THOMSON REUTERS

Westlaw®

Q&A: Privacy and security expert Christopher Ott on the California Consumer Privacy Act of 2018

By Jill Osterhaus

JULY 27, 2018

Privacy expert and attorney Christopher Ott of Davis Wright Tremaine LLP answers questions about the newly enacted California Consumer Privacy Act of 2018 — the most progressive and comprehensive consumer privacy law in the U.S. — which gives consumers unprecedented control over their personal data.

Thomson Reuters: What does the California Consumer Privacy Act require businesses to do?

Christopher Ott

Christopher Ott: Covered businesses will be required to notify consumers of their rights under the CCPA in their privacy policy, and for businesses that sell personal information, in addition to a website privacy policy, an opt-out page called "Do Not Sell My Information" will need to be developed and linked from the homepage of their website.

Additionally, businesses will need to provide consumers with access and deletion rights. A list of categories of personal information collected by the business, sold by the business or disclosed by the business for a business purpose will need to be provided.

Businesses must also be able to respond to a consumer's request for the disclosure of the specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of third parties with which the information is shared.

Businesses must be able to quickly disclose all this information and the purposes for which it is used. Most companies will need to perform a gap analysis to determine where their policies will need to change to cover the broader definitions of the CCPA and re-evaluate their data processing, storage and retention procedures to ensure they can comply with consumer requests.

TR: How did California end up passing the law so quickly?

CO: The CCPA flowed from the efforts of real estate investor Alastair Mactaggart. Mr. Mactaggart and two financial partners self-funded the drafting and submission of the California Privacy Ballot Initiative, which was set to be on the November 2018 general election ballot in California. Recent interest in online privacy issues helped the initiative to poll very favorably with the public, suggesting it would pass if on the ballot in November.

Due to the nature of the ballot initiative process in California, the initiative would have been very difficult to amend had it been approved, although it still had many problematic aspects. Mactaggart agreed to withdraw his privacy initiative from the general election ballot if California could enact a legislative replacement by the June 28 state deadline for removing it from the ballot.

As a result, California lawmakers introduced comprehensive privacy legislation June 22, and less than a week later, on June 28, the CCPA was passed and signed by the governor, just in the nick of time.

TR: Who does the law apply to? What businesses need to be concerned? Is it only businesses headquartered in California?

CO: The CCPA applies to for-profit entities that do business in the state of California (including any same-branded controlled or controlling company) that meet any one of the following three criteria: gross revenue of more than $25 million; receives or shares personal information for more than 50,000 "consumers, households or devices"; or receives more than 50 percent of its annual revenue from the sale of personal information.

This definition has a broader scope than one might initially think. Any business with a website, including a relatively small one, will likely collect personal information ("PI" as it is defined in the CCPA and which includes IP addresses, advertising and cookie IDs, and other device identifiers) from more than 50,000 consumers, households or devices that visit that website.

Certain other details about the definition of PI under the CCPA will greatly increase the number of records handled by even small businesses. For example, given that one consumer may have multiple devices, the number of devices that contain personal information defined by the CCPA will quickly multiply under the second qualifier above.

Similarly, many "free" websites that rely on advertising revenues, such as a lifestyle blogger's site, will be subject to the law. Moreover, because the definition of "consumer" is not limited to individuals with whom a business engages in an arm's-length transaction, employee data will also likely be included.

There are some narrow exceptions to the applicability of the CCPA (e.g., Health Insurance Portability and Accountability Act and Gramm-Leach-Bliley Act), but those exceptions relate to the information covered pursuant to those statutes, not the entities themselves.

The CCPA also provides other exceptions to allow businesses to comply with other state and federal laws, respond to valid legal requests, exercise or defend against legal claims, and the like. However, those exceptions do not change the fact that even very small businesses that have any online presence in California will likely be covered by the CCPA.

TR: What type of information does the law apply to? Are the examples of personal information included in the law similar to other definitions of personal information in data breach notification or data security laws?

CO: The CCPA applies to broadly defined personal information of California residents collected by businesses, regardless of how the collection is done, or the type of industry in which the business operates.

While most U.S. breach notification laws only consider information "personal" if it contains a name plus other "sensitive" information, such as a Social Security number or financial account information, the CCPA extends to all 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," including name, email address, biometric information, unique identifiers and IP addresses.

This is the first instance of non-individualized data belonging to a group of people being legally treated as PI. Further complicating matters, the term "household" is not defined by the CCPA. Many other privacy laws apply to "personally identifiable information," which courts have interpreted to be information that can readily identify a specific person.

The CCPA's definition goes far beyond that interpretation, as most entities cannot, on their own, use an IP address or a device identifier to identify a specific person.

TR: The effective date is Jan. 1, 2020. Will that be the date when businesses can start expecting enforcement actions? Should they begin preparing before that date?

CO: On Jan. 1, 2020, businesses must be compliant with the CCPA. Enforcement actions will await those who fail to prepare. Many aspects of compliance will require thoughtful changes by businesses, including data mapping, changes to privacy policies, training personnel to respond to requests, amending agreements with service providers, etc. Businesses should start to consider those changes immediately and plan to finish their changes by New Year's Day 2020.

The California attorney general is tasked with general enforcement but must give a business a 30-day period to cure a violation before bringing an action. Civil penalties in an AG action can be up to $7,500 for each violation, and any assessed penalties are divided between the jurisdiction on whose behalf the action was brought and a new Consumer Privacy Fund, which is created by the act to offset the costs of enforcement.

This does not mean that the CCPA will be completely unchanged in 2020. Given the rushed nature of the legislation, it is likely that some amendments will pass before the CCPA's effective date. Regardless of potential amendments or legal challenges that may arise in the coming 18 months, much of the CCPA is likely to remain in effect. Businesses should consider what they need to do to comply immediately and begin fashioning implementation plans.

TR: What type of regulations do you foresee the attorney general adopting under the law?

CO: While there are many issues that would call for regulatory guidance from the attorney general, there are several places where anticipated regulations are explicitly called out in the statute. For instance, the attorney general will likely issue regulations on how a consumer will delegate authority to another person to opt out of the sale of the consumer's PI, and what constitutes a "verifiable consumer request" as defined under the CCPA.

Section 1798.185 of the law provides a nonexclusive list of areas in which the "attorney general shall solicit broad public participation to adopt regulations." A few examples include: additional categories of data that may need to be included due to changes in technology and data collection practices or obstacles with implementation; updates to definitions such as "unique identifier," which inevitably will change with the development of technology and data collection; and establishing rules around required notices to consumers such that they be understandable by an average person and provide for additional accommodations required by law.

TR: How will the Consumer Privacy Fund work? Are there any similar funds in the state or elsewhere around the globe?

CO: The Consumer Privacy Fund will be financed at least in part by civil penalty or settlement monies. The act expressly sets out that 20 percent of any civil penalty or settlement monies collected from actions brought by the attorney general will be allocated to the fund (which will be part of the General Fund) with the intention of fully offsetting the costs incurred by state courts and the attorney general in connection with this law.

It is not uncommon for enforcement authorities to have specific guidelines or procedures for distributing fees collected from successful enforcement actions. It is also not uncommon for funds collected in a successful government action to be used to offset the expenses incurred through the government's investigation or litigation of the matter.

However, using this fund to offset privacy injuries to individuals would be different. It is possible that aspects of the fund could resemble the federal crime-victim fund used under the federal Mandatory Victims Restitution Act.

TR: Do you foresee an uptick in privacy litigation caused by the CCPA?

CO: The act provides a private right of action only relating to "certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information," as defined in the state's breach notification law, if the business failed "to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

In such a case, the consumer may bring an action to recover damages of no less than $100 and up to $750 per incident, or actual damages, whichever is greater. If you consider the fact that a breach notification was sent to the California attorney general's office almost every day during the month of June and assume that only 1 percent of California residents were affected (395,000), total liability at the low end of the range would be almost $40 million. I would say that's incentive for plaintiffs' attorneys.

The statute also directs the court to consider certain factors when assessing the amount of statutory damages, including the nature, seriousness, persistence and willfulness of the defendant's misconduct; the number of violations; the length of time over which the misconduct occurred; and the defendant's assets, liabilities and net worth.

There is some right to cure violations. Prior to initiating any action against a business for statutory damages, a consumer must provide the business with 30 days' written notice of the consumer's allegations and, if within the 30 days the business cures the alleged violation and provides an express written statement that the violations have been cured, the consumer may not initiate an action for individual statutory damages or class-wide statutory damages.

These limitations do not apply to actions initiated solely for actual pecuniary damages suffered because of the alleged violation. That said, it is difficult to understand how a breach, as defined in the CCPA, could be cured after the fact.

TR: The law allows any business or third party to seek the attorney general's opinion for guidance on how to comply. Do you foresee businesses taking advantage of this provision?

CO: The CCPA, as presently drafted, is still unclear in its articulation of several requirements. While it is not yet clear how many amendments to this law will be made, if any, before its effective date on Jan. 1, 2020, we can expect that, with so many drafting inconsistencies, companies will not be timid about seeking guidance from the attorney general.

TR: Do you anticipate that the CCPA will compel other states or the federal government to enact similar laws?

CO: As with many other laws in the privacy space — such as those that relate to data breach notification, disclosures for online privacy policies and student privacy rules — California will likely be setting a trend once again.

Assembly member Ed Chau, who was one of the bill drafters and is the leader of the California Assembly's Privacy Committee, has publicly stated that he believes this law will "forge[] a path forward to lead the nation once again on privacy and consumer protection issues." As far as federal legislation, it would not be surprising if there was at least an attempt at passing similar legislation that would set a national standard and preempt California's law.

This article first appeared in the July 27, 2018, edition of Westlaw Journal Computer & Internet.