Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

California Passes Landmark Consumer Privacy CCPA—What it Means for Businesses

July 9, 2018

Key Points

- California recently passed the landmark California Consumer Privacy Act that goes into effect in 2020, which grants California residents new privacy rights.
- The CCPA creates a private right of action for California residents and grants new enforcement power to the Attorney General with high damages recoverable.
- Hastily passed by the Legislature after only a week of debate, the CCPA contains provisions that require further clarification and that may prompt additional revisions.

I. Background

On June 28, 2018, Governor Brown signed into law one of the strictest and farthest-reaching consumer privacy laws in the country, the California Consumer Privacy Act of 2018 (the "CCPA"). (*See* AB-375.) The CCPA is a response to a growing concern that consumers need stronger means to protect their personal information in light of, among other things, recent data breaches and related privacy incidents that have affected millions of Americans (*e.g.*, Target, Equifax and Cambridge Analytica). The CCPA imposes a range of new requirements on businesses to further its goal of ensuring that consumers enjoy choice and transparency in the treatment of their personal information.

The hastily-passed CCPA is part of a deal brokered by the Legislature and Governor Brown to avert a costly fight over a proposed ballot initiative championed by privacy activists that would have put even more stringent measures before voters this November. Legislators and the proponents of the ballot initiative reached an agreement whereby the proponents would remove the initiative from the ballot if the CCPA was signed into law by the deadline for such removal.

The CCPA grants California residents the right: (1) to know what personal information is being collected about them; (2) to know whether their personal information is sold or otherwise disclosed and to whom; (3) to say no to the sale of their personal

Contact

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco/Abu Dhabi
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Dario J. Frommer
Partner
dfrommer@akingump.com
Los Angeles
+1 213.254.1270

Hyongsoon Kim
Partner
kimh@akingump.com
Irvine
+1 949.885.4218

Anthony T. Pierce
Partner
apierce@akingump.com
Washington, D.C.
+1 202.887.4411

Jo-Ellyn Sakowitz Klein
Senior Counsel
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

Diana E. Schaffner
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

information; (4) to access their personal information and request deletion under certain circumstances; and (5) to receive equal service and price, even if they exercise their privacy rights.

It also creates a private right of action for California residents if their unencrypted or unredacted personal information is subject to certain security incidents as a result of a business's failure to implement reasonable security. Plaintiffs may seek the greater of their actual damages or set damages of between $100 and $750 per consumer per incident. The CCPA also empowers the Attorney General to pursue cases against businesses for damages of up to $7,500 per violation for intentional violations.

There is already talk about amending the CCPA to revise and clarify certain provisions. Businesses should carefully monitor future amendments to the law and the adoption of corresponding regulations, which will likely affect the CCPA's impact on day-to-day business.

II. Key Provisions

A. Whose Information is Regulated?

The CCPA places restrictions on certain businesses as a means of protecting consumers' personal information. Importantly, "consumer" for the purposes of the CCPA means any natural person who is a resident of California as "resident" is defined in tax provisions. Thus, under this broad definition, "consumer" includes: (1) every individual who is in California for other than a temporary or transitory purpose, and (2) every individual who is domiciled in California who is outside of California for a temporary or transitory purpose. Given this definition, the CCPA may arguably apply to covered entities that process even a single California resident's personal information no matter where that entity is located.

B. What Information is Regulated?

The CCPA expands the definition of "personal information" to include any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with a particular consumer or household. This includes information like a consumer's name, postal address, social security number, education information, inferences drawn to create a profile about the consumer, consumer preferences, etc. The definition both encompasses and is broader than the definition of "personal information" used in California's data breach statute. For example, it includes biometric information (*e.g.*, imagery of the fingerprint, face, palm, etc.) collected without a consumer's knowledge.

Businesses may find that they collect information that may be considered sensitive under the CCPA even though other regulations or statutes may not classify it as such. The CCPA, moreover, contemplates that the Attorney General will adopt regulations to revise various subcomponents of the definition of personal information that, depending on the regulation adopted, could further expand the definition beyond its already broad terms. Because of the breadth of this definition, businesses in California and beyond that previously did not consider themselves to be maintaining regulated personal information may find that this is no longer the case once the CCPA takes effect, even if their data practices have not changed.

