King & Spalding

Client Alert

Data, Privacy and Security

FEBRUARY 14, 2019

For more information, contact:

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

Ehren Halse
+1 415 318 1216
ehalse@kslaw.com

Anne Voigts
+1 650 422 6710
avoigts@kslaw.com

Anush Emelianova
+1 404 572 4616
aemelianova@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

San Francisco
101 Second Street
Suite 2300
San Francisco, CA 94015
Tel: +1 415 318 1200

Silicon Valley
601 South California Avenue
Palo, Alto, CA 94304
Tel: +1 650 422 6700

Start Aiming Now: The California Consumer Privacy Act (CCPA) Is A Moving Target, And GDPR Compliance Isn't Enough

The CCPA is an unprecedented privacy law that grants California residents sweeping rights concerning the collection and use of their information. Once the law becomes effective on January 1, 2020, covered businesses can expect to weather a flurry of consumer requests, which can encompass information collected from January 1, 2019 forward. The CCPA defines both consumers and covered businesses broadly, grants far-reaching rights to consumers, and imposes extensive obligations on covered businesses. And compliance with other progressive privacy regulations like the EU General Data Protection Regulation ("GDPR") does not ensure compliance with the CCPA. California's ground-breaking legislation may encourage other states to follow suit, with some already considering similar legislation. For pharmaceutical and medical device companies, patient medical information is exempt from the CCPA, but personal information about prescribers and employees domiciled in California appears to be covered.

While the breadth of the CCPA is clear, its precise contours are still in a state of flux for two reasons: first, the California Attorney General ("AG") has yet to adopt implementing regulations. The AG is currently accepting comments in a series of public forums spanning January and February 2019. Written comments may also be submitted by March 8, 2019 for consideration in the preliminary rulemaking stage. Second, any last-minute amendments to the CCPA can still be introduced by the legislative deadline of February 22, 2019. In this client alert, we discuss the CCPA's requirements as it currently stands, summarize the likely impacts on covered businesses, address the consequences for non-compliance, and recommend CCPA compliance steps companies should consider now.

EXECUTIVE SUMMARY

- The CCPA applies broadly both in terms of who and what is covered: the definition of "personal information" (that is, information that can reasonably be linked to a "consumer" or "household") is uniquely expansive, and virtually all companies of substantial size who do business in California would be covered. The CCPA applies to all information about a consumer—not just electronic information.
- Consumers' new rights include learning what specific information companies have collected about them over the preceding year and why, accessing or requesting the deletion of the information, and opting out of the sale of information.
- Companies must implement new business processes to comply with the CCPA—for example, to fulfill consumer requests in a timely manner and to ensure that all applicable information (regardless of whether stored electronically, on paper, or by a service provider) is deleted.
- Companies that revised their business practices for the GDPR last year will still have to make additional changes to comply with new requirements under the CCPA.
- The California AG is primarily responsible for CCPA enforcement and can impose fines of up to $7,500 per intentional failure to comply with the CCPA.
- Additionally, California consumers can sue for significant statutory damages businesses who suffer a data breach of their sensitive information due to the business's failure to maintain reasonable security measures.
- The CCPA raises as many questions as it answers, such as whether and which employee information is covered and what constitutes a properly verified consumer request for personal information. Some of those questions may be resolved by the AG's forthcoming CCPA regulations or by legislative amendments, but some may not.
- Healthcare and financial services are largely exempt from the CCPA. Additionally, the CCPA "does not restrict" a business's ability to defend or to exercise legal claims or cooperate with government authorities.

TO WHOM DOES THE CCPA APPLY?

The CCPA's obligations apply to all businesses that collect, process, or store[1] personal information of California residents, as long as the business meets any one of the following three conditions: (i) the business has annual gross revenues exceeding $25 million, (ii) it annually buys or sells personal information of 50,000 or more California consumers, households, or devices, or (iii) it derives more than 50% of its annual revenue from selling California consumers' personal information.[2] What these conditions will mean in practice is not clear. For example, will a business that hits $25 million in revenue for the first time in a given year be expected to comply instantly? Does the $25 million threshold apply to global revenue or only California-derived revenue? The business community has expressed concern about these questions (and others) concerning the breadth of application and the ambiguity of the CCPA's coverage in the AG's public forums.[3]

