Simpson Thacher

Memorandum

California Consumer Privacy Act Ready to Take Effect

October 17, 2019

The California Consumer Privacy Act ("CCPA") as amended on October 11, 2019, together with proposed supplemental regulations[1] issued on October 10, 2019, will take effect on January 1, 2020. This memorandum analyzes the CCPA with its new (mostly minor) amendments and explanatory regulations.

Scope of the CCPA

Who is covered? The CCPA applies to all businesses that "do business" (not defined) in California and (i) have at least $25 million in annual gross revenues; (ii) transact in the personal information ("PI") of at least 50,000 California residents; or (iii) obtain at least half of annual revenues from selling PI of California residents.

What activities are covered? A covered transaction of a California resident's PI includes any collection, sale (exchange for value), or disclosure of information that identifies, relates to, describes, or is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with such resident or its household. CCPA's coverage of PI is broader than the European Union's General Data Protection Regulation, as it includes biometrics, Internet browsing information, products purchased or considered for purchase and geolocation data, among others. PI does not include "publicly available information" (data from public government records) or data that is de-identified or aggregated.

What activities are excluded? The CCPA does not apply to (i) conduct taking place wholly outside of California; (ii) PI covered by HIPAA, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, federal driver privacy laws and certain state vehicle laws; (iii) PI collected for a single transaction with an individual; and (iv) conduct in compliance with applicable laws, among other exceptions. Additionally, the recent amendments exclude until Jan. 1, 2021 all PI collected about job applicants, individuals in the employee, director or contractor context or individuals in the transactional "due diligence" context.

Requirements of the CCPA

Under the CCPA (and these provisions cannot be waived by consumers), businesses must do the following:

i. When PI is collected, give consumers notice about what is collected and for what use (and of a consumer's opt-out rights, if PI is being sold). The regulations require consumer-friendly notices and prohibit non-disclosed uses of PI.

[1] The comment period for the proposed regulations runs until December 6, 2019.

ii. If a consumer requests, disclose at no charge within 45 days what specific PI has been collected and certain details about it. Businesses are required to conduct reasonable authentication of the requesting consumer, and the proposed regulations detail how to respond to such requests.

iii. If a consumer requests, subject to certain exceptions (e.g., transactional purposes, detection of security incidents, compliance with law), delete such consumer's PI within 45 days. The proposed regulations detail how to respond to such requests.

iv. Honor opt-out requests by consumers not to sell their PI. Businesses must offer two mechanisms for consumers to "opt-out," including as a link on a website or privacy policy or an offline method, for offline businesses (details in the proposed regulations). If a business wants to sell PI it did not collect directly from consumers, it must provide the consumer with opt-out notice or confirm that the intermediary collector provided such notice.

v. Obtain specified "opt in" consent before selling PI of children.

vi. Disclose consumers' CCPA rights in an online privacy policy or California-specific consumer rights statement, in consumer-friendly format (details in proposed regulations).

vii. If a consumer requests, provide the consumer's PI in a readily usable and portable format.

viii. Train all employees handling consumer PI inquiries and keep records of consumer requests.

ix. Do not discriminate against consumers (e.g., charge more to access a website) for exercising any of their CCPA rights, although businesses may offer consumers financial incentives (details in the proposed regulations) to collect or sell their PI, based upon its value.

x. Implement and maintain reasonable security procedures for the PI collected.

What Businesses Can Do Now

i. Know how and where your data are collected, processed and stored, so you can determine if and how CCPA applies to your business.

ii. Monitor your data vendors and ensure that your vendor agreements have adequate protections. Businesses can be liable for CCPA violations by a service provider if they know or had reason to know that the service provider intended to commit them.

iii. Set up a system to receive and respond promptly to user requests. Businesses must provide at least two methods (details in the proposed regulations) for consumers to make PI disclosure requests, including (i) a toll-free telephone number (or email in certain cases) and (ii) a website address, if applicable. Consider if additional infrastructure and personnel are necessary to process requests.

iv. Update your privacy policies. Businesses must put proper notices on their website privacy policies and/or home pages about consumers' rights under the CCPA.

v. Maintain reasonable data security procedures. This is already required under U.S. federal and state laws, but the CCPA has penalties for certain security breaches involving California residents' PI. Businesses should consider satisfying well-known standards such as ISO or NIST, to support a finding that they had "reasonable" procedures, if a breach later occurs.

Penalties Under the CCPA

The CCPA establishes a private right of action if a business suffers a security breach involving non-encrypted and non-redacted PI and did not have reasonable controls to protect the PI. Damages are the greater of (i) a range of $100-$750 per consumer per incident (regardless of actual harm) or (ii) actual damages, and injunctive and other court-ordered relief is also available. The California Attorney General can pursue all violations of the CCPA, with penalties of $2,500-$7,500 for each intentional violation.

For further information regarding this memorandum, please contact one of the following:

NEW YORK CITY

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Genevieve Dorment
+1-212-455-3605
genevieve.dorment@stblaw.com

Melanie D. Jolson
+1-212-455-3346
melanie.jolson@stblaw.com

Jonathan S. Kaplan
+1-212-455-3028
jonathan.kaplan@stblaw.com

Jacob Lundqvist
+1-212-455-3348
jacob.lundqvist@stblaw.com

Bobbie Burrows*
+1-212-455-2333
bobbie.burrows@stblaw.com
Not yet admitted

PALO ALTO

Harrison J. (Buzz) Frahn
+1-650-251-5065
hfrahn@stblaw.com

Jeffrey E. Ostrow
+1-650-251-5030
jostrow@stblaw.com

Marcela Robledo
+1-650-251-5027
mrobledo@stblaw.com

Corina McIntyre
+1-650-251-5703
corina.mcintyre@stblaw.com