C-27: Strengthening privacy while fostering innovation and supporting Canada's digital economy[1]

By Eloïse Gratton, Andy Nagy and Simon Du Perron[2]

In the context of the reform of our federal privacy law, we find ourselves at a critical juncture where we have the unique opportunity to strike a balance that ensures the protection of our privacy rights while fostering an environment of innovation. In a rapidly evolving digital age, where information flows faster than ever before, our privacy is increasingly at risk. This makes it imperative that we reform our privacy laws to reflect the realities of today. However, data protection laws should not stifle the innovative spirit that has propelled us into the 21st century. Innovation drives economic growth, creates jobs, and improves our quality of life. It is the engine of progress. Striking the right balance between privacy and innovation is a complex task, but not an impossible one.

Bill C-27 introduces two new statutes that would make substantial changes to the federal data protection legislation, the *Personal Information Protection and Electronic Documents Act* (**PIPEDA**). First, the *Consumer Privacy Protection Act* (**CPPA)** would replace Part 1 of PIPEDA, which relates to the protection of personal information. Second, the Personal Information and *Data Protection Tribunal Act* would create a new Data Protection Tribunal. Bill C-27 also introduces the *Artificial Intelligence and Data Act*, which would create a new legal and general framework for the regulation of artificial intelligence (**AI**).

Other jurisdictions such as Europe and Québec have already updated their data protection laws. The European Union's *General Data Protection Regulation* (**GDPR**) came into effect in 2018, and Québec's data protection regime, which includes the *Act respecting the protection of personal information in the private sector* (**Québec Private Sector Act**), was recently amended by Bill 64 (Law 25), with most of the changes coming into effect in September 2023. These laws are in many ways more onerous than the CPPA, but in other aways they strike a better balance between privacy and innovation. In that sense, there are definitely lessons to be learned from these jurisdictions.

This submission identifies four specific areas where the proposed provisions of the CPPA could be refined to better support innovation, drawing on insights from the GDPR and the recently amended Québec Private Sector Act:

1. Legitimate interest consent exception

PIPEDA is based on the *Fair Information Practices* which were initially drafted in the early 1970s – and we should keep in mind that their main purpose was to address specific concerns pertaining to computerized databases and the fact that different public and private sector organizations could exchange personal

[1] Brief presented on October 24, 2023, to The House of Commons of Canada's Standing Committee on Industry and Technology in view of its study of Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts.

[2] Eloïse Gratton is a partner at Borden Ladner Gervais LLP and National Leader of the firm's Privacy and Data Protection practice group and Andy Nagy and Simon Du Perron are associates in the Privacy and Data Protection practice group. The contents of this document should not be construed as legal advice. The opinions expressed herein are solely those of the authors in their personal capacity and do not represent in any way the opinions of Borden Ladner Gervais LLP or any of its clients.

information more easily without the knowledge or consent of individuals. At the time, the best way to address these new concerns was to have individuals maintain control over their personal information.

Half a century later, this concept remains one of the dominant theories of privacy and the basis for data protection laws around the world, including PIPEDA here in Canada. But the "notice and choice" approach these laws impose is no longer realistic: individuals are overloaded with information in quantities that they cannot realistically be expected to process or comprehend. Complex information flows and new business models involving a variety of different actors have also challenged the traditional consent model. In this context, the introduction of new consent exceptions is welcomed.

The CPPA introduces new consent exceptions, which are specifically designed to facilitate the collection and use of personal information for certain defined purposes. These purposes include "business activity"[3] listed in subsection 18(2), and activities in which the organization has a "legitimate interest" that outweighs any potential adverse effect on the individual, as defined in subsection 18(3). While similar language is found in the GDPR, which creates a separate legitimate interest basis for processing personal data (see Art. 6(1)(f); recital 47), it is important to note that the CPPA differs in a few key areas.

First, the CPPA's business activities and legitimate interest exceptions are just that: exceptions to the consent requirement. As such, they are not separate legal bases for processing personal information on the same footing as consent. This is important because courts tend to interpret consent exceptions narrowly, which is likely to favour a narrower interpretation of these new exceptions.

