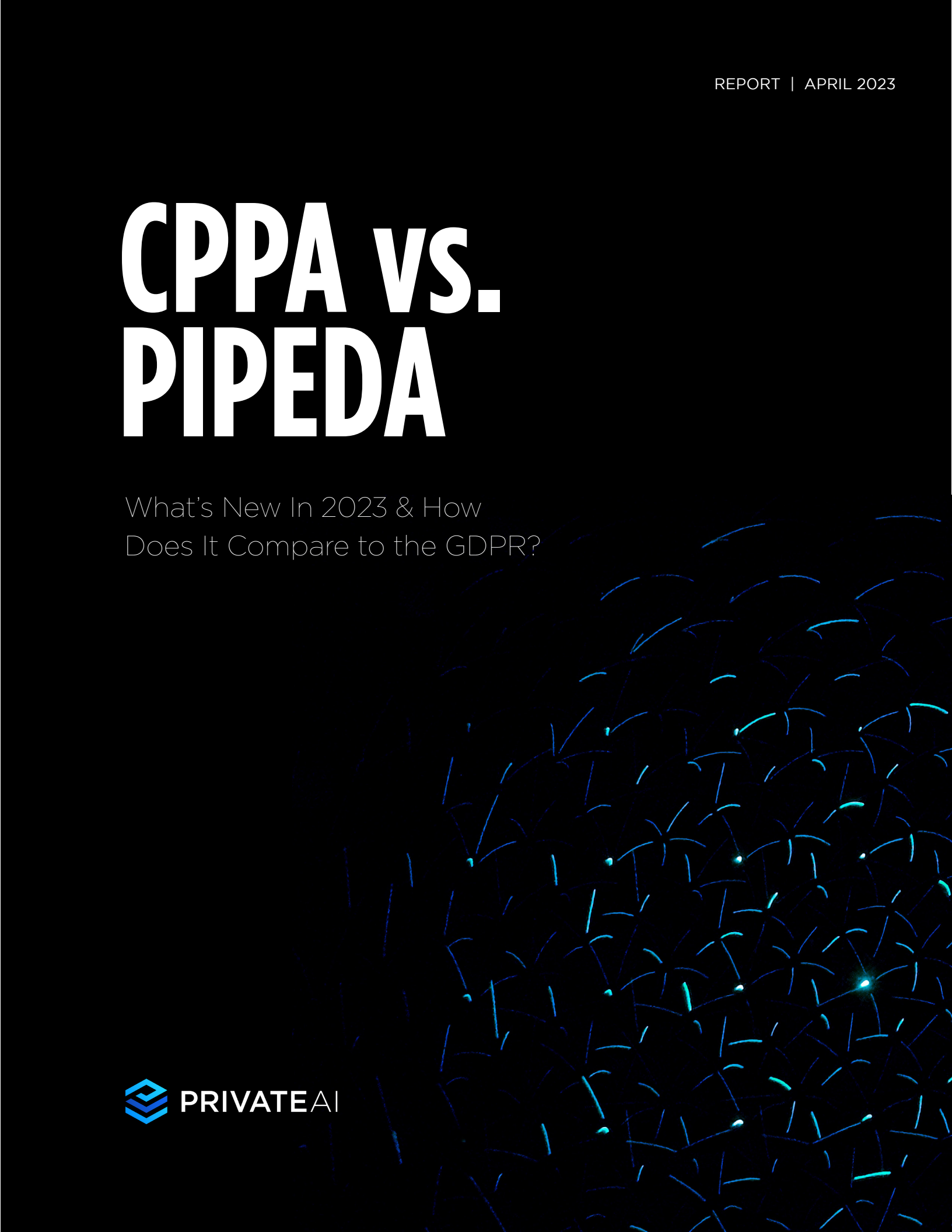
REPORT | APRIL 2023

CPPA vs. PIPEDA

What's New In 2023 & How Does It Compare to the GDPR?



PRIVATEAI

TABLE OF CONTENTS

ABOUT THE AUTHOR

Kathrin Gardhouse is the part-time Privacy Evangelist at Private AI. She also works at a Canadian Bank where she is responsible for the privacy program management. As a CIPP/C certified German- and Ontario-trained lawyer with credentials from TorontoMU in Cyber Security Policy she brings additional data privacy, legal, and compliance expertise to Private AI.

INTRODUCTION

In this report, we compare Canada's proposed Consumer Privacy Protection Act (CPPA) with the current privacy law, Canada's "Personal Information Protection and Electronic Documents Act" (PIPEDA). We focus on consent and the legitimate interest exception, anonymization and de-identification, protection of minors, the right to have one's data deleted, data portability, and new enforcement mechanisms.

