Canadian Privacy Law Review

VOLUME 15, NUMBER 10 Cited as (2018), 15 C.P.L.R. SEPTEMBER 2018

• GOVERNMENT OF CANADA RESPONDS TO STANDING COMMITTEE REVIEW OF PIPEDA •

Amanda Branch, Associate, Bereskin & Parr LLP

Amanda Branch

The House of Commons Standing Committee on Access to Information, Privacy and Ethics (the "**Committee**") has been reviewing the *Personal Information Protection and Electronics Document Act* ("**PIPEDA**") since February 2017. Earlier this year, the Committee released its report titled "Towards Privacy by Design: Review of the *Personal Information Protection and Electronic Documents Act*" (the "**Report**") which outlined its recommendations for revising the legislation. The Government of Canada recently responded to the Report.

• In This Issue •

LexisNexis®

COMMITTEE REPORT

Throughout the year of review, the Committee held numerous public meetings and heard from many interested stakeholders, including the Privacy Commissioner of Canada, Daniel Therrien, who made recommendations to the Committee in four broad sub-groups: consent, reputation, the enforcement powers of the Office of the Privacy Commissioner of Canada (the "OPC") and the adequacy of PIPEDA.

The recommendations to update PIPEDA are heavily influenced by the European Union General Data Protection Regulation ("**GDPR**") which came into force in May of this year. Among the 19 recommendations were the following:

- Protecting personal information, particularly when posted online, as it can become permanent and can have a devastating impact on reputation. To that end, the Committee recommended PIPEDA include a framework for a right to erasure

CANADIAN PRIVACY LAW REVIEW

Canadian Privacy Law Review is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

ISBN 0-433-44417-7 (print) ISSN 1708-5446
ISBN 0-433-44650-1 (PDF) ISSN 1708-5454
ISBN 0-433-44418-5 (print & PDF)

Subscription rates: $325.00 per year (print or PDF)
$495.00 per year (print & PDF)

Please address all editorial inquiries to:

General Editor
Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

LexisNexis Canada Inc.
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: cplr@lexisnexis.ca
Web site: www.lexisnexis.ca

that, at a minimum, would provide young people with the right to have information posted online taken down either by themselves or through the organization;
- Creation of a framework for the right to de-indexing (the process of ensuring that the information no longer appears in the results of search engines), especially in the case of personal information posted online by individuals when they were minors;
- Inclusion of a right to data portability so that individuals can transfer their personal information between service providers so it could be reused; and
- The importance of "privacy by design" (which encourages a focus on privacy protection right from the design stage of services) and the recommendation PIPEDA be amended to make privacy by design a central principle.

Further, there were several recommendations relating to adequacy status in the context of the GDPR, including for the Government of Canada to work with its EU counterparts and determine what changes, if any, would need to be made in order to ensure PIPEDA maintains its adequacy status under the GDPR.

There was a focus on the issue of consent, including recommendations that consent be enhanced and clarified whenever possible to ensure users are giving meaningful consent and that opt-in consent be the default for any use of personal information for secondary purposes. Recognizing that young people are heavy users of information technology and are a particularly vulnerable group, the Report also encouraged the Government of Canada to consider implementing specific rules of consent for minors, as well as regulations governing the collection, use and disclosure of minors' personal information.

Finally, the Report recommended PIPEDA be amended to give the Privacy Commissioner enforcement powers, including the power to make orders and impose fines for non-compliance. At present, the OPC's enforcement tools include public interest disclosure, compliance agreements, and applying for a Federal Court hearing; however, the

OPC cannot make orders or impose fines. Several witnesses supported this power, noting it could serve to increase compliance, particularly among small and medium-sized enterprises, and it could create a body of precedents which could benefit the industry as a whole. Similarly, the Committee recommended that the Privacy Commissioner be granted broad audit or self-initiated investigation powers. This would allow the OPC to focus on areas where there are new and serious threats in the changing context of new technology and therefore not investigate every complaint.

GOVERNMENT OF CANADA RESPONSE

In a letter of response, Navedeep Bains, the Minister of Innovation, Science and Economic Development, acknowledged that the protection of privacy remains a fundamental value and concern for Canadians and noted that the Government of Canada shares the Committee's view that changes to Canada's privacy regime are required. The government plans to engage Canadians in a national conversation on data and digital issues with a view to exploring how Canada can lead and succeed in a data and digitally driven economy while ensuring continued respect for individual rights.

