



MODERNIZING THE PRIVACY ACT



Written By

Rajrupa Saha

Josh Skeen

Zainab Raza

Andre De Biasi

Edited & Designed by:

Jevin Mathew

Anjelica Ramsewak

@engagefdn  

general@engagefdn.com 

<https://www.engagefdn.com/> 

INTRODUCTION

The modernization of the Privacy Act presents a significant opportunity to re-evaluate how privacy, accountability, and public trust are protected within Canada's federal institutions. As government services become increasingly digital, the collection, use, disclosure, and analysis of personal information are occurring within a rapidly evolving technological landscape that did not exist when the Privacy Act was first introduced. The Engage Foundation supports efforts to modernize the legislation and believes that reform should be guided by principles of transparency, individual autonomy, responsible governance, and respect for Indigenous rights and data sovereignty. Drawing upon consultation findings, policy research, and emerging best practices, this submission outlines recommendations intended to ensure that Canada's privacy framework remains effective, equitable, and responsive to the realities of the twenty-first century.

Requirement for Meaningful Consent Before Reusing Sensitive Data for New Purposes

Background: The Privacy Act, which came into effect in 1983, was enacted when most information at that time was stored in paper form. At the onset of modern technology and with evolving social and economic changes, the expectation of Canadians of how their personal information is stored, shared and used by more than 250 government agencies has changed as well. The 2024-2025 Public Opinion Research on Privacy Issues shows approximately:

Statistic Result

Canadians Concerned about Privacy	9/10
Concerned about AI using personal information	9/10
Experienced Breach	4/10
Hard to understand Policies	7/10

The federal government often obtains various personal and sensitive information such as health information, biometric information, Immigration or citizenship information, disability-related information, racial identity, financial information, etc. before delivering key services to its citizens. When information is first collected from an individual for the delivery of a particular service, reusing it without clear and specific consent could grant other authorities access to this sensitive information, which the person morally disagrees with, and thus lead to a privacy breach and erode public trust in government. **Any modernization of the Privacy Act must include clear requirements that federal institutions obtain specific and meaningful consent before reusing sensitive data for purposes other than the original purpose for which it was collected.** This reform would strengthen transparency, accountability and public trust while still allowing lawful and necessary information sharing within government.

RECOMMENDATIONS

1. The Privacy Act should be amended to establish a clear statutory requirement that federal institutions must obtain meaningful and specific consent before reusing personal information for any purpose that differs from the original purpose for which it was originally collected. The government of Canada should inform individuals whether their consent would be ongoing or whether separate consent would be collected for each secondary use.
2. Before seeking consent, federal institutions should be required to explain the proposed secondary use in clear and accessible language and assess its potential public impact. The institution should be required to complete a Privacy Impact Assessment (PIA) and should examine the purpose of reuse, the type of information involved, possible risks to individuals and possible information sharing with other institutions or authorities. The PIA would examine whether the proposed secondary use is necessary, proportionate and consistent with the original purpose of collection.
3. The Privacy Act should also clearly specify when consent is not required such as where the secondary use is authorized by law and necessary to deliver a public service.
4. The Privacy Act should further provide individuals with a clearly defined right to opt out of the secondary uses of their personal data where it is not strictly mandated by law, necessary for the delivery of the original service or justifies an overriding of public interests. When an individual opts out and their original service is already completed, federal institutions should be required to retain the relevant information only for a clearly defined period of time. After that period the institution should be required to delete or otherwise dispose of the data As prescribed by law, the Government of Canada can keep it beyond the designated time period only if there remains a legal, administrative security or a public interest needed to preserve it.