Second, these exceptions are limited to the collection and use of personal information, meaning that a disclosure to a third party for the purpose of a "business activity" or an activity in which the organization has a "legitimate interest" would not be permitted, notwithstanding that appropriate measures have been taken to mitigate the risk of harm resulting from the disclosure.

For example, an organization may need to share personal information with a number of third parties to "provide a product or service" requested by an individual (s. 18(2)(a)). This may include payment processors, package delivery providers, financial institutions, and other third-party intermediaries that merely facilitate a commercial transaction. This may also include AI system processors. While some of these third parties may be considered service providers (and benefit from a separate consent exception), others may play a role closer to that of an independent controller (for which consent would be required).

Similarly, the exception for activities in which an organization has a legitimate interest may in some cases create an arbitrary distinction between the collection and use of personal information and its disclosure. For example, an organization may collect and use personal information to measure and improve the use of its services. This may arguably fall under the legitimate interest exception, provided that the organization has a clear interest in improving its services that outweighs any potential adverse effects on individuals and takes appropriate steps to assess and mitigate those effects (s. 18(4)). However, if the same organization were to disclose the personal information for the same purpose to a third-party vendor who is also acting as a business partner in some capacity, that disclosure may not be covered by the exception.

[3] Listed in subsection 18(2).

Third, this legitimate interest exception under subsection 18(3) is narrower than the "legitimate interest" basis under the GDPR. Subsection 18(3) provides that "an organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use and 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."[4] On the other hand, article 6(1)(f) of the GDPR states that the processing of personal data is lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, "except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data".

The GDPR proposes a balancing test of the societal benefits and the benefits to the controller against the interests or fundamental rights and freedoms of impacted individuals. The CPPA instead proposes a balancing test against "any potential adverse effect on the individual" which may be less flexible than under the GDPR. Moreover, this consent exception is subject to the additional requirement found in subsection 18(3) of the CPPA, which mandates that a "reasonable person would expect the collection or use for such an activity," and the "reasonableness test." Under this test, an organization may collect, use, or disclose personal information only in a manner and for purposes that a reasonable person would consider appropriate in the circumstances (as per s. 12(1) CPPA, replacing s. 5(3) PIPEDA).What these "reasonable expectations" are in any given context, and whether certain activities are legitimate from a privacy perspective, is often a function of many factors, including the prevailing social norms. An additional challenge for innovation pertains to the fact that social norms in connection with any new technology or business practice may not yet be established at the time where such new technological product or service is deployed.

The fact that the CPPA's proposed amendment is narrower than the legitimate interest legal basis under the GDPR may greatly limit its utility. We also have to bear in mind that personal information collected from publicly available sources on the Internet does not benefit from a consent exemption simply because it is publicly available.[5] While this affords a protection for unethical uses of publicly available personal information, it also prevents legitimate organizations working on new products and services that may benefit the society, to leverage the large volume of data readily available on the web.

For these reasons, the exceptions to consent for business and legitimate interest activities should be more closely aligned with the GDPR legitimate interest legal basis to accommodate new, innovative types of business models. These adjustments could include appropriate accountability mechanisms, such as contractual measures limiting the third party's use of the information and a prior privacy assessment of the impact of an activity on the fundamental rights and freedoms of impacted individuals.

[4] S. 18(3) states that "An organization may collect or use an individual's personal information without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a legitimate interest that outweighs any potential adverse effect on the individual resulting from that collection or use and (a) a reasonable person would expect the collection or use for such an activity; and (b) the personal information is not collected or used for the purpose of influencing the individual's behaviour or decisions. Conditions precedent (4) Prior to collecting or using personal information under subsection (3), the organization must (a) identify any potential adverse effect on the individual that is likely to result from the collection or use; (b) identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them; and (c) comply with any prescribed requirements."

[5] e.g., see *A.T. v. Globe24h.com*, 2017 FC 114 (CanLII), [2017] 4 FCR 310.

