digital marketplace and create the conditions for responsible innovation.

To that end, please find below the Government's Response to the Committee's recommendations. The Response is the product of a collaborative effort among implicated federal departments, and agencies including the Department of National Defence; Justice Canada; Public Safety Canada and its portfolio agencies; Innovation, Science and Economic Development Canada; the Treasury Board of Canada Secretariat (TBS); and Transport Canada.

Recommendation 1: That the Government of Canada amend section 4 of the *Privacy Act* to require a government institution to ensure that the practices of any third party from which it obtains personal information are lawful.

The Government acknowledges the importance of ensuring *Privacy Act* requirements are respected when collecting personal information. The *Privacy Act* governs federal government institutions' collection, use, disclosure, and retention of personal information, including in connection with the use of FRT. Each Government institution is responsible for ensuring its activities involving personal information comply with the *Privacy Act*. In addition, the Policy on Privacy Protection, the Directive on Privacy Practice, and the *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions* set specific requirements on government institutions, including when employing third party providers and/or suppliers for the collection, use, retention, and disclosure of personal information. Contracts, agreements, or arrangements established with third parties should also clearly outline measures to protect personal information, including a requirement to immediately notify the federal institution of a privacy breach.

With regard to the Committee's recommendation to amend the *Privacy Act*, we would note that Justice Canada is currently reviewing the *Privacy Act* with a view to assessing proposals for its modernization. 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 (the Discussion Paper) Justice Canada outlines several potential amendments, including a strengthened framework for the collection of personal information and stronger accountability mechanisms.

The views of stakeholders including those of this Committee, will be taken into account in the continued development of proposals to bring the *Privacy Act* into the 21st century.

Recommendation 2: That the Government of Canada ensure that airports and industries publicly disclose the use of FRT including with, but not limited to, signage prominently displayed in the observation area and on the travel.gc.ca website.

The Government of Canada agrees with the recommendation. As part of its effort to ensure transparency in the use of FRT at airports, Transport Canada will continue to work with industry partners to ensure their use of FRT is publicly disclosed through appropriate signage in departure areas/any other area in the airport environment where this technology is deployed. Transport Canada and Global Affairs Canada will also continue to work together to communicate the use of FRT for air travel purposes on the travel.gc.ca website, where appropriate.

The Committee may also note that the Treasury Board Directive on Automated Decision-Making includes notice requirements that could potentially apply to automation projects deployed to support or make decisions impacting the movement of people and goods across Canadian borders. This is because the directive requires federal departments to notify clients that the service they are seeking is automated. According to the directive, notices should be provided through all relevant service delivery channels, whether online or in-person. Notices for high-impact systems should include information about the system and its role in the decision-making process. Finally, federal departments that deploy FRT at airports to make or inform decisions impacting legal rights and interests may be obliged to notify travellers via signage placed at appropriate locations in Canadian airports, digital notifications (e.g., at kiosks, on departmental websites), and/or other relevant channels.

With regard to industry, the proposed AIDA would require that persons responsible for high-impact AI systems publish relevant information about such systems. This includes publication of a plain-language description of how the AI system is used, the type of predictions it makes, and the mitigation measures it has established.

Recommendation 3: That the Government of Canada refer the use of FRT in military or intelligence operations, or when other uses of FRT by the state have national security implications, to the National Security and Intelligence Committee of Parliamentarians (NSICOP) for study, review, and recommendation; and that the Committee report its findings.

The Government would welcome, in a manner and with a scope consistent with the National Security and Intelligence Committee of Parliamentarians' (NSICOP) legislation, a study of the framework for the use of facial recognition technologies, should they deem it appropriate.

By way of background, the NSICOP was established in 2017 to provide a forum for parliamentarians to review and examine the classified activities of Canada's national security and intelligence agencies. Under its legislation, the NSICOP has a mandate to review national security and intelligence activities, as well as the legislative, regulatory, policy, administrative, and financial frameworks for national security and intelligence. NSICOP members review this information in camera, but release regular public reports on their activities, findings, and recommendations to inform the public and contribute to accountability. Ministers of the Crown may refer matters relating to national security or intelligence to the NSICOP for their review. The decision to undertake a review is made by the members of NSICOP.

