Osler, Hoskin & Harcourt LLP

De-Identification and Anonymization of Personal Information: Black, White, and Many Shades of Grey in Between

ONTARIO BAR ASSOCIATION

PRIVACY LAW SUMMIT 2019

April 3, 2019, Toronto, ON

Patricia Kosseim
Counsel, Privacy and Data Management
National Co-Lead, AccessPrivacy

April 2019

OSLER

Definition of Personal Information in the Public Sector

- *Personal information generally means information "about" an "identifiable" individual that is in recorded form*
- The definition of personal information generally includes a non-exhaustive list of examples, and a list of explicit exclusions.
- In Quebec, "nominative information" is information which relates to a natural person and allows that person to be identified.

Fed	BC	AB	SK	MB	ON	QC	NS	PEI	NB	N&L	YK	NWT	Nun
s.3	Sch.1	s 1(1)	s.24(1)	Defns	s.2(1)	s.54	s. 3	s. 1	s. 1	s. 2	s. 3	s. 2	s. 2

Definition of Personal Information in the Private Sector

- *Personal information generally means information "about" an "identifiable" individual* (Federal, BC and Alberta).
- *Business contact information* is specifically excluded from the definition of personal information in BC, whereas in PIPEDA and AB PIPA, it is excluded from the scope of application of the Acts altogether.
- In Quebec, *personal information means any information which relates to a natural person and allows that person to be identified*.

PIPEDA	Alberta PIPA	BC PIPA	Quebec
s. 2(1)	s. 1(1)(k)	s. 1	s. 2

Definition of Personal Health Information in the Health Sector

- Health information generally means identifying information – ***not*** *necessarily* in recorded form -- that includes specific, enumerated types of information.

BC	AB	SK	MB	ON	QC	NS	PEI	NB	N&L	YK	NWT	Nun
NA	s.1(1)(k)	s. 2(m)	s. 1(1)	s. 4(1)	NA	s.3(r)	s. 1(t)	s. 1	s.2(1)(p)	s.2(1)	s. 1(1)	s.2

Thresholds of "De-Identification"

- Individual's identity cannot be "***readily ascertained***" from the information (AB and PEI)

- It is not "***reasonably foreseeable***" in the circumstances that the information could be used, either alone or with other information, to identify the individual (Ontario, NB, Nfld&Lab, NWT, and NS)

- Information that may not "***reasonably be expected***" to identify an individual (SK)

- There is no "***serious possibility***" that an individual could be identified through the use of the information, alone or in combination with other available information. – *Gordon* v. *Canada (Minister of Health),* (2008) FC 258 at para 34.

Some Key Regulatory Findings re "Technical Identifiability"

IP Addresses

- MyDemocracy PA AR 2017 (when combined with internet browser characteristics)
- Deep Packet Inspection PIPEDA #2009-010 (when combined with subscriber IDs)
- OPC Research Paper: *What an IP Address can Reveal About You* (2013)

Cookies (serial numbers)

- When combined and used in connection with a particular user over time and across websites in order to track web browsing activity and infer user interests – OPC Guidelines on Privacy and Online Behavioural Advertising (2011)
- Follow-up Research Report (June 2015)
- PIPEDA # 2014-001; PIPEDA # 2014-011

Unique Device IDs

- PIPEDA # 2013-017 (when combined with Apple ID account details for each iOS device user)

Compare with U.S. HIPPA Approach

- Two thresholds of de-identification

Safe Harbor	Expert Determination
§ 164.514 (b)(2)	§ 164.514 (b)(1)
Removal of 18 specific types of identifiers, such that the residual information is deemed to be "non-identifiable"	A person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods… determines that the "risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify the individual"

Compare with EU GDPR Approach

- Introduces a "middle" concept of "pseudonymization" – calibrated risk approach
- Not exempt from GDPR (i.e., still personal data), but subject to more relaxed requirements. Gives organizations greater flexibility in terms of permissible processing, thereby incentivizing them to pseudonymize as a safeguarding measure.

identifiable	**pseudonymized**	**anonymized**
Information relating to an identifiable natural person – i.e. one who is identified or can be identified, directly or indirectly.	Personal data that can no longer be attributed to a specific individual without use of additional information, provided such information is kept separately and is subject to technical and organizational measures to ensure non-attribution. Account should be taken of all means reasonably likely to be used to re-identify, including costs, time and available technology at the time of processing.	Information which does not relate to an identified or identifiable natural person or is rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Major Legal and Policy Challenges Still to Sort out in Canada

- What does identifiable mean? Can we do a better job of defining it – quantitatively and/or qualitatively in terms of risk? (see Ontario OIPC's *De-identification Guidelines*, 2016)

- Can an organization de-identify personal information without individual consent to do so? (Several health information protection statutes permit this explicitly, whereas other statutes are silent.)

- Are there internal governance mechanisms that are sufficiently robust, proven and trustworthy to allow organizations to innovate with data that is de-identified without entirely losing its utility?



Objectives:

- Share and exchange information about internationally-evolving, legal, policy and technical standards on anonymization.
- Develop a Canadian community of practice among stakeholders that rely on effective anonymization for the success of their organizations -- across public and private sectors.
- Educate the community at large about the effectiveness of alternative anonymization methods, and meaningfully contribute to discussions about risks and opportunities.
- Identify emerging issues and challenges with anonymization, including re-identification risks, legal/policy constraints and ambiguities.
- Advocate for balanced legislative and policy standards for anonymization that enable innovative and beneficial uses of data, while reasonably protecting against foreseeable privacy risks.



Key Success Indicators:

Should CANON succeed in fulfilling its objectives in the first 3-5 years, organizations will:

- Have gained a better understanding of what anonymization means, and how it can be effectively achieved while preserving the utility of data.
- Be better able to negotiate as between controllers and processors using more streamlined and common understanding of terms and expectations.
- Be in a better position to communicate with regulators and to 'demonstrate accountability' on demand.
- See a reduction in the level of privacy risks they face and an enhancement of their reputation.
- Be more confident about their secondary uses of data and using data to drive innovations in products and services.
- Begin to gain increased trust and confidence of consumers / individuals.

Discussion