Notably, certain categories of information are apparently excluded from the reach of the Act, including: (1) publicly available information, which appears to generally mean information that is lawfully made available from government records; (2) deidentified information, which means information that cannot reasonably identify, relate to, describe, etc. a particular consumer provided the businesses takes certain safeguards (*e.g.*, protect against reidentification); and (3) aggregate consumer information, which means information that relates to a group or category of consumers from which individual consumer identities have been removed and that is not linked or reasonably linkable to a particular consumer or household. Information is not considered to be publicly available if it is used for a purpose other than the purpose for which it is maintained and made available in government records, or for which it is publicly maintained. The sections of the CCPA discussing deidentified and aggregate consumer information are somewhat opaque and businesses relying upon information in these categories should further explore the applicability of the CCPA to some uses of these types of information.

C. What Entities are Regulated?

The CCPA governs businesses (meaning for-profit entities) that (1) collect consumers' personal information, or on whose behalf such information is collected, and that determine the purposes and means of processing that information, and that (2) meet one of three criteria: (a) have annual gross revenue above $25 million; (b) alone or in combination annually buy, receive for commercial purposes, sell, etc. the personal information of 50,000 or more consumers, households, or devices; or (c) derive 50 percent or more of its annual revenue from selling consumers' personal information. Entities that either control or are controlled by such businesses are also covered by the Act. Commercial conduct that takes place wholly outside of California is not covered by the Act.

The CCPA also places restrictions on how a business should share consumers' personal information with its service providers as well as with third parties. "Service provider" means a for-profit entity that processes information on behalf of a business and to which the business discloses consumers' personal information for a business purpose pursuant to a written contract. Such contract must prohibit the service provider from, among other things, selling, retaining, using, or disclosing the personal information it receives for any commercial purpose other than the services specific in that contract. Any entity that is not a business or a service provider – as those terms are defined in the CCPA – is considered a third party. The CCPA treats service providers and third parties differently in a number of ways, including that it: (1) limits a business's liability for service provider misconduct if certain conditions are met (*see infra* Section L), but does not offer the same protection when a business sells, share, or discloses personal information to third parties; and (2) limits a business's ability to sell, share, or disclose consumers' personal information to third parties without providing consumers prior notice and the option to opt out of the sale (*see infra* Sections D and G(2)), but does not place the same requirements on sharing information with service providers.

The collection and use of consumers' personal information by California state and local government entities is **not** covered by the Act. This omission has been soundly criticized by privacy advocates and marks a departure from other privacy-focused

statutes. There is already discussion of passing additional legislation during the next session to apply similar controls to California government entities.

D. What Notices and Disclosures Must be Provided to Consumers?

Businesses are required to provide consumers certain notices and disclosures in materials posted on their websites and through other means. This includes notice of: (1) at or before the point of collection, the categories of personal information the business collects about consumers and the purposes for which they will be used; (2) consumers' rights to request that the business delete their personal information; and (3) if the business intends to sell personal information to third parties, consumers' right to opt out from that sale. In addition, businesses have to include in their online privacy policies, in California-specific descriptions of rights online, or in their websites generally information to help consumers understand and exercise their rights, including a description of consumers' rights under the CCPA (*e.g.*, to request information on what personal information has been collected, sold or disclosed about them, to have such information deleted, or to opt out of the sale of information, etc.), how to submit related requests, and lists of the categories of personal information the business has collected, sold and disclosed about consumers generally in the prior 12-month period.