5. This opt out mechanism should be clear, accessible and transparent. This would be free from punitive consequences which will ensure that individuals will not be unfairly treated in the delivery of services or put in disadvantaged circumstances for exercising control over their personal data.
6. The Privacy Act should clearly define legal consequences for federal institutions that fail to comply with requirements related to the secondary use of personal information. When personal information is reused without valid consent or without justified public interest, the institution should be subject to enforceable accountability measures such as reviews, mandatory reporting etc. This would strengthen the Privacy Act by ensuring that protection is legally enforceable rather than just a law.
7. The Privacy Act should also be amended to impose explicit obligations to federal institutions to notify affected individuals when a breach occurs. Such a situation should be notified at the earliest possible opportunity. Federal institutions should notify affected individuals directly using the most reliable, accessible and secure methods such as email, letter or secure account message. Public notification can be used when direct notification is not possible or extremely time consuming. The notice should be written in plain and understandable language. It should clearly mention to the individuals what personal information is compromised and what future risk they might face. In addition to that, the government should clearly mention the steps they have taken to protect it and what actions individuals should take to protect themselves.

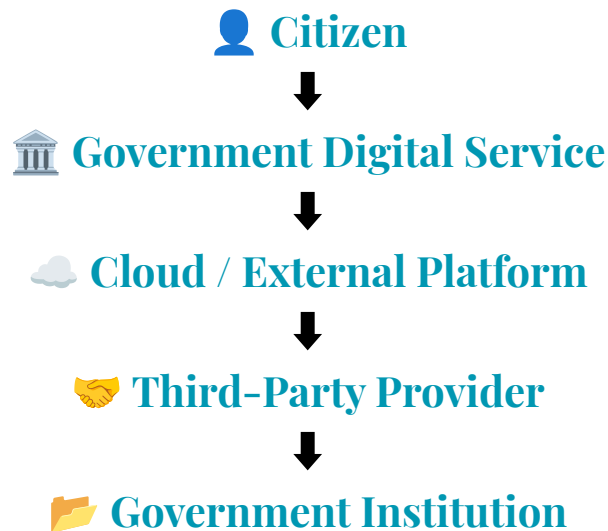
Establishing Clear Online Privacy Protection(s) for Canadians in the Privacy Act

Background: Canada has privacy laws that provide important protections for online personal information particularly through PIPEDA (Personal Information Protection and Electronic Documents Act), the Privacy Act and provincial privacy laws. PIPEDA applies to private-sector organisations engaged in commercial activities and online protections and Privacy Act works on federal institutions. The principal based approach in PIPEDA provides a useful point of comparison for modernizing the Privacy Act. However, the 2024-2025 Public opinion Research on Privacy issues shows that 92% of Canadians show some level of concern that their personal information is shared or sold with other companies and organisations. Canadians often interact with digital systems where the boundary between government, private contractors, cloud service providers, online platforms and automated tools are not obvious. For example, when a person applies online for immigration services, employment insurance, tax benefits, federal employment, grants, security clearance, etc. their personal information may pass through multiple digital platforms. It may be stored in cloud environments, processed by contractors and can be linked to other databases or shared across institutions. In all these cases it is often not clear to the individuals whether their sensitive personal information is being protected or not, creating a gap in public trust. In order to tackle this, **This proposal recommends the government to take action to ensure that privacy protections are consistent across digital ecosystems regardless of whether the information is processed via government institutions or third-party providers.**

92% of Canadians express some level of concern about their personal information being shared or sold to other companies and organizations.



RECOMMENDATIONS



**Personal information may pass through multiple digital systems before a service is delivered.*

1. The Privacy Act should require privacy-protective settings which will be the default for all online federal data collection. Here, privacy-protective settings refer to software configuration that will automatically limit the collection, sharing, and use of your personal data when using online platforms. This unnecessary data sharing, tracking, profiling and reuse of information will not be enabled by default. Privacy-protective settings should be accessible to individuals but controlled and administered under strict institutional accountability. Federal institutions should have limited rules based on administrative access for lawful operational, security, accessibility and compliance purposes. Any change in default settings should be documented, justified and auditable.
2. Federal digital services should be prohibited from using third party trackers, advertisement agencies or other tracking tools if it is not essential for the delivery of services.

