Canadian Privacy Laws and Blockchain

Presented By
Max Jarvie,
Borden Ladner Gervais LLP

November 2019

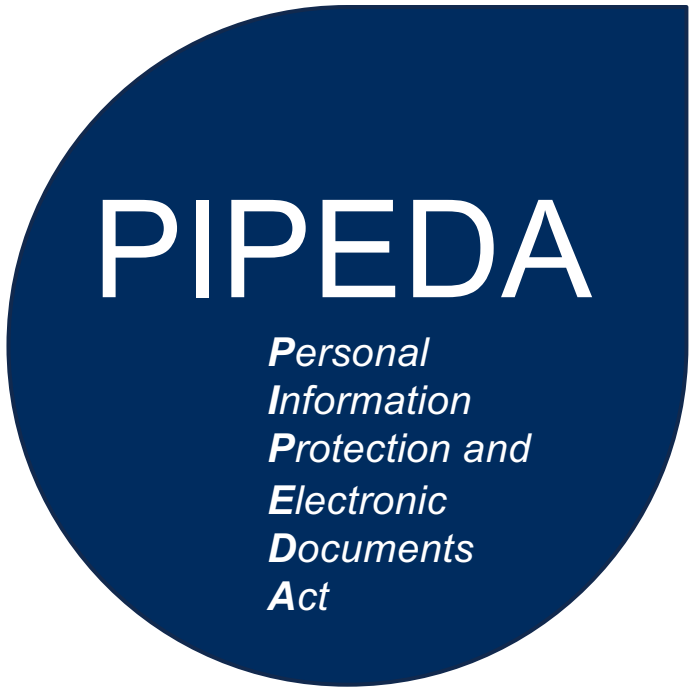
BLG
Borden Ladner Gervais

Agenda

1. Canadian Privacy Law Framework
2. Overview of Canadian Regulatory Response to Blockchain
3. Salient Differences
    1. Scope of application: organizations vs. persons
    2. Anonymity: linking data
    3. Centrality of consent: impractical requirements, possible exceptions

1. Canadian Privacy Law Framework

Canadian Privacy Law



- Sets out ground rules for how private sector organizations collect, use and disclose personal information about individuals, unless such activities are regulated by provincial legislation that has been declared substantially similar to *PIPEDA*
- Applies to commercial activities of organizations, including those involving interprovincial and international data flows

Provincial laws

Alberta PIPA — Personal Information Protection Act

BC PIPA — Personal Information Protection Act

Quebec ARPPIPS — An Act Respecting the Protection of Personal Information in the Private sector

These provincial statutes have been deemed substantially similar to PIPEDA and therefore operate in place of PIPEDA for intra-provincial matters (including for personal information of employees).
As mentioned, even in these provinces, PIPEDA continues to apply to the federally regulated private sector and to personal information in inter-provincial and international transactions.

Consequences of non-compliance

- **In contrast to EU under GDPR, Canada continues to use an ombudsman model – no direct fining powers and where fines are provided for, fairly limited.**
- **The Canadian framework relies primarily on reputational damage caused by negative findings and the possibility of private action to deter violations of the law.**
- **This may change as Canada revisits its legal framework to realign with the GDPR.**

2. Overview of Canadian Regulatory Response to Blockchain

Canadian Regulatory Response to Blockchain

- Spoiler alert: None!
- The Federal Office of the Privacy Commissioner has made few statements that refer to cryptocurrency / blockchain / DLT:
  - "Electronic and digital payments and privacy" 2016

"some people suggest virtual currencies can be used to make purchases anonymously. This isn't necessarily true because the digital trail associated with these currencies can still be tied to an individual, although the trail usually consists only of transaction records rather than personal information. To set up an account in order to use these virtual currencies, however, you may be required to provide some personal information, such as your name, credit card information, banking information, driver's licence, utility bill or even passport information."

  - "Joint statement on global privacy expectations of the Libra network" 2019
    - *Authored in collaboration with other regulators*
    - *Chiefly focused on concerns related to Facebook privacy practices, not blockchain technology in general*
  - Promised guidance to come in a list of upcoming bulletins, but blockchain is low on the list

3. Salient Differences

- Scope of application
- Threshold of anonymity
- Centrality of consent

Scope of application

- GDPR: applies to all persons, natural and legal
- Canadian privacy laws apply only to commercial activities of organizations
  - Canadian law does not apply to the collection, use or disclosure of personal information by individuals whether for commercial purposes or not - therefore, no obligations arising for individuals running full nodes
- How does Canadian law apply to organizations working with blockchain?
  - Will certainly apply if commercial activity involves the deliberate injection of personal information into the blockchain in some form.
  - Accountability obligations are triggered – regulators would likely regard an organization's use of blockchain as (irresponsible) engagement of a service provider (processor). The personal information was "theirs to lose".
- What about an organization's use of basic transactional information? Sub-question: Is this information personal information?
- In Canada, the answer is likely "yes", because of Canada's threshold for anonymity.

Anonymity

- **In the EU, notwithstanding recital 30 of the GDPR, it appears the threshold for whether (dynamic) IP addresses would constitute personal information is still governed by *Breyer*:**
  - dynamic IP addresses are personal data if website operators have **"legal means"** enabling the identification of the person associated with the IP address with the help of additional information which that person's internet service provider has.
- **In Canada, the acceptable threshold for anonymity is extremely high.**
  - "Personal information that has been de-identified does not qualify as anonymous information if it is still possible to link the de-identified data back to an identifiable individual."