PIPEDA came into force on January 1, 2001 as a response to rising concerns around privacy in light of the increasing capabilities of and use cases for information technologies. Domestic as well as international developments demanded legislative action to address and balance the often competing interests of businesses requiring access to data to drive innovation and individuals being concerned about losing control of their personal information.

To single out just one of many considerations, the EU's requirement of "adequate" privacy protection was introduced as a prerequisite for unfettered cross-border data flow. On December 20, 2001, the European Commission rendered its adequacy decision, permitting personal data to flow from the EU to Canada without any further safeguards, provided that the data recipients are subject to PIPEDA. This excludes recipients in Québec, for example, because the province had privacy legislation in place (Act Respecting the Protection of Personal Information in the Private Sector) that the EU did not recognize as adequate. This led to Quebec's recent enactment of Bill 64, now referred to as Law 25. However, even data recipients falling under PIPEDA can't simply rely on their current status to guarantee future access to European data. Because technological developments are ever evolving, and are potentially causing new threats to privacy, the European Commission revisits its adequacy decision every four years.

With the GDPR coming into force in 2018, the adequacy hurdle has been raised substantially in an effort to respond to the rapid developments in technology since the GDPR's predecessor was introduced in 1995 (Directive 95/46/EC). After all, two decades ago, the most sophisticated mobile app was Snake. Today, we are all obsessed with ChatGPT. It truly is a different world, and that world requires different data protection laws.

The Canadian federal government is attuned to the need to adequately protect the data privacy interests of Canadians and the business interests of Canadian organizations. In particular the latter would be jeopardized if Canada lost its adequacy status because it does not live up to the new EU legislation. Hence, Canada is currently making its second attempt to overhaul its private sector privacy law in the form of Bill C-27, the Digital Charter Implementation Act. Included as one of its three elements is the Consumer Privacy Protection Act (CPPA), which will replace part 1 of PIPEDA. The first attempt, Bill C-11, died on the order paper as the result of the federal election in 2021.

Let's dive in and look at some examples of how the CPPA strengthens privacy interests while still balancing the interests of businesses that want to use personal information to provide their services to Canadians.

CONSENT AND EXCEPTIONS

The general structure of the CPPA is in an important respect similar to PIPEDA; namely, insofar as consent is the default requirement for the collection, use, and disclosure of personal information. Consent is only optional under exceptional circumstances (s.15(1) CPPA). It was to be expected that this structure would persist, given that the CPPA plays an integral part in making good on the promises of Canada's Digital Charter, which, in turn, places significant emphasis on consent. The Digital Charter is a non-binding document by means of which the government signaled the future of its policies in the digital economy and data privacy protection in 2019.

There are issues with the centrality of consent, as a matter of principle and with specific consent exceptions provided for in the CPPA. First, obtaining consent is burdensome for the organization that needs to obtain it as well as for the individuals who are required to give consent to access the services they desire. For the consent to be valid, the individual must be advised of the purposes for and the manner of collecting, using, and disclosing the information, the reasonably foreseeable consequences of doing so, the specific type of personal information collected, used, and disclosed as well as the names or types of third parties to which the information may be disclosed (s. 15). As a result, a tension exists as businesses are struggling to formulate their privacy policies broadly enough to avoid having to ask for new consent every time data is collected, used, or disclosed for a new purpose – e.g., when introducing a new feature – and the requirement to make the policy terms concrete enough to provide individuals with meaningful information.

On the side of the individual, an equal tension exists. There is, at least for many, the wish to exercise autonomy over one's data and to be in the know over what happens to it. But then there is the onerous task of having to read complex privacy policies that are often left vague and do little to provide a solid basis for an informed decision. In the era of big data analytics and the internet of things putting data to uses that are beyond the grasp of the average individual, it cannot be expected of the individual to be accurately informed on what is being done with their data by whom. Furthermore, since accepting the policy's terms is a requirement for accessing the service the individual wants, having to check the box is too often treated as a mere nuisance that stands in the way of getting on with the sign-up process. It is therefore questionable whether consent should really be regarded as a meaningful safeguard for data privacy. In light of these considerations it seems to make sense to embark on a different path that intelligently supplements consent as the basis on which businesses can collect, use, and disclose information. The GDPR has once again shown the way by providing six legal grounds on the basis of which data may be processed, and consent is merely one of them. The others are contract performance, legal obligation, vital interests of individuals, public interest, and legitimate interest.