With respect to the legitimate interest consent exception (CPPA, s. 18 (3)):

- **Recommendation #1.** Consider expanding this consent exception to a new standalone legal basis or adjust the consent exception to make it more closely aligned with the GDPR legitimate interest legal basis, for instance by adjusting the wording of the balancing test (replacing "that outweighs any potential adverse effect on the individual resulting from that collection or use" by "that is not overridden by the fundamental rights and freedoms of the individual") and allowing organizations to rely on legitimate interest for disclosures.
- **Recommendation #2.** If recommendation #1 is implemented, consider including enhanced oversight measures and/or security requirements to help ensure the responsible use or implementation of this new consent exception or legal basis.

2. Limited scope of the "socially beneficial purposes" consent exception.

Section 39 of the CPPA creates a new consent exception for disclosures of de-identified personal information to specific public sector entities, including government, healthcare, and post-secondary educational institutions, as well as public libraries in Canada. Limiting this consent exception only to disclosures to public sector entities, rather than to both public and private sector entities, severely restricts its utility.

By limiting the types of entities with whom de-identified information may be shared, this new consent exception creates very limited opportunities for organizations to rely on it in practice. While the purported aim of this provision is to enhance public-private "partnerships",[6] we question whether this intent can be fully realized given the conspicuous absence of reciprocity, cooperation, or two-way exchange of information between the public and private sector. By exhibiting a distinct public sector bias, this consent exception also fails to recognize the valuable role played by private sector organizations in pursuing activities that advance socially beneficial purposes. The private sector may have access to talent and resources that could be leveraged to pursue socially beneficial purposes in more innovative or expeditious ways. This is not to say that the public sector does not play an important role in these situations, but rather that there is no clear, principled basis on which the public sector ought to be given an undue preference or privilege in pursuing such purposes.

In the digital era, many private sector organizations amass large volumes of personal information about their clients, employees, and other individuals that could be put to use for a variety of socially beneficial purposes, not all of which fit within the narrow definition provided under the aforementioned consent exception. In turn, we have seen the rise of open data initiatives that enable a broad range of third parties, not just designated public sector entities, to access and share personal information for legitimate purposes related to science, technology, and innovation. As such, it is unclear whether it is necessary to limit the CPPA's socially beneficial purposes consent exception to public-private partnerships, especially

[6] ISED, "Proposals to modernize the Personal Information Protection and Electronic Documents Act", https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html.

as private sector organizations are equally capable of utilizing this information to drive research and innovation in a number of fields and of ensuring its protection against internal and external threats.

A more principled approach would be to frame consent exceptions around requirements of adequate oversight and data protection best practices, rather than public sector exclusivities or monopolies, to facilitate and encourage responsible data sharing between a broader range of actors. That same approach would have the added benefit of addressing other shortcomings in the current drafting of the exception. More specifically, while other privacy regimes typically require organizations to implement data protection agreements with their service providers or other third parties with whom they may share de-identified information, we note that section 39 of the CPPA currently provides no similar obligation. In other words, organizations sharing de-identified information with designated public sector entities will not be required to obtain any further guarantees to ensure that such information will be adequately protected. These issues are potentially compounded by the fact that public sector entities are generally subject to a distinct data protection regime, and that this regime is subject to a degree of uncertainty as it is currently the focus of consultations at the federal level. As such, we propose expanding the scope of the consent exception at section 39 to also accommodate data sharing initiatives between private sector organizations, while simultaneously requiring organizations to implement minimum contractual protections limiting the purposes for which information can be used and ensuring information receives an appropriate level of protection.

To summarize, this section 39 could be revised to authorize and facilitate responsible data sharing among a broader range of actors (including private sector organizations) that may have access to talent and resources that they can leverage to pursue socially beneficial purposes. This review should include the introduction of additional oversight requirements and data protection practices, such as the implementation of specific contractual measures and a requirement to conduct a privacy impact assessment before relying on this consent exception.

With respect to the “socially beneficial purposes” consent exception (CPPA, s. 39):

- **Recommendation #3.** Consider expanding this consent exception to also include disclosures made to private sector organizations.
- **Recommendation #4.** If recommendation #3 is implemented, consider including enhanced oversight measures and/or security requirements to help ensure the responsible use or implementation of this consent exception.

