CANADA/U.S. CROSS-BORDER BULLETIN:

How California Data Protection and Consumer Privacy Legislation Affects Canadian Businesses

By – Vincent Neil Ho, Jeremy Mutton (Student-at-Law)

Vincent Neil Ho, Associate
416.748.4764
vho@loonix.com

Vincent is a member of the firm's Corporate & Commercial practice group, advising Canadian and international business clients on a variety of regulatory compliance and transactional matters.

Loopstra Nixon LLP
Woodbine Place
135 Queen's Plate Drive
Suite 600, Toronto, Ontario
M9W 6V7
www.loopstranixon.com

It is clear that major data protection overhauls are here to stay. On June 28, 2018, California became the first US state to enact a comprehensive consumer privacy law when it enacted the *California Consumer Privacy Act of 2018* (CCPA). On July 1, 2020, the regulatory enforcement of the CCPA begins, following various amendments to the bill since it was first introduced. The California privacy law follows a similar law enacted in the European Union (EU) in 2016.

Canadian businesses operating in California that collect data, even if it is not located in California, will likely need to make changes if they meet the thresholds set out below. For example, a Canadian entity with gross revenues in excess of US$25 million that serves residents of California, with no physical presence in the state, will be subject to the application of the CCPA and the jurisdiction of the California Attorney General.

The most notable risks of noncompliance for Canadian businesses are monetary penalties imposed by the Attorney General of California and a civil right of action for data breaches not seen in Canadian data privacy legislation.[i] Further, the CCPA has a broad scope and does not limit its application to a specific industry.

Canadian businesses changed their data collection protocols to comply with the GDPR in Europe may still need to make changes to comply with the CCPA. Businesses that avoided compliance changes because they only operate in the North American market will likely need to make changes if they meet the thresholds set out below. Additionally, with these trends expected to continue, legislatures in North America will continue enacting privacy reforms and businesses which will likely require changes to their data protection and consumer privacy practices.

This article provides a summary and overview of the changes.

Key Takeaways

1. ***The CCPA has Extraterritorial Effects***. Over recent years, numerous privacy legislation in U.S. jurisdiction have been passed; however, the CCPA is exceptional in that it has a broad and potentially wide extraterritorial application. Just because a Canadian business is not located physically in California, does not mean it is exempt from the application of CCPA.

2. ***Compliance with GDPR may be Insufficient***. The CCPA contains specific obligations that may go beyond obligations businesses may use to comply with the EU's GDPR.

3. ***Severe Monetary Penalties***. The statutory monetary penalties for a security breach can be severe—and are a higher risk than those imposed under current legislation in Canada and the provinces.

4. ***Creation of New Private Right of Action***. The CCPA empowers consumers to launch a civil action to recover their damages from a data breach, or an amount between US$100 and US$750 per incident, whichever is greater. Paired with class action legislation, this could be a substantial risk for Canadian businesses that fail to prioritize data security.

5. ***Provides Right to be Forgotten***. The CCPA provides for those protected with a "right to be forgotten": businesses must delete a California consumer's personal information upon request.

Overview and Legislative History of the CCPA

In 2016, in response to public anxiety about data collection by companies and the sale to and use by third parties, the EU passed the General Data Protection Regulation (GDPR). The GDPR required changes to data collection policies of many businesses that operate in the EU, which took effect in May 2018.

In June 2018, the State of California followed suit by passing the CCPA. The CCPA imposes new data protection responsibilities on most large businesses operating in California, and grants residents in the state new rights relating to the access to, deletion of, and sharing of their personal information. It also empowers the Attorney General of California to adopt future rules and regulations to further the CCPA's purposes. The CCPA shares many similarities with the GDPR, such as the ability to request erasure of online information commonly referred to as the "right to be forgotten".

