



AccessPrivacy and CANON Legislative Reform Roundtable: De-identification and Anonymization under Bill-36

September 24, 2026

ACCESSPRIVACY
BY OSLER



Adam Kardash (Moderator)

Co-Chair: Privacy and Data Management

National Lead, AccessPrivacy



Khaled El Emam

Canada Research Chair in Medical AI

University of Ottawa



Suzanne Morin

Vice President, Chief Privacy & Data

Ethics Officer, Sun Life

Background: CANON

- The Canadian Anonymization Network (CANON) is a not-for-profit organization whose members consist of large data custodians from across the public, private, and health sectors.
- One of CANON's core publicly stated objectives is to advocate for balanced legislative and policy standards for anonymization that enable innovative and beneficial uses of data, while reasonably protecting against foreseeable privacy risks.

CANON and Federal Privacy Legislative Reform

- In 2022, CANON struck a Working Group to consider the provisions in Bill C-27 that relate to concepts of “de-identified” and “anonymized” data.
- In November 2022, CANON held a consultative workshop on its draft proposed amendments to Bill C-27, inviting contribution from a wide variety of stakeholders.
 - More than 180 Chief Privacy Officers, senior counsel and privacy professionals across a breadth of industry sectors attended the workshop, including representatives from retail, health, banking, telecommunications, trade associations, and other public- and private-sector organizations.
- Following its consultation, [CANON submitted proposed amendments](#) and comments to the Standing Committee on Industry and Technology (INDU) and appeared as a witness at INDU committee meetings considering Bill C-27 in October 2023.

Application of the PPCDA

- Like PIPEDA, the PPCDA applies to the collection, use and disclosure of personal information in the course of commercial activities
- **Nature and scope of the concept of “personal information”:** “Information about an identifiable individual, including information that is inferred about the individual.” (s. 2(1))
- Federal government representatives have stated that the inclusion of “inferred data” is a clarification, rather than an expansion, of the definition of personal information.
 - Consistent with regulatory guidance and judicial decisions, which have considered “inferred” or “derived” data that is identifiable as part of personal information attaching to an individual.
 - See e.g. *R. v. Spencer*, 2014 SCC 43, where the Supreme Court held, in the Charter context, that an individual has a personal privacy interest in internet usage data inferred from their IP address.
- **Personal information includes “de-identified personal information”**
 - Personal information that has been modified “so that an individual cannot be directly identified from it, although a risk of the individual being identified remains” (s. 2(1))
- **The PPCDA does not apply to “anonymized” information**
 - Information generated from personal information that has been “irreversibly and permanently [modified] to ensure that there is no reasonably foreseeable risk in the circumstances that an individual can be identified from the information, whether directly or indirectly, by any means” (ss. 2(1) and 6(5))

Contextualizing the Definitions: The Spectrum of Identifiability*

A risk-based spectrum approach to defining identifiability allows for a broad range of innovative uses of information, while accounting for, and mitigating, a reasonable amount of residual risk. To that end, we propose the following spectrum of identifiability with 3 specific states of information:

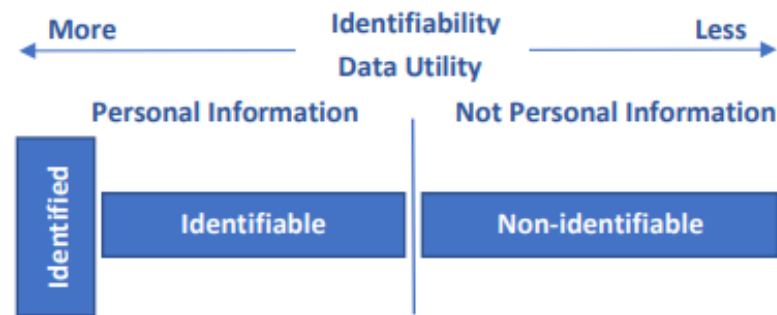


Figure 1. States of Information

DEFINITIONS – Spectrum of Identifiability
Identified information: Information which, by itself, directly identifies an individual.
Identifiable information: Information for which there is a serious possibility in the circumstances that it could be associated with an identifiable individual.
Non-identifiable information: Information for which there is no serious possibility in the circumstances that it could be associated with an identifiable individual.