The Government of Canada addressed several recommendations, grouped in the same four themes: Consent, Online Reputation, Enforcement Powers of the Privacy Commissioner and Impact of the EU GDPR.

Consent

The government agreed with the Committee that consent should remain a core element of PIPEDA and the consent regime can be enhanced and clarified. The government is committed to maintaining PIPEDA's principles-based approach and is reluctant to make sector specific changes (e.g., such as the Committee's recommendation of expanding the scope of the existing exception to consent for the disclosure of personal information related to the prevention of activities related to financial crime).

The government stated that recent incidents involving unintended uses of personal information obtained from social media highlight the need to closely study the potential impact of redefining "publicly available" information. While the government recognized this issue is particularly critical as it relates to the personal information of minors, it also noted the challenges of applying explicit protections for minors under federal law as it inherently involves the definition of a minor, which falls within provincial jurisdiction.

Online Reputation and Respect for Privacy

The OPC published its Draft Position on Online Reputation earlier this year and took the position that PIPEDA already contains protection that is similar to the European right to be forgotten (or "right to erasure"). In its Report, the Committee recommended PIPEDA include a framework for a right to erasure.

The government's response acknowledged the work being done by the OPC; however, given the potential far-reaching impacts of a right to erasure and a right to de-indexing in numerous areas, including freedom of speech and the public record, and given that PIPEDA only applies to commercial contexts involving personal information, the government is of the view that it would need to assess whether PIPEDA would be the most appropriate statutory instrument to address these issues.

Enforcement Powers of the Privacy Commissioner

The government agrees with the Committee that it is time to examine how PIPEDA's enforcement model can be improved. To do so, the government must look at other models of compliance and enforcement and consider the potential impacts on the overall mandate of the OPC, the principles of fundamental justice and the countervailing risks associated with increased enforcement powers.

The government intends to undertake further study of the full range of options for ensuring compliance with PIPEDA.

Impact of the GDPR

The government supported the Committee's recommendations relating to maintaining Canada's adequacy status. Officials are working closely with the European Commission, with an adequacy review expected by 2020. The government noted that the EU has opted for the concept of "essential equivalence" in the GDPR to examine the adequacy of non-member regimes, rather than one-to-one mapping. As a result, it is not clear that PIPEDA must reflect each of the GDPR's rights and protections to maintain its adequacy standing.

CONCLUSION

The government will be engaging Canadians in a conversation about how to make Canada a more data savvy society, with a focus on how companies can gather, use and share personal information to innovate and compete while at the same time protecting privacy. The response from the Government of Canada is an interesting discussion of the issues, but gives little insight in to the comprehensive views of the government. It seems the Government of Canada may be prioritizing issues related to online reputation, enforcement powers of the OPC and the need to maintain Canada's adequacy status in light of the GDPR; however, it remains to be seen what modifications, if any, are made to PIPEDA.

[***Amanda Branch*** *is an associate at Bereskin & Parr LLP. See https://www.bereskinparr.com/ and https://www.bereskinparr.com/people/amanda-branch*.]

• CALIFORNIA'S NEW PRIVACY LAW AND WHAT IT MEANS FOR CANADIAN BUSINESSES •

François Joli-Coeur, Senior Associate, Borden Ladner Gervais LLP

François Joli-Coeur

The California legislature passed a new privacy law, which will come into effect on January 1, 2020.

On June 28, 2018, the California legislature passed a new privacy law, the *California Consumer Privacy Act of 2018* ("CCPA"), which will come into effect on January 1, 2020. The CCPA could impact Canadian organizations doing business in California, the world's fifth largest economy (with a larger population than Canada), even if they have no physical presence in the state and only conduct business online. This bulletin provides a high level comparison between this new Californian law and Canada's federal privacy statute, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA").

SCOPE OF THE CCPA

The law regulates organizations doing business in California and collecting personal information about California consumers (essentially defined as California residents) and households, which organizations either: have annual gross revenues in excess of U.S. $25 million; buy, receive, sell, or share the personal information of more than 50,000 California residents; or derives 50% or more of its annual revenues from selling California residents' personal information.