3. The Privacy Act should clearly provide that the outsourced platforms, cloud providers, external software vendors, data centres or any third party service providers handling personal information on behalf of federal institutions are subject to the same privacy obligations, limitations, safeguards and consequences established under the Privacy Act. The federal government should be accountable for protection, oversight and legal accountability owed to the individuals. If third party service providers fail to protect private information, do unauthorised disclosure, use data for secondary purposes and fail to report breaches they should be subject to penalty or fines for serious non-compliance. However, fines against third parties should not reduce the accountability of the federal institutions.

Modernizing the Privacy Act Through Indigenous Data Sovereignty

Background: The Privacy Act unfortunately fails to recognize and respect Indigenous peoples' rights to managing their own privacy. The Privacy Act as it stands, fails to validate nor recognize Indigenous data sovereignty effectively. Settler and colonial legacies currently affect and are evident in current data collection practices. Data collection and privacy have traditionally been focused on individual rights, foregoing the considerations for collective knowledge and its value, which are important conventions that inform how Indigenous knowledge is gathered and maintained. The effects of this can lead to misunderstandings in the significance and impact of this data collection when offering services to Indigenous communities, as outsider perspectives and interpretations of the data may create unintended consequences that override Indigenous governance and undermine the integrity of the cultural significance of Indigenous practices that are usually collective, intergenerational, and are fundamental to the identity of Indigenous people. In the absence of these realities, real risks can emerge, through policies and practices based on incomplete and partial understanding of data taken outside of its context, and can in many ways uphold and reinforce structural inequities. **The Government of Canada should seek to create a robust, coherent, and rights-based framework that formally recognizes the sovereignty of Indigenous peoples and their right over their data and personal information, meaningfully reflecting and integrating the work of [its endorsement of the United Nations Declaration of the Rights of Indigenous People \(UNDRIP\)](#).** These reforms are essential in promoting Indigenous self-determination in data governance and improving trust between the federal institutions and our Indigenous communities, reflecting an understood importance of Indigenous rights.

RECOMMENDATIONS

1. The Privacy Act should recognize the authority of First Nations, Inuit, and Métis communities to govern the collection, access, use, and disclosure of their collective information through community-defined protocols.
2. Processes for gathering and maintaining consent are overseen by a Indigenous-led governance bodies to oversee its collection and ownership, and enforced to sustain cultural significance and importance to Indigenous methods of maintaining community and (other) demographic data.
3. The Government of Canada, when looking to collect data from Indigenous communities, must provide a direct and clearly established link to its objectives pertaining to the use and collection of Indigenous knowledge, and denote how this data collection will serve to respect the cultural knowledge and ideas of Indigenous communities.
4. When federal institutions are collecting data based on the access of sensitive Indigenous Traditional Knowledge and practices that conflict with Privacy Act provisions, decision-making over how this collection and use is to proceed is done jointly by Indigenous-led governance bodies and federal institutions.
5. Federal Institutions, when collecting, using, or analyzing data from Indigenous citizens should prioritize CARE principles to help in the research and gathering of Indigenous data collection, prioritizing relationship-building and community standards to minimize harm and misrepresentation.
6. The Privacy Act should be updated to establish protections for Traditional Indigenous Knowledge such as information relating to Indigenous lands, sacred practices, songs, activities, stories, and other forms of Indigenous Traditional Knowledge.

Strengthening Transparency and Accountability in Data Governance

Background: The modernization of the Privacy Act has brought about discussion on what best allows for greater transparency and understanding from Canadians about how exactly privacy is measured, and the greater extent of what is considered to be private information. The Privacy Act, in its original form, was meant to safeguard the physical integrity of data from citizens, but in the decades following its inception, the digital landscape has transformed to where new forms of information have been created, such as artificial intelligence and facial recognition software, a small list of tools that the current landscape of the Privacy Act currently fails to address. Gaps like this expose that it has become unclear what can reasonably qualify as personal data today. Not just that, but government data practices resulting from this shift in modern data collection techniques are not sufficient to help both enshrine citizens' privacy protections but also foster more trust and confidence between citizens and government data collection practices. **The Privacy Act must start operating on more precise definitions that can reflect modern practices but also use foundational principles to help guide public servants on how they ought to manage personal data to ensure accountability is meaningful and not merely a formality.** These following reforms would equip Canadians with greater visibility into how personal information should be defined, collected, and protected, and strengthen confidence in an increasingly complex digital age.