Despite the persistent centrality of consent, the CPPA seems to recognize these issues to some extent as it is making room for the non-consensual collection, use, and disclosure of data in circumstances that are similar to those captured in the other five legal grounds of the GDPR. The mechanism to achieve this in the CPPA is as an exception to the consent requirement. Some examples are s. 18(3), the legitimate interest exception to consent, s. 27, providing an exception in instances of fraud prevention,

detection, and suppression, and s. 28, allowing the disclosure of personal information if a debt is owed by the individual to the organization. Among these, legitimate interest is a new exception to the consent requirement that was not available under PIPEDA.

Making other considerations a standalone legal ground for the processing of data would, however, have the benefit that the consent requirement can be properly tightened to ensure it is actually a meaningful act, and in instances where the strict requirements cannot be met or cause too much friction, reliance on other grounds is permitted. Under the GDPR, then, implied consent is not a thing, consent must be a clear affirmative act, freely given, specific, informed, unambiguous, and easily withdrawable. Under the CPPA, the consent requirement is considerably less strict, and arguably proportionately less meaningful.

That being said, let's look at the legitimate interest exception to the consent requirement under the CPPA (s. 18(3)). This exception was introduced to Bill C-27 after feedback from the industry on Bill C-11 not being sufficiently flexible to meet business needs. The legitimate interest exception is curtailed by three requirements. First, the organization that wishes to rely on the exception has to establish that its legitimate interest outweighs any potential adverse effect on the individual. For this purpose, the potential adverse effects must be identified, and reasonable measures to reduce the likelihood of their occurrence and to mitigate their effects must be taken. Further requirements may also be introduced in the regulations under the CPPA.

Secondly, the legitimate interest requirement can only be relied upon for a business activity for which a reasonable person would expect the collection or use of their data. Lastly, the personal information must not be collected or used for the purpose of influencing the individual's behaviour or decisions.

There are problems with this way of framing the legitimate interest exception. From the perspective of the business, it is difficult to determine what may constitute a potential adverse effect, potentially deterring the organization from relying on the exception or at least causing uncertainty on how to ensure compliance with the act on this point.

Individuals, on the other hand, may feel that they are not sufficiently protected by the adverse impact provision. In light of a Québec Court of Appeal decision where the court found that the fear, anxiety, and annoyance caused by the loss of personal information is a normal inconvenience that comes with living in today's society, individuals may remain exposed to quite significant adverse effects against which they are unable to object or protect themselves. It remains to be seen how 'adverse effects' will be interpreted under the CPPA.

Similar lack of clarity remains, for now, with regard to when a reasonable person can be considered to expect the collection or use of their data in the course of an activity in which an organization has a legitimate interest. In addition, the breadth of the prohibition to collect or use the data to influence the individual's behaviour or decision is not very clear. Presumably, the provision intends to prevent harmful use of personal information but it may, on the face of it, capture any promotion, advertisement or recommendation, as such content has the potential of influencing behaviour and decisions; e.g., a recommendation about which movie to add to 'My List' on Netflix.

Compared to the GDPR, similarities are (1) the requirement to carefully assess whether a fundamental right of the data subject

overrides the legitimate interest, and (2) the fact that reasonable expectations need to be considered when making the legitimate interest determination. In contrast to the CPPA, the GDPR does not restrict the legitimate interest to activities that refrain from influencing the behaviour or decisions of individuals. In fact, marketing purposes are explicitly mentioned as an example of a legitimate interest activity.

DE-IDENTIFIED & ANONYMIZED PERSONAL INFORMATION

Just as the legitimate interest exception, the distinction between de-identification and anonymization is a novelty that did not exist in PIPEDA, and while anonymized data is mentioned, it is mentioned only once as an alternative to the deletion of data (clause 4.5.3). Anonymized data falls outside of the scope of the CPPA, which is the same under the GDPR. De-identified data, on the other hand, is considered personal information for most purposes under the CPPA, but organizations are permitted to use and disclose de-identified information somewhat more freely under certain circumstances.

De-identification is not a concept used in the GDPR, however, Article 11 implies a level of de-identification that is different from and less stringent compared to anonymization. If a data controller can demonstrate that it is not in a position to identify the data subject, the data controller need no longer comply with Articles 15 to 20, that is, the data subject has no right to access, rectify, erase, or restrict the processing of this data, and the right to portability of the data subject is also precluded. While this is not specifically spelled out in the GDPR, it seems reasonable to expect that the legal basis of 'legitimate interest' in the processing of personal data may be more readily available to data controllers if Article 11 data is at issue. This is because Article 6(1)(f) provides that the legitimate interest of the data controller to process personal data may be overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Arguably, these interests have less weight when Article 11 data is concerned.