"Doing business in the state of California" is likely to be interpreted as covering businesses with no physical presence in California but offering products or services in this state through the Internet. As such, many Canadian businesses could find themselves subject to the CCPA.

COMPARISON WITH PIPEDA

While the CCPA and PIPEDA share some similarities, they are different in many ways. Compliance with PIPEDA will therefore not ensure compliance with the CCPA. To help Canadian organizations understand the similarities and differences with both statutes, below is a high level comparison of the CCPA and PIPEDA on a few important topics.

- **Definition of "personal information."** PIPEDA defines "personal information" as "information about an identifiable individual" (s. 2(1)). The CCPA defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The law also provides a long non-limitative list of "categories" of personal information. This list includes categories such as names and other identifiers, biometric information, geolocation data and "browsing history, search history and information regarding a consumer's interaction with an Internet Web site, application, or advertisement." The CCPA definition, while not identical to the definition of "personal information" under PIPEDA, is similar in the sense that it is also quite broad and also refers to information linked to a household which may relate to a small group of individuals (instead of a unique individual).
- **Transparency.** Under PIPEDA, organizations must be transparent about their practices pertaining to the collection, use and disclosure of personal information (Principle 4.3). The CCPA includes a similar requirement that organizations be transparent, at or before the point of collection, about the categories of personal information to be collected and the purposes for which the categories of personal information shall be used (s. 1798.100(b)).
- **Right to access personal information.** Under PIPEDA, individuals have a right to be informed of the existence, use, and disclosure of their personal information and shall be given access to that information (Principle 4.9). The CCPA grants Californians a similar right under which organizations must disclose, on request, the categories and specific pieces of personal information it has collected (s. 1798.100). If the organization "sells" (a term broadly defined as discussed below) personal information, the organization must disclose, on request, the source of the collection of the personal information, the business purposes for collecting such personal information, the categories of third parties with whom the organization shares this personal information and the specific pieces of personal information it has collected (s. 1798.115). It should be noted that unlike PIPEDA, the CCPA does not specify exceptions to this right of access, providing for reasons allowing organizations to refuse to grant such access.
- **Right to delete personal information.** Under PIPEDA, organizations may only retain personal information as long as necessary for the fulfilment of the purposes for which it was collected, and individuals may request the deletion of their personal information once such purposes have been fulfilled (Principle 4.5). The CCPA provides individuals with a general right to deletion of their personal information (s. 1798.105), which

could seem to be broader than the one provided by PIPEDA and appears more akin to the GDPR's "right to erasure." However, in practice, this right is subject to many exceptions, such as when the information is necessary to: (i) complete the transaction for which the personal information was collected; (ii) enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; or (iii) use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information. As such, it could arguably be considered quite similar to the one Canadians have under PIPEDA, especially in light of the recently proposed broad interpretation by the OPC in its Draft OPC Position on Online Reputation (see summary in bulletin). It should also be noted that the Canadian House of Commons' Standing Committee on Access to Information, Privacy and Ethics' ("ETHI") recent report recommended that that the European's right to erasure be adopted in Canada (see summary in previous bulletin and the Government of Canada's response in this bulletin). The CCPA and PIPEDA may therefore eventually be aligned on this right if such amendments come into effect, although the specific details pertaining to the respective statutes' rights to deletion could vary.