Privacy Act (1983)	Today's Digital Environment
Paper-based records	AI & Facial Recognition
Traditional personal data	Digital, behavioural & inferred data
Limited data processing	Complex digital ecosystems

RECOMMENDATIONS

1. Any collection of private information should require that those tasked with its collection receive mandatory privacy training and review of privacy principles to ensure that private information is consistently known how to be handled, as well as ongoing review and critique of the current iterations of how privacy is administered
2. Information that is collected that contains a clear link to national and foreign interest should include heightened preemptive security measures that limit personal access and implement technological measures such as encryption or the limit of the types of data collection
3. Modernize and clarify the definition of ‘personal information’ to ensure it captures contemporary forms of identifiable information, including digital, behavioural transactional, and inferred data, whilst maintaining sufficient precision to avoid overly broad or overly vague interpretations.
 - a. As part of this modernization, develop statutory criteria that distinguishes ‘personal information’ from operational, administrative, transactional, aggregated, or activity-based information, while ensuring that information capable of reasonably identifying, profiling, or linking an individual remains protected under the Privacy Act.

Building an Adaptive Privacy Framework

Background: Technology evolves much faster than legislation, creating periods where new forms of personal data collection and processing are not adequately regulated. Since the Privacy Act has not required periodic review, it remained largely unchanged for over four decades despite significant developments such as cloud computing, artificial intelligence, biometrics, facial recognition, and automated decision-making. While these technological advancements have created operational benefits, they introduce new privacy risks that could not have been adequately anticipated when the Privacy Act was originally drafted. The absence of regular review mechanisms has created legal and policy gaps, which has reduced the Privacy Act's ability to respond to emerging privacy risks, created uncertainty for federal institutions, and weakened public confidence that privacy protections remain effective in a rapidly changing digital environment. The Privacy Act must remain reflexive, responsive, and able to adapt to technological changes in society before significant harms emerge. Doing so curtails potential waning of public trust that federal privacy measures will remain effective in a rapidly changing digital environment and reduce any potential for legislative obsolescence.

RECOMMENDATIONS

1. The Privacy Act should require a comprehensive parliamentary review every five years concerning the efficacy of the Privacy Act in regulating emerging and evolving practices, technologies, and risks.
2. The Government of Canada should be required to publish a public report after each review outlining proposed amendments and their implications for privacy rights.
3. The Privacy Act should allow the Treasury Board Secretariat and/or the Office of the Privacy Commissioner to issue interim regulatory updates or guidance

Improving Privacy Notice Transparency and Accessibility

Background: Although federal institutions are required to provide privacy notices, the Privacy Act does not establish clear standards for their readability, accessibility, or consistency. As a result, privacy notices often vary significantly in format and content and are frequently written in lengthy, technical legal language that is difficult for the average person to understand. This limits meaningful transparency, as individuals may not fully comprehend what personal information is being collected, why it is required, how long it will be retained, whether providing it is mandatory, or with whom it may be shared. In practice, many individuals simply accept privacy notices without reading or understanding them, undermining the principle of informed consent and reducing public confidence in government data practices. As governments increasingly rely on digital services, artificial intelligence, and automated decision-making, clear and accessible privacy information has become essential for promoting accountability and enabling individuals to make informed decisions about their personal information.

RECOMMENDATIONS

1. Require federal institutions to use standardized, plain-language privacy notices.
2. Clearly explain what information is collected, why it is needed, whether it is mandatory, and with whom it may be shared.
3. Present privacy information in a layered format, with a concise summary and links to detailed legal and technical information.