Recommendation 4: That the Government, in the creation of its regulatory framework around the use of FRT, set out clear penalties for violations by police.

The Government acknowledges the recommendation. While the Government recognizes the importance of strong oversight and accountability, it would note that the majority of law enforcement and policing agencies in Canada are provincial and municipal police forces, whose governance frameworks are primarily established through laws enacted under provincial jurisdiction. With respect to federal law enforcement institutions, the Government is considering this issue more broadly in the context of proposals for amendments to modernize the *Privacy Act,* as part of its review by Justice Canada. While this review is ongoing, the Committee may be interested to hear that among the proposals being considered is an enhanced compliance framework that includes updated enforcement mechanisms and enhanced powers for the Office of the Privacy Commissioner (OPC), mandatory privacy impact assessments (PIAs), and stronger transparency and accountability requirements.

Recommendation 5: That the Government of Canada amend its procurement policies to require government institutions that acquire FRT or other algorithmic tools, including free trials, to make that acquisition public, subject to national security concerns.

The Government acknowledges the recommendation. The *Access to Information Act* already requires federal institutions to proactively disclose information on contracts over $10,000, which is available to the public at

…5

open.canada.ca. Subject to any national security concerns, if a contract were to

acquire FRT or other algorithmic tools, these contracts, if over $10,000, would be part of this disclosure. At this time, there are no plans to require publication of contracts with values below that threshold.

Where free trials are engaged in but are single-use or where there is no intention to use on an ongoing basis then they are a known as “non-durable” assets and there is no acquisition to report. However, if after the free trial the Government decided to buy the asset, then this acquisition would be reported if it is over $10,000, subject to any national security issues.

Recommendation 6: That the Government of Canada create a public AI registry in which all algorithmic tools used by any entity operating in Canada are listed, subject to national security concerns

The Government acknowledges the recommendation. While there is no policy or law in place to create a public AI registry, the Government may consider it under the proposed new regulatory framework for AI under AIDA. AIDA would require that persons responsible for each part of the lifecycle of high-impact AI systems adopt measures to mitigate risks of harm and biased output. It would also require such persons to publish relevant information about such systems. In this context, the Government will take the Committee’s recommendation under advisement and consider further whether a public registry for high-impact AI systems may be worthwhile.

With regard to the use of AI by Government institutions, the Committee may wish to note that the Treasury Board Directive on Automated Decision-Making requires the completion and publication of an Algorithmic Impact Assessment (AIA) for new automated decision systems used in service delivery in the federal public service. The AIAs are published on the Open Government Portal and collectively form an inventory of automated decision systems deployed by institutions subject to the directive. Furthermore, this work is ongoing and TBS will continue to work with federal partners and external stakeholders to explore potential approaches to expanding the scope of AI projects disclosed to the public.

Recommendation 7: That the Government of Canada enhance the Treasury Board Directive on Automated Decision-Making to ensure the participation of civil society groups in AIAs and to impose more specific requirements for the ongoing monitoring of AI systems

The Government agrees with the recommendation. While the AIA already asks federal departments whether they have undertaken consultations with external stakeholders, including civil society organizations, TBS plans to publish guidance encouraging departments to consult external stakeholders during the development of an AIA.

…6

In addition, the Government of Canada has outlined a set of Digital Standards,

which form the foundation for the Government's shift to becoming more open, agile, and user-focused. One of these Digital Standards is "Design with users" under which federal departments are advised to research and understand user needs when designing their programs. In the case of automation projects, departments can leverage the expertise and networks of civil society organizations to understand the needs of potentially impacted individuals or communities. External stakeholders could also inform the development of an AIA and execution of an automation project by contributing to peer reviews. Such a role would support departments in carrying out their mandate responsibly, as they are obliged to have moderate and high-impact projects undergo a peer review.