E. What Information Must be Provided to Consumers Upon Request?

Consumers have a right to request and receive (if they provide a verifiable request) the following information from businesses: (1) the categories and specific pieces of personal information the business has collected about the consumer; (2) the categories of sources from which the personal information is collected; (3) the business purposes for which the personal information is collected; (4) the categories of third parties with whom the business shares consumers' personal information; and (5) the categories of personal information that the business sold or disclosed about the consumer for a business purpose. Subject to certain potential extensions, businesses have to respond to consumers' requests within 45 days. The response must cover the 12-month period prior to the consumer's request and include the required information in a transferrable format if provided electronically. In effect, businesses should be prepared operationally by December 31, 2019 (the day before the CCPA takes effect) to practically respond to consumer requests, which requires tracking the collection of personal information, as well as tracking the sources of information and any third parties that receive the information.

The CCPA does not specify whether businesses will be expected to provide information for the 12 months preceding the date the Act takes effect (January 1, 2020), or if the requirement to track and provide the various categories of covered information begins as of that date. Until this point is clarified, businesses may need to be prepared operationally as of January 1, 2019 (12 months before the CCPA takes effect) to track the various categories of information that they may need to practically respond to consumer requests as of January 1, 2020. This is yet another issue that should be clarified before the CCPA goes into force.

There are certain qualifiers that suggest the actual information that need be provided to consumers under the CCPA is more limited than may appear upon first reading. Businesses are only required to provide the "categories" of sources from which personal information is collected or the categories of third parties with which personal information is shared. It appears business could respond to consumer requests for information on these points with a general list, rather than with information specific to the particular consumer making the request. An exception to this is the requirement that businesses inform consumers of both the categories and specific pieces of personal information it has collected about the requesting consumer. Even then, the CCPA is not clear what is meant by "specific pieces" of information. It may be sufficient for a businesses to inform the consumer which of its general list of categories of personal information it actually collected about the consumer, rather than provide the consumer all of the personal information collected about the consumer in the prior 12-month period.

F. Are There Limits on a Business's Obligation to Respond to Requests?

The CCPA includes a few protections for businesses in the form of limitations on the number of responses that have to be provided to consumers within a single year (two responses per year only are required), potential extensions of the time to respond to consumer requests (can be extended by an additional 90 days), and the possibility of refusing to CCPA on requests or charging a reasonable fee where requests are unfounded or excessive. With regard to the last point, businesses bear the burden of demonstrating that the requests were unfounded or excessive should they refuse to respond or charge a fee for this reason.

G. What Rights Does a Consumer Have Beyond Requesting Information?

1. The Right to Delete Personal Information

A consumer has a right to request that a business delete his or her personal information from its records and direct any service providers to do the same. Businesses must comply with verifiable consumer requests. The CCPA does not specify how information is to be deleted or provide a specific means of testing the proper outcome.

There are nine exemptions to the deletion requirement that permit a business to avoid deleting a consumer's personal information, including: (1) to complete the transaction or service for which the information was collected; (2) to detect security incidents, protect against malicious, deceptive/fraudulent, or illegal activity, or prosecute those responsible for that activity; (3) to debug or identify errors; (4) to exercise free speech; (5) to comply with certain sections of the California Electronic Communications Privacy Act; (6) to engage in certain types of research if the consumer has provided informed consent; (7) to enable solely internal uses that are reasonably aligned with the consumer's expectations (based on his or her relationship with the business); (8) to comply with legal obligations; or (9) to use internally in a lawful manner consistent with the context in which the information was provided. The breadth of these exemptions suggests the right to delete may be fairly limited in certain circumstances, although even a limited deletion right could present material challenges for businesses.

Although akin to the GDPR's "right to erasure," California's "right to delete" appears to be narrower in application. Under the GDPR, personal data must be erased immediately as long as the data are no longer needed for their original processing purpose, the impacted person has withdrawn his or her consent and there is no other reason for justification, the impacted person has objected and there is no preferential justified reason for the processing, or erasure is required to fulfill a statutory obligation under EU law or the right of the Member States. The GDPR, as with the Act, does not specify how data should be erased in individual cases. The key result is that it is no longer possible to see the data without disproportionate expense.

