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

VIA ELECTRONIC MAIL

September 23, 2021

Hillary Hartley
Chief Digital and Data Officer, Deputy Minister
Ontario Digital Service
digital.government@ontario.ca

Dear Deputy Minister Hartley:

RE: IPC Response to the Ontario government's public consultation on a "Policy framework for Ontario's digital identity program"

On behalf of the Office of the Information and Privacy Commissioner of Ontario (IPC), thank you for the opportunity to comment on the Ontario government's consultation on a Policy framework for Ontario's digital identity program.

Attached are my office's comments in response to the themes addressed in the consultation.

In the interest of transparency, we will be making this submission available on our website.

Sincerely,

Patricia Kosseim
Commissioner

IPC Comments on the Government’s Policy Framework for Ontario’s Digital Identity Program

September 2021

INTRODUCTION

The Office of the Information and Privacy Commissioner of Ontario (IPC) is pleased to respond to the government’s public consultation on a policy framework for Ontario’s digital identity (ID) program.

The proposals for an Ontario digital ID program are still quite general. The IPC looks forward to consulting with the government on more specific proposals that describe in detail how information would flow in the system and the roles and responsibilities of the various stakeholders involved. In the meantime, we are pleased to provide our comments organized around the three themes raised in the consultation:

1. Protecting Ontarians’ privacy and security
2. Governance and following expert advice
3. Ensuring equity and inclusion of all Ontarians

The following comments are made with the expectation that the government’s digital ID program will be subject to Ontario’s privacy laws and oversight by the IPC.

The IPC is an independent office of the Legislative Assembly of Ontario, protecting and promoting the privacy and access rights of Ontarians. Provincial access and privacy laws establish rules for how Ontario’s public institutions — such as provincial ministries and agencies, municipalities, police services, universities and schools, child and family service providers, and health care providers — may collect, use, and disclose personal information. These laws also provide the public with a right of access to government-held information and/or access to their own personal information.

OVERVIEW OF ONTARIO DIGITAL ID PROGRAM

The soon-to-be launched digital ID is described as “a new form of secure, electronic government-issued ID that, over time, will offer convenient online and in-person access to public and private sector services, while protecting data privacy.”

Development of an Ontario digital ID is a signature project in the government’s *Ontario Onwards: Ontario’s COVID-19 Action Plan for a People-Focused Government*. The government has committed to introducing a digital ID by the end of 2021 — an ambitious timeline.

The government is considering several potential uses for an Ontario digital ID. For example, individuals will be able to use the Ontario digital ID to prove identity when:

- making an age-sensitive purchase (like purchasing alcohol or a lottery ticket)
- picking up a package at the post office
- checking in for virtual medical appointments
- applying for government assistance or benefits
- accessing and sharing vaccination records
- getting a birth, marriage or death certificate
- opening a bank account (private sector use)

Businesses will also have digital IDs and could use them to:

- hire new employees
- prove business identity/credentials or verify those of other businesses
- open business accounts
- apply for loans, grants or tax credits
- verify customers' identity

The stated benefits of an Ontario digital ID program include easier access to products and services that require people to show identification, and greater control by individuals over what personal information is shared. An Ontario digital ID program could also help accelerate economic recovery and growth — particularly during and post pandemic — as new ways of service delivery move permanently online. Most interestingly, a digital ID program that is designed and governed appropriately may actually help enhance security and privacy features, and mitigate the risks associated with the current proof of identification process that involves having to carry, show, or send online copies of existing physical identification cards.

The Ontario government's digital ID program is a significant initiative that could over time have far-reaching impacts on government service delivery. By sheer virtue of its scope, scale, and complexity, it will also have significant effects for the privacy and access rights of Ontarians. Overall, we commend the government on its stated commitments to individual privacy, security, and personal control, and encourage them to take a privacy-first approach when designing and putting the program into place.

Theme 1: Protecting Ontarians' privacy and security

One of the key takeaways from phase two of the government's consultation on digital ID is that privacy and security are critical drivers to encourage public trust and confidence, and ultimately, ensure the success of the program. While the government is aware of the expectations of individuals and small and medium-sized businesses, and understands the need to protect privacy and security of personal information, the specific details of the program require careful consideration. The IPC encourages open and ongoing dialogue to work out these details.