The Treasury Board Directive on Automated Decision-Making also requires federal departments to monitor their automated decision systems on a scheduled basis. This is intended to ensure that the outcomes of automated decisions are consistent with applicable policy and legislation, including on human rights. The directive also includes requirements for reporting on a system's effectiveness and efficiency; this ensures that departments continuously collect data on the ability of a system to advance program goals. TBS will develop guidelines to support the implementation of these requirements, including by identifying best practices during key phases of a system's lifecycle and facilitating public reporting on system performance.

Recommendation 8: That the Government of Canada increase its investment in initiatives to study the impact of AI on various demographic groups, increase digital literacy, and educate Canadians about their privacy rights.

The Government agrees in principle with this recommendation and notes that it has already been taking steps that will result in the promotion of initiatives to further study the impact of AI. In particular, under the proposed AIDA, the Minister of Innovation, Science and Industry, supported by a proposed new AI and Data Commissioner, would have a mandate to engage in education and research activities. These are expected to include activities studying the impacts of AI through an intersectional lens. Some of the research conducted under funding from the Pan-Canadian AI Strategy also concerns these issues. These initiatives, taken together, seek to ensure that development and deployment of AI is done responsibly, particularly to prevent discriminations and biases that often target marginalized demographic groups.

In addition, the Committee may wish to note that one pillar of the OPC's mandate is to promote public awareness and understanding of privacy matters and the rights that Canadians enjoy under privacy law. To this end, the OPC regularly

…7

prepares and disseminates public education materials, including tools and information it develops to help educators and parents engage children about privacy. Under Bill C-27, the Government has also proposed to reform the federal private sector privacy framework through the enactment of a new CPPA. The CPPA would preserve this part of the OPC's mandate, ensuring that the Privacy Commissioner can continue to promote the public's awareness and understanding of emerging privacy issues, such as the impacts of FRT. The Committee may also wish to acknowledge the work of the Global Partnership on AI (GPAI) and the Minister's Advisory Committee, notably the Public Awareness Working Group as part of an important part of our AI literacy and education effort.

Finally, the Government is also considering this issue in the context of the ongoing review of the *Privacy Act*. For example, one proposal under consideration is to provide the Privacy Commissioner with the authority to engage in public education. This policy proposal is also included in the Discussion Paper.

Recommendation 9: That the Government of Canada ensure the full and transparent disclosure of racial, age, or other unconscious biases that may exist in FRT used by the Government, as soon as the bias is found in the context of testing scenarios or live applications of the technology, subject to national security concerns.

The Government acknowledges the importance of the Committee's recommendation as well as the principle that technologies used by Government should not contribute to or perpetuate unconscious biases. The Committee should note that the Directive on Automated Decision-Making does require federal institutions to test data used by automated decision systems for unintended bias before they are launched. The directive also requires that institutions monitor active systems on a scheduled basis in order to guard against discrimination in decision-making and other unintentional outcomes that may compromise an automation project's compliance with applicable laws and policies. Automated decision systems are broadly defined and could include FRT, considering that they are deployed to carry out or support tasks that typically involve human judgment.

While the directive does not require institutions to disclose the results of bias testing *per se*, the AIA prompts institutions to consider publishing information about their bias testing processes and related frameworks, methods, guidelines, and tools. The directive also includes a reporting requirement whereby institutions are expected to publish information about the effectiveness and efficiency of their systems. This could include data about different aspects of system performance in service delivery, including accuracy.

The *Privacy Act* also requires institutions to take all reasonable steps to ensure that personal information used for an administrative purpose is as accurate, up-to-date, and complete as possible. The Directive on Privacy Practices expands on the Act's accuracy obligations to also require institutions to document the source or technique used to validate the accuracy of the personal information and identify these in the description of the relevant Personal Information Bank. The directive also requires that individuals be given the opportunity, whenever possible, to correct inaccurate personal information before any decision is made that could have an impact on them.

Recommendation 10: That the Government of Canada establish robust policy measures within the public sector for the use of FRT which could include immediate and advance public notice and public comment, consultation with marginalized groups, and independent oversight mechanisms.