2. The Right to Opt Out of the Sale of Personal Information

Consumers must be provided the option to opt out of the sale of their personal information to third parties at any time. Once consumers have opted out, their information cannot be sold unless they later provide authorization. The CCPA restricts businesses from requesting reauthorization from a consumer for 12 months after the consumer opts out. The right to opt out only covers the sale of personal information to third parties.

To facilitate the opt-out process, businesses are required to provide a "Do Not Sell My Personal Information" link on their websites' homepages that link to a form enabling consumers to opt out of the sale of their personal information and providing related information. Consumers must be permitted to opt out of the sale of their data without creating an account with the business. The CCPA also contemplates the eventual development of a standard "Do Not Sell My Personal Information" link that will have a similar appearance and function across different entities. Development of that common icon will take place sometime in the future.

There are special authorization or "opt-in" rights provided to minors. Businesses may not sell the personal information of a consumer if they have "actual knowledge" that the consumer is younger than 16 and have not received specific authorization. Children age 13 to 16 can provide authorization for the sale of their own personal information, while only the guardians of children under 13 can provide such authorization. Businesses that "willfully disregard" a child's age will be considered to have "actual knowledge" of the child's age. The CCPA does not provide guidance on what constitutes "willful disregard" in this context.

The CCPA does not appear to regulate the access that companies provide to advertisers regarding targeted individuals where that access is granted without providing specific information from individual users. In this manner, some large companies that maintain they do not sell consumers' data (*e.g.*, Facebook) appear to fall outside the reach of those portions of the CCPA that govern sale-specific issues. It remains to be seen if or how the Attorney General may seek to apply the CCPA to such a context. Unless the CCPA were revised to clarify its applicable to this use of consumer information, or the Attorney General were to issue a regulation or guidance related to the same, it is not clear how consumers would opt out of having their information shared with third-party advertisers.

H. Are There Limits Placed on the Collection of Information?

The CCPA does not appear to place limits on businesses' ability to collect personal information on consumers, although, as noted above, it does require that businesses provide consumers certain notices and disclosures related to the collection of that information. In this way the CCPA may be a continuation of the status quo with some additional disclosure protections layered on top of the existing data-collection framework. The GDPR, in contrast, requires that companies obtain a data subject's permission before they collect data on that data subject.

I. Can a Business Treat Consumers Differently if They Exercise Their Rights?

Businesses are generally prohibited from discriminating against consumers who choose to exercise their rights under the Act, including by opting out of the sale or disclosure of their personal information to third parties. This includes through actions like increasing fees, slowing services, etc. Businesses *are* allowed to differentiate among consumers in terms of prices charged or level of services provided if the difference is reasonably related to the value provided to the consumer by the consumer's data. In addition, businesses may offer financial incentives for the collection, sale, or deletion of consumers' data, if the business provides notice of the incentive to consumers.

Some commentators have remarked that by permitting differentiation among consumers linked to the value provided by the consumer's data, the CCPA effectively permits businesses to charge more or offer lesser services to consumers who elect to exercise their rights to greater privacy. A few lawmakers expressed concern with the CCPA for this reason suggesting it was setting California on a path toward a "pay-for-privacy" regime. (Sacramento Bee (07/05/18), quoting Sen. Hannah Beth-Jackson.) Other commentators have suggested that this permits businesses to effectively market services where consumers would prefer to provide information rather than pay for a service.

J. Are Businesses Required to Implement Certain Security Measures?

To help minimize the risk of a consumer action, businesses must implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information that is to protected. What constitutes "reasonable security" is not discussed in the Act. Indeed, California has not codified what is meant by "reasonable security" although it requires businesses that own, license or maintain personal information about California residents to provide reasonable security for that information both in the CCPA and in other state privacy-related statutes. (*See* Cal. Civ. Code § 1798.81.5(a).)