The phrase “**in the circumstances**” involves consideration of contextual factors that include: likelihood that an actor will attempt to identify the information; what other datasets are accessible to an adversary which might be combined with the information; the environment in which the information will be used or into which it will be released; and, any controls associated with the information.

De-Identification & Anonymization within the PPCDA Framework

- Organizations are authorized to use personal information to de-identify or anonymize it **without the individual's knowledge or consent** (s. 20)
- De-Identification is a **condition precedent to relying on certain exceptions to consent**:
 - Use for an organization's internal research, analysis and development purposes (s. 21)
 - Use and disclosure for a prospective business transaction, unless the requirement to de-identify would undermine the objectives for carrying out the transaction (ss. 22(1) and (2))
- De-identified personal information is **carved out of certain data subject rights**, and organizations are not required to maintain its accuracy

Requirements for De-identification and Anonymization Processes

- When de-identifying personal information, an organization must:
 - **consider re-identification risk** when applying technical and administrative measures to the information; and
 - ensure those measures are **proportionate** to the purpose for which the information is de-identified and its sensitivity (s. 74).
- The Governor in Council may make regulations “respecting the anonymization of personal information” (s. 139(1)(a))

Prohibition on Re-Identification:

- Organizations are **prohibited** from using de-identified personal information – alone or in combination with other information – to identify an individual, **except**:
 - to conduct testing of the **effectiveness of security safeguards** that the organization has put in place;
 - where the personal information was de-identified **solely for the purpose of protecting the information***;
 - where the organization obtains the **individual's valid consent***;
 - where one of the following **exceptions to consent in respect of the use** of personal information applies: ss. 18, 23, 24, 26, 27(2), 29(2), 30, 38(2) or 50*;
 - where the personal information is used **solely for the purpose of anonymizing it***;
 - **to comply with any requirements** under the PPCDA or other federal or provincial law;
 - to conduct **testing of the fairness and accuracy** of models, processes and systems that were developed using de-identified personal information;
 - to conduct **testing of the effectiveness** of the de-identification process;
 - for a purpose or situation authorized by the Division under s. 138 (i.e., where, on an organization's request for authorization, the Division determines it is clearly **in the interests of the individual**); or
 - in any other **prescribed circumstance**. (s. 75)

**Carve-outs from the default prohibition not included in the former CPPA.*

Exception to Consent – Internal Research, Analysis and Development

- The PPCDA provides organizations with an exception to consent for the use of personal information for the broad concept of “internal research, analysis and development purposes”, on the **condition** that the information be “**de-identified**” **prior to the use** for such purpose (s. 21)
 - Unlike exception to consent for business transactions, no carve-out where de-identification would “undermine the objective” of the R&D or analysis activity
 - Many R&D activities and analysis that legitimately require the processing of personal information (including standard customer research, AI and other complex analytics) would fall outside the scope of this exception to consent authority
- The PPCDA removes the disclosure exception for “statistics, study or research purposes” (former C-27, s. 35). There is no equivalent in Bill C-36.

Exception to Consent – Prospective Business Transactions

- Background: PIPEDA contains a helpful (and widely used) exception to consent for parties to disclose personal information in connection with a prospective and completed business transaction as long as certain requirements are met (including notice to impacted individuals upon completion of the transaction)
- The PPCDA contains a similar “**business transaction**” provision, but it has been amended very restrictively to require that personal information be **de-identified before it is used or disclosed** in connection with a prospective transaction (and remain de-identified until the transaction is complete)
- This de-identification requirement will not apply if:
 - de-identifying would “undermine objectives for carrying out the transaction”, and
 - the organization has “taken into account the risk of harm” to the individual that could result from using or disclosing the information (s. 22(2))

