David Young Law
Compliance Bulletin

May 2021

Bill C-11 needs a comprehensive model for non-personal information

Bill C-11, the federal government's *Digital Charter Implementation Act* currently before Parliament to enact a new private sector privacy law,[1] includes, significantly, provisions enabling the use and disclosure of de-identified personal information. Such provisions are very appropriate in a law that seeks to enhance and modernize privacy protections as well as to encourage innovation.

However Bill C-11's approach to facilitating de-identification is incomplete and, if not adjusted, likely will lead to a lack of clarity and confidence for stakeholders seeking to comply with the law, thereby compromising the government's stated goals of advancing research, innovation and social good. Establishing an alternative model to the consented use of personal information is understood to be essential for not only scientific research and statistical analysis purposes but more broadly, for machine learning, innovation and, potentially, diverse "socially beneficial purposes".[2]

In a world where obtaining valid, meaningful consent to diverse potential uses of personal information is becoming increasingly difficult and algorithmic models arguably function without consent, alternatives to existing privacy idioms of consent and control over personal information are ripe for re-consideration. Bill C-11 attempts to address these issues partly through expanding PIPEDA's current approach of a consent requirement attached to a "laundry list" of exceptions, including for situations where consent is either not practical or not needed.[3] However it then seeks to respond further by enabling non-consented uses for specified purposes through the mechanism of de-identification.

The Bill C-11 model

Bill C-11 retains PIPEDA's general rule of application - to "personal information" - meaning information about an identifiable individual. However it adds a new concept, "de-identified information" which, by its definition,[4] should be understood to mean information that is *outside application* of the law since what it describes is not personal information. Unfortunately, the Bill confuses the issue by then providing specified permitted uses for

---

[1] *Consumer Privacy Protection Act* (CPPA)

[2] See, for example, the OPC's recent report, *A Regulatory Framework for AI: Recommendations for PIPEDA Reform* (Nov. 2020).

[3] *Personal Information Protection and Electronic Documents Act.*

[4] The CPPA defines "de-identify" to mean "to modify personal information — or create information from personal information — by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual".

such de-identified information,[5] leading to the conclusion that the law continues to apply to such information at least in some respects since, it would be surmised, other uses are not permitted.
Supporting this conclusion, the Bill also includes a number of other provisions dealing with de-identification including: an exception permitting an organization to de-identify personal information held by it, without consent; provisions addressing the proportionality and technical measures to be applied by an organization in de-identifying and using such information; and a prohibition against using de-identified information to identify anyone. The conclusion that Bill C-11 is intended to continue to apply to de-identified information, as well as to personal information, is supported by comments made by officials in the federal Department of Innovation, Science and Economic Development (ISED) in briefings subsequent to introduction of the Bill. [6]

The difficulty with this interpretation of the Bill is that it is not clear whether the intended application is to *all* de-identified information - meaning to include information that by any objective standard would be considered "non-personal" and therefore not identifiable within the law's stated intended application - or only to information that does not meet this high standard. Supporting the latter interpretation is the argument that since it reasonably can be expected that such information may (and in certain circumstances will) be re-identified it should be governed by the rules applicable to personal information generally, or some appropriate subset of such rules. Without clarification, the arguable conclusion is that the Bill is intended to apply to both categories.

What is "de-identified" (or non-personal) information and how do other laws deal with it?

To understand and potentially improve on Bill C-11's approach to de-identified information, it is useful to provide a more comprehensive terminology than that currently proposed for the new law. Instead of de-identified information, a more readily understandable term would be "non-personal" information, encompassing all information that is derived from personal information whether or not there is any reasonable likelihood, or expectation, that it could (or will) be re-identified or used to identify an individual – in other words, both categories described in the preceding paragraph. As noted, Bill C-11 does not make this distinction. However comparative international and provincial laws, or proposed laws, do and it is instructive to understand not only how they define the relevant terms but also how they address application to these categories of non-personal information.

Reference may be had to the EU's *General Data Protection Regulation* (GDPR), Quebec's proposed Bill 64 and the *California Consumer Privacy Act* (CCPA). All these laws or proposed laws define a category of non-personal information to which the law does not apply, with some differences in terminology. The GDPR and Bill 64 call this category "anonymous" or "anonymized" information. They then provide for categories of non-personal

[5] Research and development (s. 21), due diligence for a prospective sale of a business (s. 22(1)), socially beneficial purposes (s. 39).
[6] ISED conference call briefing, November 17, 2020.