COMPLIANCE WITH THE GDPR DOES NOT ENSURE COMPLIANCE WITH THE CCPA

As currently drafted, the CCPA is broader than existing U.S. state privacy laws and the GDPR. As a result, compliance with the GDPR does not ensure compliance with the CCPA. Businesses that have complied with the GDPR should consider the following ways the two laws differ significantly:

1. **Unpredictable territorial reach**: For a U.S.-based business (that does not have an establishment in the EU), GDPR applies to individuals located in the EU; CCPA applies to California residents, who are not always located in California.
   a. The *GDPR* applies to the personal data of data subjects "who are in the Union" if the business is offering goods or services to data subjects in the EU or monitoring their behavior in the EU.[4]
   b. The *CCPA*, on the other hand, applies to (1) all individuals in California for other than a temporary or transitory purpose, and (2) every individual domiciled in California who is outside the state for a temporary or transitory purpose.[5] Given the difficulty of determining whether a particular individual is in the state for a temporary purpose or not, businesses will likely assume the CCPA applies to all information gathered about individuals in California. But identifying those individuals domiciled in California, but temporarily outside the state, is likely to pose a greater compliance challenge—especially for businesses that do not gather address information as a matter of course.
2. **No discrimination:**
   a. The *GDPR* does not include an anti-discrimination provision.
   b. The *CCPA* does include an anti-discrimination provision, which states that a business cannot discriminate or suggest that it will discriminate against a California resident exercising their rights under the CCPA (for example, by providing a different product or price or refusing service to California residents).[6] Businesses can still: (1) opt to stop doing business with all California residents altogether (an unlikely strategy); (2) comply fully with the CCPA; or (3) attempt to tailor their business practices to fall under one of the exceptions to the CCPA's anti-discrimination provision, by:
      - Charging different prices or offering different product levels if the difference is "reasonably related to the value provided to the consumer by the consumer's data[;]" or
      - Offering financial incentives to consumers for their data, as long as consumers (a) opt in, after being informed of the material terms of any such financial incentives program, and (b) have the right to revoke consent at any time. However, because the relevant measure is not how the business or the market values the data, but rather how the *consumer* values the data, businesses may struggle to reasonably assess each consumer's individual valuation of their own data.
3. **Definition of personal information:**
   a. The *GDPR* defines personal information as "any information relating to an identified or identifiable natural person."
   b. The *CCPA*'s definition is more expansive.[7] First, personal information means "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**" (emphasis added).[8] Thus, information that may not have previously identified an individual—such as IP addresses—is now "personal information" if it identifies, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a household. The CCPA's nexus for personal information—information that is "capable of being associated" or could "reasonably" be "indirectly" linked with a person or household—is ambiguous and potentially significantly broader than the GDPR. Second, it is not clear

how the new “household” concept interacts with the CCPA's provisions requiring businesses to respond to verifiable consumer requests for data portability, deletion, or information about data collection or sale—including the “specific pieces” of personal information collected.[9] Per the statute, businesses must respond to consumer requests only from the consumer about whom the information is collected, about the consumer's minor child, or from a person who has been authorized by the consumer to act on the consumer's behalf.[10] There is not yet guidance as to whether businesses should give information collected about a household to a consumer who is part of the household. Doing so may raise new privacy concerns—for example, in situations where there is a risk of domestic violence, or where one household member may be improperly seeking information about another. At a CCPA forum on January 25, 2019 in Los Angeles, one commentator requested additional direction from the AG on this point to avoid unintentional disclosure within a household.

c. In general, verification of access requests is likely to prove challenging: at the AG’s CCPA forums on January 8, 2019 and on January 25, 2019, multiple speakers expressed concern that businesses would need to collect or process additional personal information to verify and respond to access requests.

WHAT RIGHTS DOES THE CCPA CREATE?