Psychologist's anonymized peer review notes are the personal information of the patient - PIPEDA Case Summary #2009-018

PIPEDA Report of Findings #2013-001 (January 2013)

- 41. Based on our review of the above process, we found that WhatsApp's treatment of out-of-network numbers was not an effective form of anonymization. True anonymity is only achieved where information can ***never*** be linked to an individual, either directly or indirectly. In our view, WhatsApp's use of all digits in an out-of-network phone number, coupled with a fixed salt value for the hash function, does not result in a true anonymization of out-of-network numbers. (…)

- (…) This is because the number could be recovered, with a modest amount of computing effort, if the out-of-network number database and salt value were breached. Indeed, simple test programs created by our technical experts showed that phone numbers could be recovered, once the salt is known, in under 3 minutes using a standard, low-power desktop computer. **The fact that the phone numbers can be recovered – albeit through a data breach and some computing effort – means that the storage is not truly anonymous.**

(PIPEDA Report of Findings 2013-001, *Investigation into the personal information handling practices of WhatsApp Inc.*)

Anonymity cont'd

Conclusion: Dynamic IP addresses are always personal information under Canadian law, and *mere possibility of reidentification* is the threshold for anonymity.

- Public permissionless blockchain networks typically broadcast IP addresses along with new transaction information (sending and receiving blockchain addresses + amounts to be transferred) to all listening nodes
- It would be trivial to retain and compile such information over time, in much the same manner as is presently done by various entities tracking members of P2P swarms and it is very likely that for any given blockchain, multiple parties are compiling such information, depending on the value of the digital assets on that chain.
- Because the possibility of existence of such a data set cannot be eliminated (coupled with the existence of the log of dynamic ip address assignments made by ISPs) means that under Canadian law, the transactions on public permissionless blockchains of this type are personal information.

Anonymity cont'd

- As such, organizations using blockchain would need to treat basic transactional information as personal information, requiring a legal basis for its collection and use, when entering into transactions with users.

- What legal bases are available in Canada?

CENTRALITY OF CONSENT

- Consent is the legal basis for all processing in Canada.
  - The knowledge and consent of the individual are required for the **collection, use, or disclosure** of personal information, except where inappropriate. (PIPEDA Schedule 1, Principle 3)
- However, the notion of consent is broader than GDPR consent.
  - Consent should generally be express (opt-in, requiring positive action), but it can be implied (opt-out, consent implied by conduct) in strictly defined circumstances (*Royal Bank of Canada v. Trang*, 2016 SCC 50 § 23; See also Alberta PIPA, sections 8(2) – 8(2.2), 8(4); OPC *Guidelines for obtaining meaningful consent,* 2018)
- Could organizations rely on a notion of implied consent?

CONSENT Cont'd.

- Answer: Probably not.
- Generally, consent should be express when :
  - The information being collected, used or disclosed is sensitive;
  - The collection, use or disclosure is outside of the reasonable expectations of the individual; and/or,
  - The collection, use or disclosure creates a meaningful residual risk of significant harm.
- If basic transactional information is personal information in virtue of Canada's threshold for personal / non-personal information, express consent is probably required, as such transactional information is *de facto* financial information and hence likely sensitive.

- HOWEVER: THERE ARE EXCEPTIONS!

Exception for publicly available data

- S. 7(2)(c.1) PIPEDA: An organization may use personal information, even without the knowledge or consent of the individual concerned, if it is publicly available and is specified by the regulations.
- Among these (specified in the regulations):
  - personal information that appears in a publication, including a magazine, book or newspaper, in printed or electronic form, that is available to the public, where the individual has provided the information.
- Question: could this exception be broad enough to apply to publication of information on a blockchain?
  - Con: the federal OPC has taken a narrow view of this provision in the past, criticizing an organization's collection of personal information available on Facebook profiles and groups as falling outside the scope of the exception. (PIPEDA Report of Findings #2018-002 (re: Profile Technology Ltd.'s collection of profile and group information in order to provide search engine services);
  - Pro: key to that decision was that power of individuals to dynamically update their profile / group information.

Organization use of basic transactional information

- Yes, Canadian law applies.
  - Such information is personal information;
  - Therefore, organizations need consent to use such information;
  - Such consent would probably need to be express;
  - But the publicly available information exception could also potentially apply.

Future developments?

- In it 2017 report to Parliament, the OPC proposed new exceptions to consent be added to PIPEDA:
- *exceptions would need to be limited to circumstances where the societal benefits clearly outweigh the privacy incursions and where several prior conditions must be met before information can be used for such purposes. We would recommend that Parliament consider the circumstances where such exceptions might be warranted from a broader societal perspective. In our view, situations where consent is likely not always practicable include: search engines indexing web sites and presenting search results to Internet users where appropriate; geolocation mapping services that society has become increasingly reliant upon; or certain data processes, such as big data analytics, Internet of Things, artificial intelligence or robotics applications where commercial and societal interests align.*

Questions?

Thank You

For more information, contact:

Max Jarvie
Lawyer
514.954.2628
MJarvie@blg.com

BLG
Borden Ladner Gervais