The Government agrees with the Committee on the importance of having comprehensive and robust policy instruments in place to help guide the use of any emerging technology with heightened privacy and other legal risks, including FRT, and has taken steps to ensure that the current policy instruments remain both robust and effective. In particular, the Treasury Board Directive on Automated Decision-Making establishes guardrails for the use of automated decision systems in service delivery. The requirements of the directive could potentially apply to uses of FRT in administrative decision-making. The directive requires federal departments to notify clients that the service they are seeking is automated. The policy instrument also includes quality assurance measures such as mandatory legal consultation, bias testing, and human oversight for high-impact systems. The AIA also prompts departments to undertake consultations with various external stakeholders, which could include marginalized groups. TBS is obliged to periodically review the directive. Future reviews of the instrument could explore the prospect of introducing measures that specifically seek to regulate the use of FRT.

The Directive on Privacy Impact Assessment requires federal institutions to conduct a PIA when the collection of personal information is for an administrative use, which would include the use of biometric information by FRT as part of a decision-making process. Federal institutions are required to provide the PIA to both TBS and the OPC and 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 Government also recognizes the sensitivity of biometric information used by FRT, as this type of personal information is unique to each individual and cannot be changed. Existing requirements under the *Privacy Act* and related policy instruments continue to apply to biometric information collected and handled in the context of a program or activity leveraging FRT.

…9

Recommendation 11: That the Government define in appropriate legislation acceptable uses of FRT or other algorithmic technologies and prohibit other uses, including mass surveillance.

The Government acknowledges the Committee's recommendation and is working through Bill C-27 to define acceptable uses of AI systems. Under the proposed AIDA, the Government could make regulations defining the criteria for high-impact AI systems. These are the systems that have the most significant impacts on Canadians. Other regulatory powers would be used to ensure that such systems, when developed or deployed in the context of international trade and commerce, are appropriately assessed for risks of harm and bias throughout the lifecycle. If it is determined that a high impact AI system could cause harm or biased output, the Minister of Innovation, Science and Industry may request to examine records, order an audit, impose measures in response to an audit (including the publication of the remedy), impose administrative monetary penalties (AMPs), and issue a cessation order. Furthermore, in serious cases, unlawful use of an AI system can even be enforced under criminal law. It is important to note that AIDA is concerned with regulating only high-impact AI systems.

The Committee should also note that privacy laws, including the federal *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), are technologically neutral in their nature and apply to the collection, use, and disclosure in all regulated contexts and regardless of the specific technology in play. The same is true of the proposed new CPPA which would replace PIPEDA with the passage of Bill C-27. In this respect, privacy laws already govern the collection, use, and disclosure of personal information through FRT. Maintaining technological neutrality in these legal frameworks is important to ensure they have the flexibility to protect privacy in the face of rapidly changing technologies.

Recommendation 12: That the Government of Canada amend the *Privacy Act* to require that prior to the adoption, creation, or use of FRT, government agencies seek the advice and recommendations of the Privacy Commissioner, and file impact assessments with his or her office.

The Government acknowledges the Committee's recommendation about the importance of Government agencies seeking the timely advice of the Privacy Commissioner and filing impact assessments. The Committee may wish to note that the TBS's Directive on Privacy Impact Assessment, which enshrines the requirement for conducting a PIA for new or substantially modified programs or activities, already provides an opportunity for federal institutions to engage with the OPC to help appropriately identify and mitigate the privacy risks of their programs and activities. Additionally, federal institutions can engage their

…10

departments' privacy officials, often located within their Access to Information and Privacy office, to seek privacy advice and recommendations on their specific use of FRT or similar technology. The Directive also requires that federal institutions provide the completed PIA to TBS, in order to ensure that the President, as Designated Minister, can discharge their oversight role for several areas of policy, including the Directive on Automated Decision-Making.

The TBS Policy on Privacy Protection also requires institutions to notify the Privacy Commissioner of any planned initiatives that could relate to the Act or to any of its provisions, or that may have an impact on the privacy of Canadians. As set out in TBS Policy, this notification permits the Commissioner to review and discuss the issues involved.