The CCPA came about in a way Canadians might find peculiar—it began as a ballot initiative launched by a private citizen, which would have resulted in a state constitutional amendment. In response, the California legislature negotiated with the sponsor of the ballot initiative, before hurriedly passing the bill to avoid the ballot initiative. Once the ballot initiative was removed (so that it would not be voted on by Californians at large) the legislature revised the law.

Who does the CCPA apply to?

One of the major differences between the GDPR and CCPA is in the scope of businesses captured by the law. While the GDPR applied to "data controllers" and "data processors", the CCPA applies to any for-profit entity doing business in California, that meets any one of the following requirements:

1. Gross revenues greater than US$25 million (to be adjusted for inflation);

2. Annually buys, receives, sells, or shares personal information of more than 50,000 consumers, households or devices for commercial purposes;

3. Derives 50 percent or more of its annual revenues from selling consumers' personal information.

The CCPA also applies to any entity that controls or is controlled by a business covered by the criteria above, or shares common branding with that business (including a shared name or trademark). The CCPA defines "selling" personal information very broadly, to include any communication or transfer of consumer's personal information to another third party for monetary or other valuable consideration.[ii]

Despite the differences with the EU law, if a business has already implemented measures to be compliant with GDPR, they will be in a relatively good position to comply with CCPA as well. If an Ontario or Canadian business or organization meets the criteria for CCPA to apply, the CCPA does not relieve the business from compliance with Canadian privacy legislation, such as the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA

applies to the collection, use and disclosure of personal information by any Ontario business that is not in the health care sector (which has its own data protection and privacy law).

Who and what is protected?

The law protects California residents, including those domiciled in California but currently outside the State for a temporary or transitory purpose.[iii] It protects those residents' personal information, which is defined as any information that directly or indirectly:

- Identifies, relates to, or describes a particular consumer or household; or,
- Is reasonably capable of being associated with or could reasonably be linked, to a particular consumer or household.

The statutory definition also includes specific information *categories* to which the CCPA applies, which include:

- identifiers;[iv]
- commercial information;[v]
- biometric information;
- internet information;[vi]
- geolocation data;
- inferences drawn from pre-existing data to create a consumer profile of preferences, characteristics, psychological trends, predispositions, behavior, intelligence, abilities, and aptitudes;
- professional or employment-related information;
- education information; and,
- audio, electronic, visual, thermal, olfactory, or similar information that can be reasonably linked to a particular consumer.[vii]

However, "personal information" does not include:

- Information lawfully made available from government records; and,
- Deidentified or aggregate consumer information.[viii]

Therefore, if a Canadian entity that meets the thresholds does business with a California resident, which requires the collection of any personal information as described above, it will likely be subject to the CCPA.

The scope of information captured is similar to the broad definition under PIPEDA, which defines personal information as including "any factual or subjective information, recorded or not, about an identifiable individual". Information will be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.[ix]

Information Rights/Privacy Notices

Before or at the time of collection, businesses must inform consumers about the categories of information collected and the intended use of the information, and a link to or online location for the business's privacy notice. If the business sells personal information, it must also provide a link to or online location for its Do Not Sell My Personal Information notice. For websites, this will take the form of an interactive pop-up menu.

Note that under the CCPA, a business that does not collect personal information directly from a consumer does not need to provide a notice at collection to the consumer, provided it does not sell the consumer's personal information.

Responding to Requests

On the consumer's request, organizations must provide specific information about the personal information collected about the consumer, sold to third parties or disclosed to a service provider. Businesses must also make available at least two methods for submitting requests, including a toll-free telephone number. However, where a business operates exclusively online and has a direct relationship with consumers, it may only provide an email address instead.

This is similar to PIPEDA, which gives individuals a right to access the personal information that an organization holds about them, and a right to challenge the accuracy and completeness of the information and have that information amended. There is a high bar for refusing access to "confidential commercial information" under PIPEDA.

Any Canadian businesses operating in California will be required to comply with California consumers' requests, or risk penalties for non-compliance as described below.