Before we look at the use cases of de-identified data under the CPPA, let's get clarity on the definitions of de-identification and anonymization under the CPPA: "de-identify means to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains." Anonymize, on the other hand means "to irreversibly and permanently modify personal information, in accordance with generally accepted best practices, to ensure that no individual can be identified from the information, whether directly or indirectly, by any means."

In other words, stripping direct identifiers from the data suffices for the de-identification of the data in this context. It has been firmly established that even with only indirect identifiers, such as the approximate location, religious affiliation, and age, it is often possible to re-identify the individual to which the de-identified data pertains. Re-identification is therefore a risk one needs to keep in mind when examining the liberties organizations are allowed to take when personal information is de-identified before using or disclosing it. With regard to anonymized data, note that the proposed standard is very high and only few data will therefore fall outside of the scope of the CPPA, unless the requirements are softened by interpretation going forward.

De-identified data, then, can be shared without consent to facilitate proposed business transactions (s. 22(1)(a)). This is a gain in privacy protection compared to PIPEDA, which allows sharing personal information for this purpose without requiring de-identification. PIPEDA merely requires organizations to enter into an agreement that

sets out the protection of the data by appropriate safeguards, a requirement which remains in place in the CPPA. Under the CPPA, de-identification is not required in this context only if it would undermine the 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)).

De-identified data can also be disclosed to a limited set of organizations for socially beneficial purposes. These organizations include government, health care, and post-secondary educational institutions (s. 39). "Socially beneficial purpose means a purpose related to health, the provision or improvement of public amenities or infrastructure, the protection of the environment or any other prescribed purpose." It is worth flagging that the legislation does not require any additional safeguards to be put in place for the protection of the data thus disclosed. Note that under Bill C-11, the definition of de-identification was considerably stricter:

Definition of De-identify in Bill C-11:

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.

Definition of De-identify in CPPA:

To modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains.

Yet, the socially beneficial purpose exception to the consent requirement has not been changed from Bill C-11 to C-27, leading now to greater risks for individuals whose information is disclosed to the listed institutions.

A certain comfort may be found in the fact that organizations are prohibited from attempting to re-identify an individual using a de-identified data set except for limited purposes listed in the act (s. 128). The knowing violation of this provision constitutes an indictable offence and exposes the organization to a fine of max. $25 million or 5 percent of the global revenue in the financial year preceding the one in which the organization was sentenced. In case of a summary conviction, the cap is at $20 million or 4 percent of gross global revenue. It remains to be seen how this will affect research in re-identification risk. We've learnt a lot from researchers or journalists trying their hand at re-identification.

A further problem that arises from changing the definition of de-identify without changing other provisions of the act that refer to de-identification revolves around s. 74. This provision sets out how to de-identify personal information. It requires the organization to "ensure that any technical and administrative measures applied to the information are proportionate to the purpose for which the information is de-identified and the sensitivity of the personal information." It is unclear how measures can be taken proportionally to the sensitivity of the personal information if the definition of de-identify requires only one thing, namely stripping the direct identifiers from the data.

MINORS

Under PIPEDA, minors are not subjected to greater protection than anyone else. With the exception of a brief note saying that it may be impossible to obtain consent from minors, PIPEDA does not address the per-

sonal information of minors at all. Under the CPPA, the personal information of minors is considered sensitive information. Handling sensitive information places certain additional requirements onto organizations.

First, under s. 62(2)(e), organizations are required to make the retention period applicable to sensitive personal information they collect readily available to the individual to whom the information pertains, and they must do so in plain language.

Secondly, sensitivity of data is a factor organizations are required to consider when developing their privacy management system; when determining what a reasonable person would consider to be an appropriate purpose of the collection, use, or disclosure of personal information without which the collection is not permitted, regardless of consent (s.12(2)(a)); when determining whether reliance on implied consent is appropriate (s.15(5)); when determining what would be an appropriate safeguard when information is held, used, or disclosed (s.22(1)(b)(ii)); when determining for how long data should be retained (s.53(2)); and when determining whether a breach created a real risk of significant harm (s.58(8)(a)). Thirdly, with regard to the right of disposal, covered in greater detail below, minors have greater rights to request the deletion of their information (s. 55(2)).

With regard to consent and other rights and recourses under the act, the minor's representative may exercise them on behalf of the minor, unless the minor wishes to personally exercise those rights and recourses and is capable of doing so (s. 4(a)).