At this time, however, our focus is on addressing the questions posed by government in its consultation paper:

1. To ensure a safe and secure digital ID what privacy and security protections, not already embedded in current laws, should be considered to safeguard personal information and minimize fraud or identity theft?
2. What measures should the program take to enhance the privacy and security of a digital ID?

An Ontario digital ID requires a clear and comprehensive statutory privacy framework, with robust and effective oversight. Currently, there are significant gaps that require legislative attention and action before the launch of a digital ID program.

Provide for express lawful authority, prohibitions, penalties, and redress

The legal authorities to create and administer digital IDs should be clearly set out in legislation and related regulations. Prohibitions and penalties for misuse of the system by all stakeholders involved in the digital ID ecosystem, including government, public institutions, service providers, and businesses, should be clear, meaningful, and effective. It should be obvious from the law and from related policy instruments what their respective roles are and who is accountable for what. This includes who is responsible if, and when, something goes wrong. Individuals must be able to challenge inappropriate collection, use, and disclosure of their digital ID, as well as its accuracy, and be able to seek correction and assistance in resolving these issues.

All aspects of the government’s program and activities related to digital ID — both in terms of its privacy and access obligations — should form part of a robust governance regime and continue to be subject to independent oversight and enforcement by the IPC.

Strengthen existing privacy laws to support digital governance

The digital ID program is part of a broader strategy to improve digital governance and services. When introducing any new legal authorizations necessary for moving that agenda forward, the IPC strongly recommends the government also strengthen the corresponding protections in the province’s existing privacy and access laws. To secure and maintain public trust, key amendments are needed to modernize the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) and its municipal counterpart, the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*). In their current form, these laws are missing critical protections needed to support the privacy, security, and transparency aspects of a successful digital ID program, particularly in respect to basic accountability principles.

For example:

- Our office has long called for mandatory privacy impact assessments (PIA) for all new or substantially changed programs and activities that pose a certain level of risk, and for a requirement to publish summaries of those PIAs in the interest of public transparency and accountability.
- A mandatory requirement to notify affected individuals and the IPC of data breaches above a certain threshold — a mainstay of most modern privacy regimes — is noticeably absent from Ontario’s public sector laws and should be added.

- The IPC currently lacks power to make an order directing public institutions to perform a duty, correct, amend, or cease certain privacy management practices. This is a power any modern privacy regulator must have —and be able to use when needed — to hold governments to account for their actions.
- The application of these laws should be expanded to cover any public sector organization that receives a significant amount of operating funds from the government, delivers a program designed to support government objectives, or in respect of which the Ontario government plays a significant role in their policy development and operational directions.

Address gaps in private sector privacy protection

Based on the uses currently under consideration, it appears that the government intends for private sector organizations in Ontario to use the digital ID. The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), a federal law, currently governs private sector organizations, including small and medium-sized businesses in Ontario. There are significant gaps in this law, such as the lack of order-making powers by the federal privacy commissioner and effective enforcement measures, including meaningful administrative penalties to ensure compliance.

Even with a major overhaul of the scope and scale contemplated in a recently tabled federal bill (that died on the order paper with the recent election), federal privacy law reform will not — and constitutionally *cannot* — extend to all private sector transactions within the province that will make use of Ontarians' digital ID. For example, the privacy of employees or prospective employees of provincially regulated businesses, and the non-commercial activities of not-for-profit organizations, charities, unions, professional associations, and provincial political parties are currently not covered by any private sector privacy law. The IPC has responded positively to the government's proposal to create a made-in-Ontario private sector privacy law with a detailed submission. We strongly urge the government to connect the important dots between these parallel consultations that require a coordinated and coherent approach to ensuring seamless privacy protections for Ontarians across different sectors.

In addition to the broader statutory initiatives needed to design a stronger, more comprehensive, and better-integrated privacy and security regime around all the various components of Ontario's digital ID ecosystem, below are some of the high level principles and values we believe should govern the operational design and implementation of such a program.