3. Absolute standard for anonymization may not be appropriate.

The use of anonymized datasets is a key aspect of reasonable and necessary analytics activities that help shape Canada’s future. The CPPA introduces new definitions for the terms “anonymize” and “de-identify,”[7] which provide greater flexibility regarding the processing of these categories of information. However, for data to be considered “anonymized” under the section 2(1) of the CPPA, it must be “irreversibly and permanently modif[ied]…, in accordance with generally accepted practices, to ensure

[7] Under the CPPA, to “de-identify” will mean “to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains” (s. 2).

that no individual can be identified from the information, whether directly or indirectly, by any means."[8] This definition – which was not featured in the previous iteration of the CPPA under Bill C-11 – seems to be strongly inspired from Québec Bill 64, which provides that personal information is anonymized "if it is, at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly".[9] However, unlike Québec Bill 64, the CPPA does not introduce a wording similar to "reasonably foreseeable in the circumstances". This is, in our view, an important omission given the relevance of a reasonableness criterion when it comes to sophisticated data management techniques such as anonymization.

It is relevant to mention that this wording was introduced by an amendment adopted during the clause-by-clause review of Québec Bill 64. As demonstrated by the debates from the sittings held by the Committee on Institutions, a reasonableness notion was introduced in the definition of anonymized information in order to avoid holding organizations accountable to an absolute standard that is impossible to achieve in practice. Minister Éric Caire, the bill's sponsor, explained the amendment during the clause-by-clause review of Bill 64 as follows:

> « En fait, l'idée de départ, c'était que dans cet article-là tel qu'il avait été rédigé en toute bonne foi, c'était la notion d'irréversibilité. Puis, je pense qu'on a discuté de ça avec les collègues abondamment, la loi exigeait quelque chose qui est… bon, qui n'est pas impossible, mais qui est quasi impossible, et c'est la raison pour laquelle je voulais vraiment valider… Et la notion de… quand on dit « lorsqu'il est raisonnable de prévoir dans les circonstances qu'il ne permet plus de façon irréversible », là, il y a la notion de raisonnabilité. Donc, si je prends vraiment tous les moyens pour le rendre irréversible, je serai conforme à la loi. »[10] (Our underlines)

In turn, Jean-Philippe Miville-Deschênes, the government lawyer, remarked that « l'aspect irréversible était un peu, selon les experts, utopique »[11], with Minister Caire subsequently adding:

> « …] Mais la notion d'irréversibilité, sans l'amendement, là, la loi nous amène dans un univers qui n'est pas réaliste. Alors, je voulais apporter cette nuance-là sur ce point-là. »[12] (Our underlines)

As we can see, the addition of "reasonably foreseeable in the circumstances" in the definition of anonymized information under Québec Bill 64 was intended to reflect a growing consensus among the academic and technical literature regarding the impossibility of achieving a zero risk of re-identification within an anonymized dataset.[13] For this reason, many jurisdictions have favoured a more nuanced, risk-

[8] For data to be considered "anonymized" under the section 2(1) of the CPPA, it must be "irreversibly and permanently modif[ied]…, in accordance with generally accepted practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means."

[9] See new section 23 para. 2 of Quebec's *Act respecting the protection of personal information in the private sector*, CQLR c. P-39.1.

[10] Please note that the transcription of the parliamentary debates on Bill 64 is only available in French: http://www.assnat.qc.ca/en/travaux-parlementaires/commissions/ci-42-1/journal-debats/CI-210331.html.