Current	Recommended
Long and technical	Plain language
Difficult to understand	Easy to understand
Inconsistent formats	Standardized format
One long document	Layered summary with detailed information

Strengthening Privacy Impact Assessment (PIA) Requirements

Background: Privacy Impact Assessments (PIAs) are an important tool that helps federal institutions identify and address privacy risks before introducing new programs, services, or technologies that involve personal information. By assessing how personal information will be collected, used, shared, stored, and protected, PIAs help build privacy protections into projects from the beginning rather than after problems arise. Although federal institutions are required to conduct PIAs under Treasury Board policy, this requirement is not set out in the Privacy Act itself. In practice, PIAs are sometimes completed only after a program has already been launched or are delayed until late in the development process, reducing their ability to prevent privacy risks before they affect individuals. **As governments increasingly use digital services, artificial intelligence, and other data-driven technologies, making PIAs a clear legal requirement would help ensure that privacy is considered early in decision-making and that potential risks are identified and addressed before implementation.**

Privacy Impact Assessment Process

Plan ➤ Conduct PIA ➤ Identify Risks ➤ Implement Program

RECOMMENDATIONS

1. Require all federal institutions to complete a Privacy Impact Assessment before implementing any program, initiative, or technology involving personal information.
2. Empower the Office of the Privacy Commissioner to require corrective measures or recommend delaying implementation where significant privacy risks remain unresolved.
3. Require an interim Privacy Impact Assessment in exceptional circumstances, such as public emergencies, followed by a comprehensive assessment as soon as practicable.
4. Government programs involving the collection of Indigenous data must have mandatory Privacy Impact Assessments (PIAs) for any initiative involving Indigenous data and the collection of knowledge about community members, communities and interests, outlining the identification of cultural risks and an assessment of impacts on community rights and governance

Strengthening Protections for Sensitive Personal Information

Background: Not all personal information presents the same level of privacy risk. Information such as health records, biometric identifiers, financial information, precise geolocation data, Indigenous data, and children's personal information can cause significantly greater harm if it is improperly collected, accessed, disclosed, or misused. However, the current Privacy Act generally applies the same legal protections to all categories of personal information and does not establish enhanced safeguards based on the sensitivity of the data. As government institutions increasingly collect and process large volumes of sensitive information through digital platforms and emerging technologies, a risk-based approach is needed to ensure that stronger protections apply where the potential impact on individuals is greatest. Modern privacy frameworks increasingly recognize that the level of protection should correspond to the sensitivity of the personal information being processed. **A risk-based approach ensures privacy protections are proportional to the potential harms associated with different categories of information, allowing federal institutions to strengthen safeguards and improve accountability in government data practices.**

"Modern privacy frameworks increasingly recognize that the level of protection should correspond to the sensitivity of the personal information being processed."

RECOMMENDATIONS

1. Introduce tiered privacy protections that provide enhanced safeguards for sensitive categories of personal information, including health, biometric, children's, financial, and precise geolocation data, whilst establishing and maintaining separate protections for Indigenous data.
2. Require stricter retention and disposal requirements for high-risk personal information.
3. Mandate enhanced technical and organizational safeguards, including stronger encryption, access controls, and monitoring for sensitive datasets.

Foundational Principles for Privacy Act Modernization

Background: One of the key themes of the Privacy Act reforms is the desire to make data gathered more accessible within the federal government. A driving idea is that data reuse and sharing will improve service integration and innovation as data can be used in many more ways than it currently can. However, these changes can also pose many harms to privacy if made without the necessary considerations. **To ensure policy changes open the door for responsible data use, reuse, and sharing, they must be rooted in protecting privacy rights.** The proposed changes risk taking control of personal data away from the individuals, as long as the reason fits within broad requirements of data reuse and sharing. Instead, individual control should be championed, allowing people to make their own decisions on how their data will be used beyond what is required for the program they are using. The Government of Canada needs to allow citizens to decide to let their data be used more broadly, and give them the choice of how exactly the data can be used. Allowing people to choose for themselves promotes their right to privacy, and provides better incentives for real protections and proper conduct when people decide to allow greater use of their data, and provides a foundation for modernizing privacy reforms by ensuring federal institutions are properly equipped to reuse and share data.