With regard to potential amendments to the *Privacy Act*, as mentioned above, the Government recognizes the importance of a modern privacy regime which respects contemporary expectations of privacy, which is why Justice Canada 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 Canadians. The Committee may wish to note that in its Discussion Paper, Justice Canada explores several potential changes, including elevating to legislation the requirement to undertake a Privacy Impact Assessment and requiring a copy be provided to the Privacy Commissioner.

Recommendation 13: That the Government of Canada update the *Canadian Human Rights Act* (CHRA) to ensure that it applies to discrimination caused by the use of FRT and other AI technologies.

The Government agrees with the Committee about the importance of preventing discrimination caused by the use of FRT or AI. In this respect, the Committee may wish to note that the CHRA already applies to the use of FRT and AI in the context of federally regulated employment and provision of goods, services, facilities, and accommodation. Clarifications of CHRA application are achieved when appropriate or necessary by policies and guidelines of the Canadian Human Rights Commission and decisions of the Canadian Human Rights Tribunal and the courts.

The Government also recognizes that policy tools other than complaints-based ones such as the CHRA are helpful to address the potential risks of these technologies. For example, the Treasury Board Directive on Automated Decision-Making requires federal departments to develop processes to test data and information used by automated decision systems for unintended data biases and other factors that may unfairly impact outcomes. It also requires departments to develop processes to monitor outcomes on a scheduled basis to safeguard against unintentional outcomes and to verify compliance with applicable policy

…11

and legislation. This is one example of a measure that, in combination with the complaints-based mechanism of the CHRA, serves to address the risks of discrimination posed by these technologies in the public sector.

In recognition of the increasing importance of the use of AI in the private sector in terms of impacts on human rights, the Government has proposed the *AIDA*. AIDA would require that persons responsible for each part of the lifecycle of high-impact AI systems adopt measures to mitigate risks of harm and biased output. The definition of biased output in AIDA is aligned with the prohibited grounds in the CHRA in order to ensure that AI systems with highest potential impacts on Canadians are proactively assessed for potential discriminatory results from the earliest stages of their development. Proactive assessment and mitigation are critical in addressing systemic bias due to the use of AI systems, as those affected would in many cases not be aware of the bias.

Recommendation 14: That the Government of Canada implement the right to erasure ("right to be forgotten") by requiring service providers, social media platforms, and other online entities operating in Canada to delete all users' personal information after a set period following users' termination of use, including but not limited to uploaded photographs, payment information, address and contact information, posts, and survey entries.

The Government agrees with the Committee on the need for the law to provide Canadians with greater control over their personal information, including the ability to dispose of information for which there is no legitimate purpose for an organization to continue to handle. That is why the proposed CPPA would provide an explicit right for individuals to request that organizations dispose of their information, subject to legal or reasonable contractual restrictions, as well as to a limited number of other exceptions (for example, to protect the information of other individuals, or where there is a preservation demand from police or a preservation order from the courts under the *Criminal Code of Canada*). In addition to strengthening the right to disposal, the CPPA would strengthen the general rules around how long organizations are allowed to retain personal information. Organizations that contravene the rules around the right to disposal or the retention of personal information could be subject to AMPs.

Recommendation 15: That the Government of Canada implement an opt-in-only requirement for the collection of biometric information by private sector entities and prohibit such entities from making the provision of goods or services contingent on providing biometric information.

The Government agrees with the Committee that Canadians should wield a high level of control over their most sensitive personal information, including biometric data. Greater individual control is one of the key objectives for the proposed

…12

CPPA, and one of the ways that the new law would achieve this is through stronger and clearer rules around consent.

Under the CPPA, organizations will need to request consent in plain language that an individual can understand and provide the clear ability for the individual to say “yes” or “no.” The law would also explicitly prohibit organizations from, as a condition of a product or service, requiring an individual to consent to the handling of information beyond what is necessary to provide that product or service. Organizations will also need to take the sensitivity of personal information into account in assessing whether they are handling information for appropriate purposes, and in determining whether to rely on implied or express consent to handle personal information. The guidance and findings of the OPC under the current law have emphasized that biometric information is a particularly sensitive form of personal information, and the Government expects that similar guidance would apply under the new law.