In the absence of codified standards, industry best practices suggest ensuring security policies and practices are in line with one of the several internationally-recognized information security frameworks. These include, among others, the Center for Internet Security's ("CIS") 20 Critical Security Controls, the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework and related NIST standards (*e.g.*,

NIST SP 800-171), or the International Standards Organization's (ISO) various series governing information security management (*e.g.*, ISO/IEC 27001). Adoption of these or equivalent information security frameworks and incorporation of the same into internal policies and practices would likely assist a business in establishing its good-faith effort to implement and maintain reasonable security measures. Guidance from the California Attorney General's Office in its 2016 Data Breach Report, suggests that businesses that abide by CIS's Critical Security Controls would likely meet the reasonable security requirement. (*See* CA 2016 Data Breach Report, p. v.) The guidance does not rule out the ability for businesses to follow equivalent, industry-recognized information security frameworks to achieve the same goal.

K. Are there Limits on the Re-Sale of Personal Information?

A third party that purchases consumers' personal information from a business cannot in turn sell that information to another without providing the consumers explicit notice and the opportunity to opt out. The CCPA does not specify how that notice or opt-out option should be provided to consumers. Once the CCPA goes into force, businesses may want to take precautionary measures like automatically providing options to opt out of the sale of personal information prior to any collection to easily enable the sale of such information down the line, segregating all personal information from California residents and not selling the same, or seeking guidance from the Attorney General as to how best to comply prior to re-sale.

L. Are there Protections Against Liability for Service Provider Misconduct?

Businesses that share consumers' personal information are not liable under the CCPA for service provider misconduct, if, at the time the business discloses the personal information, the business did not have actual knowledge, or reason to believe, that the service provider intended to violate the Act. Businesses also must have complied with the requirements of the CCPA in terms of having a proper written contract in place that prohibits the service provider from retaining, using or disclosing the personal information for any purpose other than for performing the services specified in the contract for the business that provided the personal information, or as otherwise permitted by the Act. A service provider is similarly free of liability for the obligations of a business from which it receives personal information.

To help preserve this limit on liability, businesses should ensure that their contracts with service providers include specific provisions prohibiting the service providers from using any consumers' personal information provided in connection with the contract aside from carrying out the purposes of the contract or related administrative tasks. Businesses should also require service providers to represent that they are aware of and abide by the terms of the Act, as well as related regulations. Representations of this kind could assist businesses in establishing that they did not have actual knowledge or a reasonable basis for believing the service provider was planning to violate the CCPA at the time personal information was transferred to the service provider. It may be wise to have businesses reaffirm their awareness of and compliance with the CCPA and related regulations until both are fully adopted and in force.

M. Can Consumers Waive Applicability of Act?

The CCPA explicitly empowers courts to deem unenforceable any provision of a contract or agreement that purports to waive or limit in any way a consumer's rights under its terms. This includes any right to a remedy or specific means of enforcement. A consumer can still opt not to request information from a business or decline to take other actions under the Act.

III. Enforcement and Penalties

The CCPA contemplates two main avenues for enforcement of and recovery under the CCPA–private consumer rights of action (whether through individual or class actions), and actions brought by the Attorney General in the public interest. Both pose risks to businesses. Businesses also have the ability to seek guidance from the Attorney General on how to comply with the Act.

A. Consumer's Private Right of Action

Any consumer whosenonencrypted ornonredacted personal information is subject to an unauthorized access andexfiltration, theft or disclosure as a result of a business's failure to implement and maintain reasonable security procedures and practices may institute a private right of action for any of the following: (1) the greater of either the consumer's actual damages or damages in an amount not less than $100 and not greater than $750 per consumer per incident;[1] (2) injunctive or declaratory relief; or (3) any other relief a court deems proper. A consumer is apparently not required to establish actual harm to pursue a private right of action.

A consumer may only bring a private right of action where he or she meets two additional requirements. First, prior to initiating any action, the consumer must provide the business 30 days' written notice identifying the specific provisions of the CCPA he or she alleges have been or are being violated. If the business cures the issue within 30 days, no consumer action is permitted. If not, the consumer may proceed with filing. If a business informs a consumer that an issue is cured and it is not, that consumer is entitled to initiate an action against the business that seeks damages for each breach of the written representation as well as any other violation of the CCPA that postdates receipt of the written representation. Consumers seeking to recover only their actual, monetary damages do not have to provide such notice and may proceed directly to filing and notifying the Attorney General.