.

information that *are,* either expressly or impliedly, subject to their privacy rules, defined as "pseudonymized" or "de-identified" information. The CCPA's defined term for information outside the law is "de-identified" information" which is confusing because this is the term used in the CPPA as well as in Bill 64 for information either potentially or actually subject to the law. The CCPA does not expressly provide for a category of non-personal information to which it has application.[7]

The GDPR defines *pseudonymized information* as personal data that has been processed in such a manner that it can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to prevent re-identification. Since such data is considered re-identifiable it therefore continues to be treated as personal information subject to the GDPR's general data protection rules. However the GDPR recognizes that pseudonymization may reduce the privacy risks to individuals and its rules contemplate lesser protection than that required for identifiable, personal information.

On the other hand, the GDPR defines *anonymous information* as information which does not relate to an identified or identifiable natural person and provides expressly that such information is outside the application of the law.

Similar to the GDPR, Quebec's Bill 64 provides for "de-identified information" and "anonymized information", with the former fully subject to the law and the latter outside of it. De-identified information is information that no longer allows the person concerned to be directly identified; in other words, information from which direct identifiers (example - name, driver's licence) have been removed. Anonymized information is defined as information that irreversibly no longer allows a natural person to be identified directly or indirectly. The Bill provides that information within the excluded category must be anonymized according to generally accepted best practices. It does not stipulate any specific rules regarding ensuring against re-identification.

California's CCPA provisions define a category of "de-identified" information in language similar to the CPPA but, unlike the CPPA, clear up any ambiguity by expressly excluding such information from application of the law, provided that a business seeking to rely on the exclusion has implemented technical safeguards and processes to prohibit the information from being re-identified.[8]

Application of a privacy law to anonymized information

An important caveat to the exclusion of appropriately anonymized information from any general application of the privacy law is that if the anonymity of the information is not protected it will again become subject to the law. This potential eventuality is reflected in the CCPA's definition of de-identified information as well as in the CPPA's treatment of de-identified information. Both regimes stipulate that an organization seeking to use such information (and benefit from whatever exclusion from the law's application is provided) must apply technical

[7] The CCPA includes as a defined term "pseudonymized information", with language similar to the GDPR but other than in respect of use for research activities makes no reference to its application to such category.
[8] Also a requirement of the CPPA – see s. 74.

safeguards and procedures to prevent the information from being re-identified. In reality, whether or not this stipulation is made in the law expressly, if a user of anonymized information fails to protect its non-personal character with the result that the information becomes identifiable, then the user *does become subject to the law* and the resulting identifiable information again would have full privacy protection.

Since the rules defining the excluded category (anonymous information) implicitly extend the reach of the privacy law to this category by requiring compliance with such rules and, therefore potentially, extending its full application to such information, an argument can be made that personal information and non-personal information are really just two ends of a spectrum – one of which is full identifiability and the other "irreversible" non-identifiability.

To be clear, any discussion of these categories of non-personal information contemplates a category of information outside the law, whether it be called anonymized or de-identified information, that may have originated as identifiable information but has been made non-identifiable, potentially irreversibly. For purposes of the discussion, we are not talking about anonymous information that never had, or has, any connection to identifiable information, so it is appropriate to include the "excluded" category in a comprehensive regime for non-identifiable information.

Conclusion - a comprehensive regime for non-personal information is required

To properly provide a framework for non-personal information that has clarity and confidence for stakeholders as well as to ensure alignment with evolving international and Canadian provincial norms, the CPPA should make provision for a limited category of non-personal information that will be subject to its generally applicable rules, at least in part, as well as provision for non-personal information outside of its rules.

The category of information that would be governed in a specified manner by all of its provisions (subject to stipulated exceptions), should be termed *de-identified*, or *pseudonymized*, information, and should be defined as "personal information that has been processed in a manner that it cannot be used in reasonably foreseeable circumstances to identify an individual without additional information". The excluded category of non-personal information should be termed *anonymized* information and defined – using language drawn from the GDPR and Bill 64 – as "information that irreversibly no longer allows an individual to be identified".

Stipulating the full application of the law to the first category of non-personal information is key because while such information may be de-identified, it still enables identification of individuals by adding back identifying features. Consequently, such information should be protected substantially in the same manner as personal information. However, as the GDPR provides, since the risks associated with such information are likely to be lower, the levels of protection in respect of such information can be lower.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca