The California Consumer Privacy Act of 2018

On June 28, 2018, the California Legislature passed AB 375, the California Consumer Privacy Act of 2018 ("CCPA"), which makes sweeping changes to California's data privacy laws and will have major compliance and litigation implications for most companies that have data on California consumers.

The CCPA imposes a series of new requirements on covered companies, including responding promptly to requests for information from consumers about how their data is collected, used, sold and disclosed; providing advance notice of data collection and how the data will be used; deleting consumers' data in many cases where the client submits a deletion request; and allowing consumers to opt out of having their information sold. The CCPA also creates a significant new statutory damages remedy for California consumers that may substantially increase liability for data breaches.

Background

The CCPA traveled at light speed through the California Legislature. Although the CCPA is being compared to the European General Data Protection Regulation ("GDPR"), which took four years to draft and negotiate, AB 375 made it through the Legislature in only seven working days and was signed by the Governor minutes after it had passed both chambers. The tech industry decided not to oppose the CCPA for fear that an even worse initiative would be passed by voters in November. That initiative had recently qualified for the November ballot, but its proponent offered to withdraw the initiative if AB 375 was passed and signed into law by June 28, 2018. Because the CCPA was passed as a bill, and not an initiative, the Legislature can amend the law with a simple majority rather the two-thirds majority that would be required to change a law enacted via initiative.

The CCPA's Scope

The CCPA's scope is broad. It applies to any for-profit entity that collects California consumers' personal information and that has annual gross revenues of $25 million or more; that buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers; *or* that derives 50 percent or more of its annual revenues from selling consumers' personal information.

The new law defines "personal information" much more broadly than is typical of state data breach notification statutes; it covers any data that identifies, relates to, describes, can be associated with, or can reasonably be linked to (directly or indirectly) a California consumer or household. The law excludes publicly available information from the definition of "personal information." But it limits the definition of "publicly available" to data that is available from federal, state or local government records. The CCPA's "personal information" definition specifically covers, but is not limited to, names, IP addresses, email addresses, sales records, browsing histories, as well as interactions with a web site, application or advertisement. The CCPA covers all personal information collected by a business, and expressly states that it is not limited to information collected over the Internet.

The CCPA's Duties

The CCPA's significant new duties include:

- Promptly responding to requests from individual consumers (which consumers can make twice in any 12-month period) that the company disclose the categories of data and specific pieces of data that the company has collected from that individual, the categories of sources from which the data is collected, the categories of third parties that the data has been disclosed or sold to, and for what business or commercial purpose. This information must be provided within 45 days of the request (subject to a 90-day extension where necessary), for free, and if provided electronically, in a portable and readily usable format (if technically feasible).

- Providing consumers with advance notice of data that the company will be collecting and the purpose for which it will be used.

- Limiting the use of data to the purposes for which it was collected unless the company provides notice of the new use.

- Subject to certain exceptions, deleting data about consumers, and instructing service providers to do the same, where the consumer submits a "request to be forgotten."

- Allowing consumers to opt out of having their data sold to others. Businesses may not request authorization from an opt-out consumer to sell the consumer's data until 12 months have passed from the date of the opt-out request.

- Not selling the personal information of minors without affirmative authorization from the child (if between the ages of 13-16) or the parent or guardian (for children under 13).

- Not discriminating based on price or the provision of goods or services against customers who exercise these rights unless the difference is "reasonably related to the value provided to the consumer by the consumer's data." (The CCPA also renders void and unenforceable contractual waivers of the law's duties).

- Updating website privacy policies to notify consumers of their rights under the CCPA; the categories of personal information the company has collected, disclosed or sold in the last 12 months; and information on how to opt out of having their data sold.

- Ensuring that employees responsible for privacy practices and compliance with the CCPA fully understand its requirements and how to inform consumers how to exercise their rights under the CCPA.

- Including a link on the company's homepage that is titled, "Do Not Sell My Personal Information," which links to a page that allows consumers to opt out of the sale of their personal information.

The law also places certain limits on third parties, such as restricting third parties who purchase personal information from another business from selling the data themselves without explicit notice and an opportunity to opt out.

The law will go into effect on January 1, 2020. Businesses have approximately 18 months to establish compliance structures. However, as businesses subject to the European GDPR learned, establishing the necessary compliance procedures is a multi-month process.

The CCPA's Exceptions

The CCPA contains numerous exceptions, the significance of which will vary by business and the context in which the information is being collected, used, disclosed or sold. The CCPA states that it shall not limit: compliance with other state laws or with federal or local laws, responding to subpoenas or regulatory inquiries, exercising or defending legal claims, or providing personal information as part of a privileged communication. The CCPA also does not apply to de-identified or aggregated consumer information, or to information covered by certain other privacy laws, such as HIPAA.

Key Litigation and Enforcement Provisions

The CCPA creates a statutory damages remedy that could significantly increase the potential liability for data breaches. Where a consumer's non-encrypted and non-redacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of a company failing to implement and maintain reasonable security procedures, consumers can recover up to $750 per consumer per incident *or* actual damages, *whichever is greater*. This would appear to open up a company with data on one million customers to damages liability of up to $750 million for a single breach.

Consumer plaintiff attorneys may attempt to argue that this statutory damages remedy is available even without an actual security breach and in cases where there is an intentional but unauthorized disclosure. But there are also strong arguments to be made that the statutory damages provision was not intended to address situations other than security breaches. Plaintiffs' attorneys may also seek to impose liability on a business for the misconduct of its service provider, although the CCPA limits liability in such instances to cases where the principal has actual knowledge or reason to believe that the service provider intended to commit the violation.

Before bringing a statutory damages claim under the CCPA, the consumer must give the potential defendant 30 days' notice and, if a cure is possible, an opportunity to cure. The consumer also must provide the Attorney General with 30 days' notice before filing a lawsuit, and the Attorney General can then choose to prosecute the action, refrain from doing so and allow the consumer to proceed, or notify the consumer that he or she may not proceed with the action.

The Attorney General also may seek a civil penalty of up to $7,500 for each intentional violation of the CCPA's provisions.

For further information, please feel free to contact:

Rosemarie T. Ring
Partner
(415) 512-4008
Rose.Ring@mto.com

Jonathan H. Blavin
Partner
(415) 512-4011
Jonathan.Blavin@mto.com

Grant A. Davis-Denny
Partner
(213) 683-9225
Grant.Davis-Denny@mto.com

Bryan H. Heckenlively
Partner
(415) 512-4015
Bryan.Heckenlively@mto.com

Nefi D. Acosta
Associate
(213) 683-9564
Nefi.Acosta@mto.com