Finally, it is important to note that, under the CPPA, organizations that fail to obtain valid consent or that require consent beyond what is necessary to provide a product service could be subject to penalties.

Recommendation 16: That the Government of Canada strengthen the ability of the Privacy Commissioner to levy meaningful penalties on government institutions and private entities whose use of FRT violates the *Privacy Act* or the PIPEDA to deter future abuse of the technology.

The Government agrees with the importance of considering privacy protections in the early stages of development and implementation of initiatives or activities. In support of this, as set out in its Discussion Paper, Justice Canada is considering policy proposals for a modernized *Privacy Act* to create a legal obligation for federal public bodies to undertake 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 to identify and mitigate privacy risks, and to provide a copy of PIAs to the OPC.

With regard to the private sector privacy framework, the Government agrees with the Committee on the need to strengthen the enforcement and oversight role of the OPC. That is why the 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. The Commissioner would also be able to recommend penalties for contraventions of key provisions of the new law. A new Personal Information and Data Protection Tribunal would

…13

be authorized to levy the penalties, and would serve as a recourse mechanism for individuals and organizations affected by OPC actions. Penalties under the CPPA could be as high as 3% of global turnover or $10 million—whichever is higher.

This regime responds to longstanding calls from the OPC and stakeholders to strengthen the enforcement of the law and would align Canadian law with leading jurisdictions such as the European Union. Given the potential impact of AMPs on companies' bottom line, this will provide a significant incentive to ensure that their practices are in compliance with the law.

Recommendation 17: That the Government of Canada amend the *Privacy Act* and the PIPEDA to prohibit the practice of capturing images of Canadians from the Internet or public spaces for the purpose of populating FRT databases or AI algorithms.

The Government acknowledges the Committee's recommendation. As a technologically neutral Act, policy proposals envision a modernized *Privacy Act* that would not prohibit specific technologies; rather it would provide a strong legal framework to regulate the Government's treatment of personal information, including in connection with the use of new and emerging technologies. That being said, in the review of the Act, Justice Canada is exploring proposals for a modernized Act that could add specialized rules for using or sharing "publicly available" personal information. In addition, Justice proposals for a modernized *Privacy Act* contemplate changes to rules for collecting personal information.

The Government agrees with the Committee that the private sector privacy law should include strong protections to ensure organizations do not collect sensitive information in a manner that runs counter to Canadians' expectations. In this regard, it is important to note that the proposed CPPA would continue the current law's approach to strictly limiting the meaning of "publicly available information" that an organization can handle without an individual's consent. These rules have been central to recent OPC investigations that found the collection of biometric information to be offside the current law, including the Clearview AI case.

While the CPPA would contain new exceptions to consent covering business activities, these exceptions may only be used where an individual would reasonably expect the collection or use. At the same time, the law would also require organizations to handle information for appropriate purposes, even if an organization is relying on exception to consent. Taken together, these rules will provide robust protections against activities where organizations might deploy emerging technologies in a manner that runs counter to Canadians' privacy expectations.

…14

Recommendation 18: That the Government of Canada impose a federal moratorium on the use of FRT by (federal) policing services and Canadian industries unless implemented in confirmed consultation with the Office of the Privacy Commissioner or through judicial authorization; that the Government actively develop a regulatory framework concerning uses, prohibitions, oversight, and privacy of FRT; and that the oversight should include proactive engagement measures, program level authorization, or advance notification before use, and powers to audit and make orders.

The Government acknowledges the Committee's recommendation for a moratorium on the use of FRT by federal policing services. *The Privacy Act* already governs federal institutions' collection, use, and disclosure of personal information, including those that might flow from the use of FRT. The Government has committed to modernizing the *Privacy Act* to ensure it keeps pace with the digital age. In connection with this initiative, Justice is considering a number of policy proposals that align with the Committee's recommendation, including proposals for a modernized *Privacy Act* to require federal public bodies to undertake 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 to identify and mitigate privacy risks, and to provide a copy of PIAs to the OPC. In addition, policy considerations involve enhancing the powers of the OPC, including the power to audit the personal information practices of federal public bodies, and to enter into binding compliance agreements with federal public bodies.