[11] *Ibid.*

[12] *Ibid.*

[13] See in particular Luc Rocher, Julien M. Hendrickx and Yves-Alexandre de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models", (2019) 10-1 *Nature Communications* 3069; Martin Scaiano, Grant Middleton, Luk Arbuckle, Varada Kolhatkar, Liam Peyton, Moira Dowling, Debbie S. Gipson and Khaled El Emam, "A unified framework for evaluating the risk of re-identification

based approach to the anonymization of personal information. For instance, the conceptualization of anonymization under the GDPR requires consideration of "all objective factors, such as costs and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".[14] The UK data protection authority has adopted the "motivated intruder test" for evaluating the risk of re-identification.[15] The risk-based approach has also been successfully implemented in under Ontario's *Personal Health Information Protection Act* and the associated "De-identification Guidelines for Structured Data" of the Information and Privacy Commissioner of Ontario.[16]

Some may suggest that a relative standard is subtly incorporated into the CPPA definition of anonymized information given that anonymization under the CPPA must be done "in accordance with generally accepted best practices" (CPPA, s. 2(1)). As previously explained, experts have generally recognized that anonymization techniques do not produce datasets for which there is *zero* probability of re-identification, but rather datasets for which the probability of re-identification is *very low*, taking into account the specific characteristics of the dataset. Nevertheless, to avoid conflicting interpretations, the CPPA definition of "anonymize" should expressly include a reasonableness standard. Including such a standard would also be more realistic than holding organizations accountable to an absolute standard that may be impossible to meet in practice.

Recommendation #5. Consider including a reasonableness standard in the definition of "anonymize" to avoid imposing an impractical, absolute anonymization standard on organizations.[17]

Please note that the Canadian Anonymization Network has published an in-depth analysis of these challenges in their publication, Proposed amendments to the de-identification and Anonymization provisions in the Digital Charger Implementation Act, 2022 (Bill C-27), which should be read alongside this section.

of text de-identification tools", (2016) 63 *Journal of Biomedical Informatics* 174 and Khaled El Emam, *Guide to the De-Identification of Personal Health Information*, New York, Auerbach Publications, 2013.

[14] Recital 26, GDPR.

[15] The 'motivated intruder' is assumed to be "reasonably competent, has access to resources such as the internet, libraries, and all public documents, and would employ investigative techniques such as making enquiries of people who may have additional knowledge of the identity of the data subject or advertising for anyone with information to come forward". However, this person is "not assumed to have any specialist knowledge such as computer hacking skills, or to have access to specialist equipment or to resort to criminality such as burglary, to gain access to data that is kept securely". This test should be periodically re-assessed to take into account new technologies and the public availability of data, as these factors will likely increase the risk of re-identification. See UK Information Commissioner's Office, "Anonymisation: Managing data protection risk code of practice", at pages 22-25, <https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>.

[16] Information and Privacy Commissioner of Ontario, "De-identification Guidelines for Structured Data", June 2016, <https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf>. PHIPA defines the "de-identification" of personal health information as to "remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual" (s. 2) (our emphasis). It should be noted that the notion of de-identification under PHIPA should not be confused with de-identification under the CPPA. Indeed, the standard formulated by PHIPA is one of anonymization, as illustrated by the French version of the Act which uses the term « *anonymiser* ». Thus, we note that Ontario has also included a notion of reasonableness in its definition of anonymized information. When interpreting the reasonableness of their anonymization techniques, organizations subject to PHIPA can rely on the Ontario IPC's "De-identification Guidelines for Structured Data" which provide a useful risk-based framework. Particularly, the Guidelines require organizations to determine an acceptable re-identification risk threshold for a specific dataset and to apply various privacy and security controls in order to reduce the risk below this threshold.

[17] For instance, section 2 (1) could be modified as follows: ***anonymize*** means to "irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that it is at all times reasonable to expect in the circumstances that no individual can be identified from the information, whether directly or indirectly, by any means."

4. Use of de-identified information for research, analysis, and development purposes.

Section 21 of the CPPA introduces a new consent exception for the use of de-identified information for "internal research, analysis and development purposes." This would enable an organization that holds a large volume of personal information about clients, employees or other individuals, to use this information, without knowledge or consent, for a broad range of innovative purposes, provided the information is "de-identified" beforehand. The addition of the term "analysis" in section 21 of the CPPA, which was not featured in the previous iteration of the CPPA under Bill C-11, is welcomed as it not only expands the scope of research activities covered by the consent exception, but also harmonizes the provision with its counterpart in the recently amended Québec Private Sector Act.