The continuing value of anonymity

A digital ID should not be required as identification for information or services that could be feasibly offered to individuals on an anonymous basis. The Supreme Court of Canada has recognized anonymity as an element of informational privacy. We should continue to protect and uphold this value in a free and democratic society, in both public and private spaces. People should not be asked for identification when it is not necessary for a transaction. Systems should not be designed in a way that ends up making identification mandatory if another design, just as effective in achieving the stated purpose, does not require people to identify themselves.

Data minimization

The government's communications suggest that digital ID would disclose only the information that is required for a transaction. There should be clear rules governing when an Ontario digital ID may be accepted for a specific use case and what minimal personal information is necessary for that use. For example, an alcohol purchase requires only the information that a person is over 19 years of age — not their actual date of birth and address, which are visible on a physical driver's licence. The IPC supports work towards this goal of minimizing the collection of personal information by government and businesses. This feature will depend upon the government's specific use cases as well as the design and functionality of the digital wallet. We look forward to reviewing additional details of both as the government rolls out its program.

User-centric approach

We understand that the digital ID will be entirely optional for Ontarians and will coexist with existing physical cards such as driver's licences. The current proposal is that digital IDs will be stored and managed in smartphone digital wallets for both online and offline uses.

This decentralized, "self-sovereign" identity trust model mentioned in the technology and standards is promising because it puts the individual in control of their digital ID and does not require a central database or involvement of the issuing government when used. This type of digital ID can only be accessed with the informed consent of the individual and at their will. In principle, the IPC supports a user-centric approach based on individual choice and looks forward to learning additional details.

No tracking

The government has stated its commitment not to store digital IDs in a central database and not to use the digital ID system as a way to track individuals' activities and whereabouts. We understand this commitment to mean no tracking when an individual's "interaction triggers a request to the verifiable data registry to retrieve the Ontario government's public key, which confirms that the holder's presented credential is accurate and hasn't been tampered with". This is consistent with the user-centric approach. That said, in the course of providing a service, the details of many transactions with government or private sector organizations could still be otherwise recorded. How such data may be recorded, aggregated, and analyzed to track individuals over time and across multiple contexts, and to profile them, remains a concern for the IPC. For these reasons, the IPC recommends that the identification verification purposes of the digital ID program be clearly defined and that strong limits be placed on the collection, retention, and use of identifiers associated with users' network access, mobile device and wallet software.

If artificial intelligence (AI) capabilities are being contemplated to help manage the digital ID program, then additional privacy guardrails would be needed. The application of AI technologies, including automated processing, to predict and influence user behavior and make significant decisions about them and their eligibility to access certain programs or services, raises significant risks that must be prevented or mitigated accordingly. The IPC recently outlined some of these risks in its submission to the government's consultation on developing a trustworthy artificial intelligence framework for Ontario. The IPC strongly encourages government to see this initiative through, and to finalize, codify, and enforce the overarching values and principles of its trustworthy framework that will ensure the responsible use of artificial intelligence by Ontario's public institutions in a manner that is transparent, accountable, fair, safe, and rights-based.

Theme 2: Governance and following expert advice

1. How can the program continue to benefit from expert advice as it grows? What is the best way for the public, industry and other interested stakeholders to provide ongoing input into the program's governance?
2. What best practices from other jurisdictions would help inform the governance structure of digital identity in Ontario?

We commend the government for reaching out to Ontarians and asking these fundamental questions early on in the design, conception, and development phases of the program. Again, the IPC welcomes the opportunity to consult on the more specific privacy aspects and technical security safeguards of Ontario's digital ID program as the proposal progresses. We look forward to continuing to engage in an ongoing dialogue with government and other stakeholders at key stages of program development. Practical tools such as privacy impact assessments and data flow maps would be particularly useful in grounding discussions at a more practical and operational level.

That said we fully acknowledge and understand that many issues fall outside of our office's jurisdiction. For example, interoperability with other data protection regimes and regulators in Canada and around the world will be critical to enabling public-private partnerships and the smooth workings of a global economy. We also recognize that digital ID raises human rights issues beyond privacy and that other stakeholders, such as human rights commissions and community advocates, must also be at the table to bring their perspectives to the discussion and ensure related issues are examined from all angles.

