The California Consumer Privacy Act and its Impact on Canadian Businesses

Authors: Doug Tait

published 10/29/2019

The California Consumer Privacy Act (the "CCPA") establishes the rights of California consumers with respect to the collection, use, and disclosure of personal information. It comes into effect on January 1, 2020. Enforcement of the CCPA will begin 6 months after the publication of final regulations or on July 1, 2020, whichever is sooner.

Like the European General Data Protection Regulation, in certain circumstances, the CCPA can apply to businesses outside of California that collect, use, and disclose personal data on California consumers. This client alert examines the territorial reach of the CCPA, how your business may be affected, and next steps to consider to move towards compliance.

Who is considered a "consumer" under the CCPA?

A "consumer" is a California resident or individual domiciled in California who may be out of state for a "temporary or transitional" purpose.

What is the scope of the CCPA and how does it apply to for-profit businesses?

The CCPA applies to for-profit businesses that collect, use, and disclose personal information on California consumers, even if the businesses are not physically located or have employees in California, and that meet or exceed one of the following criteria:

1) have annual gross revenue more than $25 million;

2) buy, receive, sell, or share the personal information of more than 50,000 California consumers; or

3) derive at least 50% of annual revenue from selling California consumers' personal information.

If your business falls within one of the above categories then your business is “caught” by the CCPA.

What is the definition of personal information?

Under the CCPA, “personal information” is very broadly defined 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 definition hinges on any information that is “reasonably capable” of being associated with a consumer and may be available on any medium – not just information collected electronically.

Examples of personal information under the CCPA are quite exhaustive and include, but are not limited to, the following:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier internet protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers;
- Biometric information; and
- Internet browsing history.

In short, personal information is defined so broadly that it can, in theory, be any and all information associated with an individual. Thankfully, aggregated or de-identified data is not considered personal information.

What rights do California consumers have under the CCPA?

- Right to know what information is collected;
- Right to know what information has been shared (and with whom);
- Right to opt out of the sale of data;
- Right to request deletion of personal information; and
- Right to receive equal services, even if exercising privacy rights.

What are the penalties for non-compliance with the CCPA?

Generally, CCPA enforcement falls into two categories: enforcement by the Attorney General of California and action taken by private individuals.

Fines of up to US $7,500 per intentional violation may be imposed by the California Attorney General. In addition, a business can face a statutory penalty of up to US $2,500 per violation. Both are subject to notice being provided to the business and a 30 day opportunity for the business to cure a violation.

Where a data breach has occurred, private individuals have the right to launch an action

without proof of harm. By definition, a data breach 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" (See Section 1798.150 (a)). Data that is encrypted or redacted is not subject to the CCPA's private right of action.

In the context of a data breach, statutory damages are set between US $100 – $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.

What do you need to do to comply with the CCPA?

The following are some general steps you can take to move towards compliance with the CCPA:

- Conduct Data Mapping:
    - What personal information is collected and from whom?
    - Where is personal information stored?
    - How is personal information stored?
    - How long do we retain personal information and for what purpose?
    - With whom do we share personal information and why?
- Third Party Agreements:
    - Review all third party agreements and ensure they are compliant with the CCPA.
- Develop a process to respond to access and deletion requests.
- Develop and implement an employee training regime regarding the collection, use, disclosure, and protection of personal information.
- Develop or amend your Privacy Policy and/or other privacy notices.
- To minimize litigation liability, develop and implement:
    - Reasonable security practices (such as encryption and/or redaction);
    - Data breach response plan; and
    - Incident response plan.

The content of this client alert is for general information purposes only and is not intended to

constitute legal advice or a recommended course of action in a particular situation. This article is not intended to be, and should not be, relied upon by the reader in making decisions of a legal nature with respect to the issues discussed herein. Readers should consult with legal counsel before making any decision or taking any action concerning the matters in this article.

For further information, please contact Thompson Dorfman Sweatman LLP Privacy and Data Protection Practice Group Members:

B. Douglas Tait

Email | bdt@tdslaw.com

Phone | 204 934 2440