The Government also acknowledges the Committee's recommendation for a moratorium on the use of FRT by Canadian industries. It is important that organizations be accountable for their handling of personal information and apply strong privacy protections. A strength of the current law, which would also be true of the proposed CPPA, is that it is technology-neutral: this ensures that the law remains relevant, and does not constrain innovation, in the face of rapidly changing technology and business practices. Of note, the CPPA would strengthen the existing overarching "appropriate purposes" obligation in PIPEDA: the law would prescribe the factors organizations must take into account to ensure that their purposes for handling personal information, and the manner in which they handle the information, are appropriate. The existing provision has already provided the OPC with the basis for issuing guidance on "no-go zones" (purposes that it considers to be categorically offside the law). It has also been central to recent OPC findings, including in the case involving Clearview AI. Under the CPPA, the "appropriate purposes" provision would be more robust, as would the powers for the OPC to enforce the law. In particular, the OPC would

have the authority to issue binding orders to non-compliant organizations, and could, for example, order organizations to cease handling personal information for purposes that are offside the “appropriate purposes” requirement.

Recommendation 19: That the federal government ensure that appropriate privacy protections are put in place to mitigate risks to individuals, including measures addressing accuracy, retention, and transparency in facial recognition initiatives as well as a comprehensive strategy around informed consent by Canadians for the use of their private information.

The Government acknowledges the need for the private sector privacy law to enhance privacy protections to individuals, including with respect to accuracy, retention, transparency, and individual consent and control. These principles are central to the current law and they would be carried over and strengthened by the proposed CPPA. As noted earlier, the new law would strengthen and clarify the rules around consent and would heighten organizations’ obligations with respect to the retention and disposal of personal information, to ensure that this information is not held indefinitely.

In addition the CPPA would contain a number provisions to increase the transparency of organizations’ information handling practices. In particular, the CPPA would introduce new requirements for organizations to make information available about how they use automated decision-making systems to make significant decisions. Individuals would also have the right to request that organizations provide them with an explanation of the predictions, recommendations, or decisions made by such a system. These rules could apply in the context of the use of FRT.

The *Privacy Act* currently requires federal institutions to take all reasonable steps to ensure that personal information used for any administrative purpose is as accurate, up-to-date, and complete as possible. Additionally, all personal information must be retained for a minimum of two years if used for an administrative purpose, as set out in the *Privacy Regulations*. The *Privacy Act* also sets out a requirement to inform individuals from whom the institution collects personal information of the purposes for which personal information is being collected (subject to certain exceptions). This requirement is elaborated on in the TBS Directive on Privacy Practices. Canadians benefit from the independent oversight of the OPC, whose role includes investigating complaints filled with their office. While the *Privacy Act* and *Regulations* set out requirements relating to accuracy and retention of personal information, Justice is considering proposals to modernize these aspects. In addition, proposals contemplate new openness and transparency requirements to enhance individuals’ ability to obtain specific information about a federal public body’s policies and practices with respect to the management of personal information.

…16

The Treasury Board Directive on Automated Decision-Making establishes measures for ensuring that data collected and used by automated decision systems is tested for unintentional bias and assessed for quality criteria. Where the use of FRT is subject to the directive, these measures could help ensure that the system is trained on representative data and that the client data it processes is relevant, accurate, and up to date. Finally, TBS is seeking to strengthen the directive's quality assurance measures. As part of the third review of the directive, measures to ensure that both data inputs and outputs are traced, protected, and retained and disposed of appropriately have been proposed.

On behalf of the Government, I would like to express my appreciation for the efforts of the Members of the Committee and its staff in preparing the Report, which I believe will provide guidance as we continue to work to ensure our federal legislative frameworks remain up to date and responsive to new technology.

Sincerely,

The Honourable François-Philippe Champagne, P.C., M.P.

Attachment