- **Right to portability.** The CCPA includes a right to data portability requiring organizations to provide consumers with their personal information in a portable and readily usable format allowing the consumer to transit the information to another entity, without hindrance (s. 1798.100(d)). PIPEDA does not include such a right, although the ETHI report discussed above has suggested that the Canadian government adopt it. This right is also included in the GDPR.
- **Consent.** PIPEDA is based on a consent model for the collection, use and disclosure of personal information (Principle 4.3). Consent may be express (opt-in) or implied (opt-out), depending on the type of information (i.e. sensitive or not) and the reasonable expectations of the individual who may withdraw their consent (Principle 4.3.8). The CCPA does not specifically rely on a consent model, but it grants Californians a right to opt out of having their data "sold" (s. 1798.120(a)). The term "sold," which is used throughout the CCPA, is defined to encompass more than its common meaning, as it includes releasing, disclosing, disseminating, making available, transferring, or otherwise communicating to a third party for monetary or other valuable consideration. It also requires that businesses provide a clear and conspicuous link on their website's homepage titled "Do Not Sell My Personal Information" leading to a page enabling consumers to opt out of the sale of their personal information (s. 1798.135).
- **Anti-discrimination.** Under PIPEDA, an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes (Principle 4.3.3). The CCAP incorporates a similar concept by restricting organizations' attempts to penalize consumers who exercise any right under the CCPA. It prohibits organizations to deny goods or services to such consumers (or charge different prices by offering discounts to those who do not opt out), or offer them different level or quality of goods or services, *unless it is reasonably related to the value the consumer's data provides to the consumer* (s. 1798.125). This requirement which seems to take into account free business models that may generate revenue from advertising is also aligned with the view articulated by the OPC in the CIPPIC v. Facebook finding that it was reasonable for a company offering a free social networking service to require that users consent to having their personal information used for advertising purposes as a condition of service. The CCPA incorporates another related concept (which has no explicit equivalent in PIPEDA) in allowing organizations to offer financial incentives to consumers for the collection or sale of their personal information,

with prior opt-in consent. Some commentators have noted that this concept could be in contradiction with the anti-discrimination principle.

- **Method of consumer request.** PIPEDA provides that organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information (Principle 4.10.2). While PIPEDA specifies that the complaint procedures must be "easily accessible and simple to use", it does not specify the method of communication that must be made available for individuals wishing to contact the organization. The CCPA (s. 1798.130) is more specific as it requires that organizations make available to consumers two or more designated methods for requests for information about their personal information, including, at a minimum, a toll-free number and a website (if the organization maintains a website).

ENFORCEMENT

While there have been suggestions to strengthen the OPC's enforcement powers in the recent ETHI report as well as the September 2017 OPC report, under PIPEDA, the OPC does not have the power to impose fines and individuals do not have a private right of action (although individuals may seek damages before the Federal Court after the OPC has issued a finding on their complaint).

In terms of enforcement, the CCPA provides for a private right of action, but only in the case of security breaches (s. 1798.150). This right may be exercised without proof of harm and statutory damages are set at no less than US $100 and no greater than US $750 per consumer per incident, or actual damages, whichever is greater. The other provisions of the statute are enforced by the Attorney General of the State of California, who can bring actions for civil penalties up to US $7,500 per intentional violation (s. 1798.155).

CONCLUSION AND BUSINESS TAKEAWAYS

It is likely that many Canadian organizations conducting business online will be subject to the CCPA if they collect personal information about California residents. These organizations should take note that complying with PIPEDA will not necessarily be sufficient to ensure compliance with the CCPA (and vice versa). Businesses collecting personal information from California residents must also bear in mind that the private right of action for data breaches includes statutory damages without proof of harm and that the California Attorney General has broader enforcement rights under the CCPA than the OPC has under PIPEDA.

Before modifying their business practices to ensure compliance with the CCPA, organizations should keep in mind that there are still many uncertainties pertaining to the scope and future interpretation of many of the CCPA's provisions. Moreover, the CCPA has already been criticized by commentators for having been adopted in a mere seven days and it has been described as being overly complicated, with a few drafting errors. It may therefore be amended before it comes into effect on January 1, 2020.

We will be closely following the developments of the CCPA and providing updates relevant to Canadian businesses.

[***François Joli-Coeur*** *is a senior associate in the Privacy and Data Protection practice group at Borden Ladner Gervais LLP. He advises and assists international and domestic clients from various sectors on a wide range of issues, including privacy and anti-spam, information technology, telecommunications (including CRTC regulatory requirements), advertising, marketing and sponsorship, consumer protection, cybersecurity issues and data breach management. François regularly deals with access to information requests and with the preparation of license agreements for clients from various industries. François has authored and contributed to various publications pertaining to privacy, technology and copyright law. He previously acted as associate editor for the Berkeley Technology Law Journal. He is co-author of the* Online Advertising and Linking *module of Lexis Practice Advisor Canada.*]