Second, the consumer must notify the Attorney General within 30 days that the action has been filed. The Attorney General then has 30 days to take one of the following three actions: (1) notify the consumer of its intention to prosecute the action; (2) refrain from acting for 30 days, thus permitting the consumer to proceed; or (3) notify the consumer that he or she shall not proceed with the action. With regard to the first option, the Attorney General has six months in which to initiate its prosecution. If the

[1] In assessing what statutory damages may be imposed, the CCPA directs courts to consider factors including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

Attorney General fails to CCPA within that period, the consumer may proceed with his or her action.

B. Attorney General Enforcement

The Attorney General has the sole right to pursue civil penalties against businesses in violation of the CCPA through a civil action in the public's name. Businesses are in violation of the CCPA if they do not cure any alleged violation within 30 days of notification of the same. Penalties of up to $2,500 for general violations could be imposed, while penalties for intentional violations could be up to $7,500 for each violation. The term "violation" is not defined in the CCPA and it is not clear how penalties might be imposed. The private right of action, in contrast, limits the collection of its set damages to a per consumer per incident basis.

The CCPA created a new Consumer Privacy Fund (the "Fund") within California's General Fund into which 20 percent of the funds recovered will be deposited, while the remaining 80 percent will go to the jurisdiction that brought the action. The Fund is intended to offset any costs incurred by state courts or the Attorney General in bringing cases connected with the Act.

C. Ability to Seek Attorney General Guidance

Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the Act. This provision may be of particular importance with regard to gaining clarity on some of the more opaque sections of the CCPA before it goes into force in 2020. This may be a particularly useful tool in some cases for groups of businesses facing the same issue that may wish to submit a joint request for an opinion on as both a means of gaining guidance and as an advocacy tool to highlight a particularly unclear section of the CCPA, although the CCPA remains silent concerning how long the Attorney General has to respond to opinion requests.

IV. Conclusion and Proactive Steps to Take Now

- Passage of the CCPA marks a watershed moment for privacy law in the United States. California's size, population and the predominance of the state's technology sector ensure that the Act's requirements will have consequences far beyond the state's borders. The best way to respond to these developing requirements is to implement strong security and privacy measures and to periodically review the same. We recommend that businesses take the following steps now to begin to protect themselves from the likely effects of the Act.
- Determine if you collect, maintain or hold California residents' personal information or if an entity you control or that controls you does so. Understanding if the CCPA actually applies to you is the first step in defense.
- If you do not already have someone in your organization responsible for following and addressing requirements relating to personal information, consider establishing a role that makes sense for your organization.
- Engage in a data mapping activity that provides information on who in your organization collects, uses and shares what personal information for what purposes, and that tells you where and how that data is stored and accessed. This

effort will assist in compliance with a range of regulatory regimes (*e.g.*, California, GDPR, etc.).

- Incorporate an internationally-recognized framework like the CIS's 20 Critical Security Controls, NIST's Cybersecurity Framework, the ISO/IEC series 27001, or an equivalent in your information security policies and practices to help ensure your company is employing reasonable security measures. Consider implementing other industry-specific best practices that may meet special needs of your business.
- Take steps now to encrypt or redact consumers' personal information when collected, stored, and transmitted as a means of helping to mitigate some of the potential litigation burden that could arise if unencrypted or unredacted personal information is the affected by a security incident.
- Draft strong written contracts with service providers and vendors with which you share consumers' personal information to ensure those contracts meet the requirements of the CCPA and will afford you the strongest protection from liability.
- Consider requesting guidance from the Attorney General before the CCPA goes into effect regarding its applicability if unclear. Official guidance could protect against consumer litigation, particularly on ambiguous sections of the Act.
- Begin considering whether it is feasible to segregate personal information you collect, maintain or hold on California consumers to enable eventual easy compliance with the Act. Consider taking similar steps to those your organization may already have taken to comply with other regulatory regimes like the GDPR or Massachusetts's Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00).