California’s New Privacy Law And What It Means For Canadian Businesses

July 16, 2018

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.

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749