Ultimately, as major pieces of the program start coming together, we will be urging the government to be completely open and transparent with Ontarians about the defined purposes of the digital ID program, what personal information will be used, how, and by whom. These details must be clear, readily accessible, explained in plain language and presented in a user-friendly manner for audiences with no special or expert knowledge. This is critical to building the trust needed to sustain the success of Ontario's digital ID program. The IPC stands ready to provide guidance on this and other aspects of the program.

Other jurisdictions have tried, and in some instances failed, to fully leverage the benefits of their digital ID programs and achieve their intended goals for a variety of reasons. We encourage the government to continually scan and keep abreast of these international developments and draw lessons from the experiences of others — both the good and bad.

The IPC understands that the Ontario digital ID program will continue to evolve, and that emerging technology standards in other Canadian and international jurisdictions may present new choices and opportunities. We recommend the Ontario government follow the path of other jurisdictions by establishing one or more independent consultative bodies to provide multiple perspectives and interdisciplinary advice.

Theme 3: Ensuring equity and inclusion of all Ontarians

1. How can the program ensure it is inclusive and equitable so all Ontarians have access to a digital ID?
2. What standards and practices does the program need to follow to advance access and equity?

Inclusive enrolment

The key to an inclusive digital ID system is ensuring that as many people as possible can participate. This means that the enrolment process must be accessible to all — not only adult, literate, tech-savvy, able-bodied, official-language speakers who are in good mental health, have a fixed address and the time and resources to access a new system. Inclusive enrolment will necessarily involve addressing all the potential barriers to enrolment whether they are economic, social, physical, or administrative.

Special attention should be paid to enrolment of persons who may not already have adequate government-issued identification, or whose identification is not issued by a Canadian jurisdiction.

Earning and maintaining trust

Lack of trust can be an invisible barrier to enrolment in a digital ID. There are many reasons for lack of trust in an identification scheme. These range from poor design, to misinformation, to distrust of Canadian governments by communities who have been subject to colonial policies, to negative experiences of immigrants and refugees with state systems abroad. We recommend the government make earning and maintaining public trust in digital ID systems its major focus. Building strong privacy and transparency elements into the scheme, and then explaining these in a simple way should be the priority. The IPC further recommends specific consultations with representative groups and organizations to learn about any concerns and barriers that may have unplanned impacts on marginalized communities and decrease people’s willingness to enrol.

Social inclusion of those who do not enrol

Despite best efforts, it seems clear that some Ontarians will choose not to enrol in digital ID. The government has said that digital ID would be voluntary. To be truly inclusive, services will need to have ways of verifying identity that do not require enrolment in the digital ID for people who choose not to enroll. While identification may be less convenient for these individuals, their choice should not prevent them from being able to access government services and information.

Inclusion and protection of children

Children may sometimes require digital ID. This may challenge many of the built-in assumptions about the system. In the case of young children, concepts of consent and autonomy may be attenuated. Often parents or guardians provide children’s identification when seeking services on their behalf. For this reason, including mechanisms for designating and recognizing substitute decision-makers, should be considered carefully when designing the enrolment and authentication system.

Preventing fraud without adding bias

The government should carefully consider how to prevent ID theft and the growth of an illegal marketplace for fake digital ID creation or use. Yet, great care should be taken when designing automated audit and risk-management programs designed to identify, detect, and prevent fraud, to ensure these do not act in a biased way that could reinforce existing patterns of disadvantage.

CONCLUSION

Some form of digital ID will likely be needed as the foundation for a move towards digital service delivery that will assist Ontario in its economic recovery efforts post-pandemic, and position the province as a world leader in digital innovation. The IPC applauds the government’s commitments to work towards minimizing data collection, and developing a decentralized model of storing and using digital IDs that puts control in the hands of the individual and only for the transactions which are needed. The overall effect of digital ID on the value of anonymity and on vulnerable populations will need to be carefully managed.

The IPC looks forward to consulting with government on the more specific privacy aspects and technical security safeguards of the digital ID program as they become available through tools such as data flow maps and PIAs.

The IPC is ready to provide advice on the type of modern statutory regime needed to strengthen privacy protections in line with new levels of risk introduced by digital IDs; ensure effective accountability throughout the entire digital ID ecosystem; and ensure comprehensive regulatory compliance and enforcement in respect of all the actors involved.