PORTABILITY

Under ss. 72 and 123, individuals now have the right to data portability. They can request an organization to transfer the data the organization has collected on the individual to another organization of their designation. Importantly, however, both organizations have to be subject to a data mobility framework, which the Governor in Council may establish by means of regulations under the act. Hence, we need to wait and see how this right will take shape in the future. One thing to note right now, however, is that the CPPA limits this right to the data that is collected by the organization and excludes data created by the organization as well as inferences that it drew from the data with regards to the individual. For example, if the collecting organization has run the individual's data through an automated decision system it developed, the new information that arises from such processing would not be subject to portability rights. However, the individual would at least have a right to access that information under s. 63, provided that the prediction, recommendation, or decision made by the system could have a significant impact on the individual.

DISPOSAL

Similar to PIPEDA, the CPPA limits the time period for which data may be retained to what is necessary to fulfill the purposes for which the data was collected, used, or disclosed, or to comply with the requirements under the CPPA, other legislation or reasonable contractual terms, e.g., to grant individuals access to their information (s. 53). As soon as feasible thereafter, the organization must dispose of the information. Alternatively, the information can be anonymized. The same obligation exists if the individual withdrew the consent for the collection, use, or disclosure and made a written request for this purpose, or if the information was collected, used, or disclosed in contravention of the act (s. 55(1)).

Several exceptions exist to the obligation to dispose of personal information (s.

55(2)). An interesting one applies in the situation where the organization has established an information retention policy according to which the information is scheduled to be disposed of and the organization informs the individual of the remaining time period for which the information will be retained. An exception to this exception is made if the information pertains to a minor. In that case, the organization is not entitled to refuse the disposal request.

ENFORCEMENT

PIPEDA has long been facing major criticism regarding the lack of enforcement powers the Office of the Privacy Commissioner has at its disposal. The CPPA remedies this but it also increases the complexity of the enforcement process to some extent. Where the Commissioner was only able to issue non-binding recommendations under PIPEDA, the CPPA toolkit now comprises of ordering powers to ensure compliance with the act as well as the ability to recommend to the new Personal Information and Data Protection Tribunal the imposition of administrative monetary penalties (AMP) up to 10 million dollars or 3 percent of the organization's gross global revenue for contraventions of the 14 provisions listed in s. 94(1).

Even higher fines can be imposed by the criminal courts for indictable offences and offences punishable by summary conviction. The CPPA expands on PIPEDA's list of these particularly serious contraventions. An organization is now committing an offence under the CPPA when knowingly:

	PIPEDA OFFENCE (S. 28)	CPPA OFFENCE (S. 128)
contravening a Commissioner's order		✓
obstructing the investigation, an inquiry or an audit of the Commissioner	✓	✓
failing to report a security breach	✓	✓
failing to retain records of security breaches	✓	✓
failing to keep information long enough to enable individual access to that information	✓	✓
attempting to re-identify individuals using de-identified information		✓
punishing employee whistleblowers	✓	✓

The fines for a committing an offence were increased from $100,000 for an indictable offence under PIPEDA to the higher of $25,000,000 or 5 percent of the annual gross global revenue under the CPPA (s. 128).

An important change to the enforcement regime lies in the introduction of a new tribunal entrusted with the enforcement of the act, the Personal Information and Data Protection Tribunal. It is to this tribunal that the Commissioner can recommend imposing AMPs after finding that an organization failed to comply with the act (s. 94). The organization can then appeal the Commissioner's decision to recommend an AMP. It can also appeal a compliance order (s. 101). If a compliance order is not appealed, or the appeal is dismissed, the order may be made an order of the Federal Court and is enforceable in the same manner as an order of that Court (s. 103(1)).

These increased review mechanisms are arguably required given that the monetary consequences for a contravention of the act are so much more significant now. It remains to be seen, however, how effective the enforcement of the act will be.

CONCLUSION

Overall, the CPPA as proposed as part of Bill C-27 makes great strides towards increasing privacy protection, in particular that of minors, while not losing sight of the needs of businesses, as can be gauged, for example, from the introduction of the legitimate interest exception to the consent requirement. It will be interesting to see, first, what the bill will look like when it comes out on the other end of the legislative process and, second, whether the EU Commission will consider Canada's federal private sector law to be granting adequate protection to privacy interests going forward. As we have seen, there remain considerable differences between the CPPA and the GDPR, including in the treatment of de-identified data.

One regrettable observation has been made which is worth echoing here. It is with regard to the CPPA's failure to expand its application generally to all information flowing from the EU to Canada. As is, an adequacy finding by the Commission would still only apply to those data recipients that are covered by the CPPA. Note that the CPPA has the same scope as PIPEDA, carving out the public sector to which the Privacy Act from 1985 (!!!) applies as well as organizations that fall under provincial privacy laws that have not yet obtained adequacy status.