RECOMMENDATIONS

1. The Privacy Act should be redefined using a rights-based framework informed by international human rights and recognized privacy-protecting legislation.
2. Modernization of the Privacy Act should be guided by principles that necessitate that individuals hold meaningful control over how their data is used beyond what is necessary for a particular service.
3. Require federal institutions to collect, use, and disclose personal information only when it is necessary, proportionate, and the least intrusive means of achieving a legitimate purpose.
4. The Privacy Act should outline and embed a robust Privacy by Design framework that should be followed by federal programs, services, and technologies that interact with people's data.

FOUR PRINCIPLES OF MODERNIZATION

Rights-Based Framework	Protect privacy as a fundamental right.
Individual Control	Give individuals meaningful control over how their data is used.
Necessity & Proportionality	Use only what is necessary and proportionate for a legitimate purpose.
Privacy by Design	Build privacy protections into programs, services, and technologies from the beginning.

Modernizing Privacy Protections for Artificial Intelligence Systems

Background: Artificial Intelligence (AI) and related technologies continue to become embedded itself in everyday life. Large language models (LLMs) operate on publicly available data on the internet to synthesize, create, and present content in many forms. AI and automated decision-making systems are being used in areas such as immigration, benefit administration, fraud detection, and risk assessment, where they can have a significant impact on people's rights, access to services, and privacy. Although the federal government has introduced the Directive on Automated Decision-Making, these safeguards are based on policy rather than legislation and are not fully reflected in the Privacy Act. Without proper safeguards, this can make Canadians' personal information accessible to LLMs. It is clear that AI, in some form, is here to stay, thus the Privacy Act should ensure that Canadians' personal data is stored securely and if used by LLMs, done so in a transparent, secure, and robust method that protects rights to privacy. The Privacy Act has not been meaningfully updated in over 40 years and is not suitable to tackle the challenges of this current technological landscape. As AI technology continues to evolve, and as the Privacy Act modernizes to suit a 21st century context, it is imperative that Canada introduce regulations that protects citizens' privacy and data and incorporates AI in a manner that respects the rights of its citizens. **The law should provide stronger protections to ensure that information is collected responsibly and that automated decisions are transparent, fair, and subject to meaningful human oversight.**

RECOMMENDATIONS

1. Federal institutions should require a documented justification for collecting or processing sensitive personal information.
2. The Government of Canada should require regular audits of automated systems to identify bias, discrimination, and accuracy issues.
3. The Government of Canada should introduce stronger safeguards for high-risk technologies, including facial recognition and biometric systems. The Government should also Acknowledge the use of facial recognition technology (FRT) and disclose when the use or creation of a database of biometric data occurs, followed by full disclosure of deals/agreements between private FRT companies and government services
4. The federal institutions should clearly disclose when online information is used in automated decision making, to combine information, to identify patterns, assess risk , verify eligibility and access inconsistencies. Online information should include personal information, application details, uploaded documents, login credentials, communications and any other data collected through federal websites, online portals, digital forms, mobile applications or digital service platforms.
5. Individuals should have the right to request human review when data is sensitive in nature and/or requires nuance beyond analytical language models and can have significant impact on rights, benefits, or services.

6. The Government of Canada should establish guidelines governing high-risk uses of AI and identifying circumstances in which AI may or may not be used, consistent with the Federal AI strategy, including data of children or in instances involving elections and democratic processes. This should also apply on instances where data is shared between departments.
7. Instances of cross-department use and involving AI should be logged, archived, and accessible to individuals upon request for at least 6 months. Service level agreements should be established by the Federal Public Service so that requests are handled safely and in a timely manner.