Opt-Out Right for Personal Information Sales

Businesses must include two opt-out submission methods, including an interactive form accessible online through a "Do Not Sell My Personal Information" or "Do Not Sell My Info" link in a clear and conspicuous location on its website or mobile application.[x] Businesses must not request reauthorization to sell a consumer's personal information for at least 12 months after the person opts-out, with some exception.

When consumers opt-out of the sale of their personal information, a business cannot refuse to provide goods or services to the consumer, apply different prices or rates for goods or services by way of discounts, benefits or penalties, provide lesser quality of goods or services, or suggest better prices or rates or better quality will be offered if the consumer consents.[xi]

There is currently no opt-out right under PIPEDA, but recent indication from the Government of Canada indicates that user control over what data is used for is likely coming to Canada.[xii]

Right to be Forgotten

CCPA grants California consumers deletion rights similar in principle to the "right to be forgotten" that GDPR granted to EU citizens.

PIPEDA currently does not give Canadian consumers rights of deletion or erasure. However, the Government of Canada has signalled that it is considering a move in this direction under its recent "Digital Charter".[xiii] Canadian businesses should not be surprised if deletion/erasure rights come to Canada soon.

Penalties (Civil Fines and Regulatory Action)

Under the CCPA, the Attorney General of California may impose fines of up to US$7,500 per intentional violation. In addition, a business can face a statutory penalty of up to US$2,500 per violation. In either situation, the Attorney General must provide notice to the business and a 30-day period to cure the violation.[xiv] These may appear minor in

the context of individual violations, but these civil penalties likely extend to each affected individual and could result in large aggregate fines.

PIPEDA, by contrast, contains two categories of offence based on their severity: summary offences carrying a penalty of a fine up to $10,000, and indictable offence carrying a penalty of a fine up to $100,000. The Attorney General of Canada has the discretionary power to qualify the contravention as either type of offence depending on the nature of the contravention.

Canadian businesses often must register a "foreign qualification" in the US states in which they operate or form a US corporate subsidiary. This will allow the California Attorney General (or consumers who are resident in California) to exercise jurisdiction over the US subsidiary or branch and sue it in a California court for breaching the CCPA.

Private Rights of Action

If a business suffers a data breach, private individuals in California have the right to launch a lawsuit without having to prove they've suffered harm. A data breach, as defined in the CCPA, occurs when non-encrypted or non-redacted personal information has been "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information".[xv]

Statutory damages are set between US$100 to US$750 per consumer per incident, or actual damages, whichever is greater. An individual may also seek injunctive or declaratory relief, and any other relief the court deems proper. Again, while the individual amount appears relatively small, paired with U.S. class action litigation, the risk to a business with a data breach affecting a substantial number of people becomes significant.

PIPEDA contains no private right of action – instead, it contains an onerous staged procedure where an individual may submit a complaint to the OPC. The OPC will issue a report. The complainant can then apply to the Federal Court within one year after the OPC's report is released for a hearing in respect of a matter that was the subject of the original complaint to the OPC or a matter that was referred to in the OPC's report, and is captured by obligations under PIPEDA. The Federal Court may do one or more of three things:

a) order an organization to correct its practices to comply with PIPEDA;

b) order an organization to publish a notice of corrective action outlining any action it has taken or intends to take to correct its practices; and/or

c) award damages to the complainant, "including damages for any humiliation that the complainant has suffered".[xvi]

This model does not fit easily with class action legislation in Ontario, making class action risk lower where there is not a substantial data breach.[xvii]

However, there are signs that the Canadian "ombudsman model" of data privacy enforcement and oversight is nearing its end. In its 2019 discussion paper *Strengthening Privacy for the Digital Age*, the Government of Canada stated that the PIPEDA enforcement regime is "outdated and does not incentivize compliance, especially when compared to the latest generation of privacy laws." The paper stated that the "current state of affairs cannot continue".[xviii] We expect that CCPA will only exacerbate the discrepancy, and near-future changes to PIPEDA to bring it more in line with CCPA and GDPR are likely.