However, by using the term "internal" to qualify the meaning of "research, analysis and development", the CPPA seems to place a further limitation on the types of research activities that qualify for the exception, restricting its scope to activities that are pursued exclusively by and for the organization itself. Restricting the use of de-identified data to internal uses by the organization which collected the data may undermine the development of innovative research partnerships that allow various stakeholders to share datasets, subject to industry best practices around confidentiality, data security, and use restrictions (to name but a few), in order to create broad enough data substrates for the production of useful and actionable insights. More specifically, in a variety of industries including healthcare and others, the ability to produce industry-wide analytics depends on the ability of each industry actor to participate in data pooling models enabled by independent third-party analytics firms who provide syndicated data offerings that have been appropriately anonymized and aggregated so as to negate concerns over the sharing of competitively sensitive information between competitors. However, while it is possible for analytics firms to produce market-level analytics leveraging anonymized datasets within a data pooling model, the development of more insightful analytics is restricted to the extent that the same data pooling models are prevented from leveraging de-identified data.

In addition to the stifling effect which section 21 would have on research and innovation overall, it is also worth noting the risk it creates with respect to the development of unique anti-competitive market dynamics. More specifically, it is possible that the inherent differences between large organizations, on the one hand, and small and medium-sized enterprises ("**SMEs**"), on the other, will compound the drawbacks of section 21 in a way that results in a very uneven playing field with respect to access to research and analytics. Simply due to their size, SMEs tend to possess neither the resources nor the raw data to produce meaningful analytics and actionable evidence-based insights when acting alone. Without access to data pooling models, syndicated third-party data offerings, and research partnerships, they simply cannot hope to compete against the type of insights which large organizations will be able to draw from the vastly larger sample sizes reflected in their datasets, and will inevitably fall further behind. Similarly, by restricting each organization's research to the internal use of de-identified datasets which it already possesses, organizations will be inherently limited in their ability to explore advancements in new areas, further stifling innovation and prospection among both large and small enterprises alike.

To summarize, restricting the new consent exception for the use of de-identified data to internal uses by an organization may limit the collaboration and the fostering of research partnerships. These partnerships are crucial, as they allow stakeholders to share datasets to create data pools that are broad enough for the production of useful and actionable insights.

Section 21 could be reviewed to authorize the use and sharing of de-identified information amongst different organizations, subject to industry best practices regarding confidentiality, data security, and additional restrictions to adequately protect individuals (which may include specific contractual measures and a requirement to conduct a privacy impact assessment).

With respect to the "internal research, analysis and development" consent exception (CPPA, s. 21):

- **Recommendation #6.** Remove the qualifier "internal" at section 21, as this could place an undue limit on the scope of this consent exception.

***

C-27 represents an important step for Canada in modernizing its federal data protection law so that it is better adapted to the realities of the 21st century. Innovation and privacy can coexist, and the responsible use of personal information can be the cornerstone of building new and exciting technologies while respecting our fundamental rights. A number of suggestions were put forward in this submission with the hopes that they will be taken into account in the next version of C-27 to strike the right balance.

Interoperability concerns should also be considered when evaluating C-27. For example, s. 2(1) defines automated decision systems as "any technology that assists or replaces the judgment of human decision-makers," which is inconsistent with the Québec Private Sector Act which defines an automated decision system as one that is fully automated. The definition should be reviewed and harmonized with other privacy statutes by limiting its scope to fully automated systems.

Please note that the BLG privacy team members published earlier this year an article entitled "Consumer Privacy Protection Act (Canada's Bill C-27): Feedback from industry participants" in which a more complete list of operational challenges and concerns with C-27 are detailed. This article is available on BLG's website in both French and English.

We are hoping that these comments and suggestions will be helpful in studying the bill and look forward to reading the next version of C-27.

We remain at your disposal to discuss these suggestions at your convenience.

Eloïse Gratton
Partner and National Leader, Privacy and Data Protection
Borden Ladner Gervais LLP

Andy Nagy
Associate, Privacy and Data Protection
Borden Ladner Gervais LLP

Simon Du Perron
Associate, Privacy and Data Protection
Borden Ladner Gervais LLP