Data Subject Right Carve-Outs for De-identified Personal Information

- **Rights of information and access**
 - An organization is not required to act on a request for information about, or access to, de-identified personal information (s. 63(2))
- **Right of amendment**
 - An organization is not required to amend de-identified personal information (s. 71(2))
- **Right of data portability**
 - An organization is not required to disclose de-identified personal information on request, even if both organizations are subject to a data mobility framework (s. 72(2))
- **Right of disposal**
 - An organization is not required to dispose of de-identified personal information, regardless of whether any other conditions to refuse the request are met (s. 54(3))
- An organization is also not required to maintain the **accuracy** of de-identified personal information (s. 55(2))

Enforcement: Potential Penalties, Fines, and Orders

- Prohibition on re-identification: knowingly using de-identified information in contravention of s. 75 is an offence, and an organization could be liable for a fine of up to the greater of \$25 million and 5% of gross global revenues (s. 145)
- AMPs (up to \$10M or 3% of gross global revenue) are potentially available if the organization:
 - has not obtained consent and has not met the requirements for an exception to consent (ss. 15(1), 113(1)(f)),
 - processed personal information for inappropriate purposes (ss. 12(1), 113(1)(c)), or
 - contravened openness/transparency provisions (ss. 62(1), 113(1)(n)).
- The Commission may make an enforceable order for an organization to:
 - take “any measure necessary” in order to comply with the PPCDA, and/or
 - cease “any act” that is in contravention of the PPCDA (s. 110(1))

The Statutory Standards: Requirements for De-identification and Anonymization Processes

- Definition: “de-identified” personal information
 - Personal information that has been modified “so that an individual cannot be directly identified from it, although a risk of the individual being identified remains” (s. 2(1))
- When de-identifying personal information, an organization must:
 - **consider re-identification risk** when applying technical and administrative measures to the information; and
 - ensure those measures are **proportionate** to the purpose for which the information is de-identified and its sensitivity (s. 74).
- Definition: “anonymized” information
 - Information generated from personal information that has been “irreversibly and permanently [modified] to ensure that there is no reasonably foreseeable risk in the circumstances that an individual can be identified from the information, whether directly or indirectly, by any means” (ss. 2(1) and 6(5))
- The Governor in Council may make regulations “respecting the anonymization of personal information” (s. 139(1)(a))

Exceptions to Consent – Standard Business Activities

The PPCDA clarifies and expands the circumstances where organizations may collect and/or use personal information without consent in the course of standard “business activities”.

- No consent required for the collection and use (**but not disclosure**) of personal information for a “business activity” that:
 - **is necessary to provide a product or service** that the **individual has requested** from the organization;
 - is necessary for **the security of the organization’s information, systems or networks**;
 - is necessary for the **safety of a product or service** that the organization provides; or
 - is a prescribed activity (s. 18(2));

provided that:

- a **reasonable person would expect** the collection or use for such an activity; and
- the personal information is not collected or used for the purpose of **influencing the individual’s behaviour or decisions**. (18(1))

Exceptions to Consent – Legitimate Interests

- Substantively distinct from GDPR “legitimate interests” authority
- Collection, use **or disclosure*** of personal information without consent is authorized if done for the **purpose of an activity in which the organization has a legitimate interest that outweighs any reasonably foreseeable adverse effect on the individual** that could result from that collection, use or disclosure, and:
 - a reasonable person would expect the collection, use or disclosure for such an activity; and
 - the personal information is not collected, used or disclosed for the purpose of influencing the individual’s behaviour or decisions (s. 18(3))
- Before collecting, using or disclosing personal information in reliance on s. 18(3), an organization must:
 - **identify and describing the organization’s legitimate interest** in the proposed activity;
 - carry out, in accordance with regulations, **a privacy impact assessment**, in which the organization must identify any **reasonably foreseeable adverse effect** on the individual that is likely to result;*
 - identify and take **reasonable measures to reduce likelihood of adverse effects** or to mitigate them; and
 - comply with any prescribed requirements (s. 18(4)).
- **A record of such assessment** must be created and, upon request, provided to the Commission (s. 18(5))

**New: expansion of authority to disclose and explicit requirement to conduct a PIA, neither contained in former C-27*

Thank you for attending!