Conclusion

Canadian businesses should take proactive measures to comply. Even if a multinational business enterprise managed to avoid the application of GDPR, it will likely be subject to CCPA if it operates within American markets. Every business

operating in American markets should evaluate whether CCPA might apply, and then consider putting in place compliance measures.

Even if the CCPA does not apply to a business, putting in place the practices to comply with CCPA may be a good habit, as similar legislative reforms may come to Canada in the future.

---

[i] By contrast, the federal data privacy legislation, *Personal Information Protection and Electronic Documents Act* (PIPEDA), provides for monetary penalties only in limited circumstances and are capped at $10,000 for summary offences, and $100,000 for indictable offences. Typically, summary offences are less serious than indictable offences.
[ii] CCPA, Cal. Civ. Code §1798.140(t)(1). Sale includes renting, disclosing, making personal information available, transferring, etc. There are narrow exceptions for some service providers, consumer requests, mergers and acquisitions, and to honour sale opt-out requests: §1798.140(t)(2).
[iii] CCPA, Cal Civ Code §1798.140(g). The GDPR is similarly broad; it protects European "data subjects", defined as identified or identifiable persons to which personal data relates.
[iv] For example, a real name, an alias, a postal address, an email address, a unique personal or online identifier, an IP address, an account name, a Social Security number, a driver's license or passport number, or another form of persistent or probabilistic identifier that can identify a particular consumer, family, or device.
[v] For example, records of personal property and other products acquired or services contracted, and other consuming tendencies.
[vi] For example, browsing and search history.
[vii] CCPA, Cal Civ Code §1798.140(o)(1).
[viii] CCPA, Cal Civ Code §1798.145. Note that the CCPA sets a high bar for a claim that data is deidentified or aggregated.
[ix] *Gordon v. Canada (Health)*, 2008 FC 258, at para 24.
[x] CCPA, Cal Civ Code §1798.135(a).
[xi] CCPA, Cal Civ Code §1798.125(a)(1).
[xii] Innovation, Science and Economic Development Canada, *Strengthening Privacy for the Digital Age — Proposals to modernize the Personal Information Protection and Electronic Documents Act*. This discussion paper is part of Canada's "Digital Charter" initiative.
[xiii] Innovation, Science and Economic Development Canada, *Strengthening Privacy for the Digital Age — Proposals to modernize the Personal Information Protection and Electronic Documents Act*: the Government is explicitly considering a policy option for "[p]roviding all individuals with the explicit right to request deletion of information about them that they provided, with some caveats." This would be a major expansion of existing rights of Canadians under PIPEDA, and corresponding compliance obligations on businesses.
[xiv] CCPA, Cal. Civ. Code §1798.155(b).
[xv] CCPA, Cal. Civ. Code §1798.150 (a).
[xvi] PIPEDA, s 16.
[xvii] See for example, *Condon v. Canada*, 2018 FC 522 where 583,000 individuals settled a PIPEDA class action for approximately $60 per person when financial and other information from student loan applications contained on an external hard drive was lost. In part due to PIPEDA's onerous structure, the risk of a class action for merely breaching PIPEDA is much more rare, but not zero: see for instance *Haikola v. The Personal Insurance Company*, 2019 ONSC 5982.
[xviii] Innovation, Science and Economic Development Canada, *Strengthening Privacy for the Digital Age — Proposals to modernize the Personal Information Protection and Electronic Documents Act*: "There is a growing view that the ombudsman model and enforcement of PIPEDA, which relies largely on recommendations, naming of organizations in the public interest, and recourse to the Federal Court, to effect compliance with privacy laws, is outdated and does not incentivize compliance, especially when compared to the latest generation of privacy laws. The current state of affairs cannot continue; meaningful but reasoned enforcement is required to ensure that there are real consequences when the law is not followed."