The CCPA grants California residents expansive rights concerning their personal information, including the rights to:

- **Know what personal information the business collects, sells, or discloses about them**, including the specific pieces of information the business has collected and the categories of third parties who purchased or received their data.[11] (As discussed further below, the CCPA’s definition of personal information is very broad, generally encompassing information that is capable of being linked back to the consumer in some fashion.) Moreover, the CCPA is not limited to information collected electronically or over the Internet, but also applies to the collection and sale of all personal information collected by a business from consumers. Businesses must provide this information for the preceding 12 months in response to a consumer request—so a business that receives a verifiable consumer request on January 1, 2020, when the law is currently slated to become effective, must disclose what information has been collected, sold, or disclosed about a California resident between January 1, 2019 and January 1, 2020.[12]

- **Receive notice,** before or at the point of collection, about what categories of personal information the business collects and what it intends to do with such information. A business may not collect additional categories of personal information or use collected personal information for unrelated purposes without providing notice.[13]

- **Receive their personal information in a portable format** free of charge after submitting a verifiable request.[14] The AG must adopt regulations to clarify what qualifies as a “verifiable” consumer request.

- **Request that a business and its service providers delete the consumer's personal information**, subject to certain exceptions, such as to complete a transaction or to comply with a legal obligation.[15]

- **Opt out of the sale of their personal information** if the consumer is 16 years old or older, via a clear and conspicuous “Do Not Sell My Personal Information” link on the business’s homepage.[16] (Opt-in consent is required for individuals between 13 and 16, and parental authorization is required for under 13.)[17]

WHAT OBLIGATIONS DOES THE CCPA IMPOSE?

Beyond the obligations to consumers articulated above (i.e., obligations to provide explanation and notice concerning the collection and treatment of personal information, the right to receive such information in a portable format, the right to deletion upon request, and opting out of the sale of personal information) under the CCPA, covered businesses must also:

- **Provide a privacy policy**, updated annually and accessible on its website, that:
  - describes the consumers' rights and at least two methods to submit requests;
  - lists the personal information categories the business has collected about consumers in the past 12 months; and
  - provides separate lists of the personal information categories the business has sold or disclosed for business purposes in the past 12 months, or statements that it has not sold or disclosed any consumer information.[18]
- **Implement procedures to respond to consumers' verifiable requests** for access, deletion, opt-out, or information about collection, disclosure, or sale of personal information, free of charge, within 45 days. This time period can be extended once by another 45 days with notice to the consumer.[19] Generally, businesses cannot discriminate against consumers or provide different services based on the consumers' exercise of CCPA rights.[20]
- **Train employees** responsible for handing consumer inquiries about the business's privacy practices and compliance requirements.[21]
- **Not resell consumer information** unless the consumer has received notice and an opt-out opportunity.[22]

WHAT DOESN'T THE CCPA COVER?

The CCPA does provide some limited exemptions that are largely specific to the medical and financial services industries and that are designed to avoid conflicts with existing statutory protections. Those exemptions include:[23]

- **Information that would restrict a business's ability "to exercise or defend legal claims"** if subject to a CCPA request.[24] A business may be able to use this exemption to avoid disclosing or deleting the personnel file of a potentially litigious employee, for example.
- **Personal information collected and sold outside of California**: the CCPA "shall not restrict a business's ability" to collect and sell personal information where "every aspect of that commercial conduct takes place wholly outside of California." That exemption, however, applies only to information collected about someone outside California that is sold outside California.[25]
- **Healthcare Exemptions**:
  - **Medical information,** which is "individually identifiable information in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment."[26]
  - **Protected health information ("PHI")** collected by a covered entity or business associate under the Health Insurance Portability and Accountability Act ("HIPAA") is also exempt.[27] The statute implies that PHI held by a third-party company that is neither a covered entity nor a business associate under HIPAA would still be exempt, as long as the PHI was originally collected by a covered entity or business associate.

  - **Non-medical information held by a HIPAA covered entity**: to the extent that a healthcare provider or covered entity maintains other information in the same way as its medical information or PHI, the non-medical information is also exempt.[28] This exemption does not cover business associates, who will still need to comply with CCPA to the extent that they have personal information that is not medical information.
  - **Clinical trial data:** information collected as part of a clinical trial that otherwise complies with federal rules protecting human subjects in clinical trials.[29]
- **Financial Services Exemptions**:
  - **Creditworthiness information** subject to the Fair Credit Reporting Act (FCRA) and sold to or from a consumer reporting agency.[30]
  - **Financial information collected or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA)**: the GLBA covers personally-identifiable financial information, which means any information a consumer provides to a financial institution to obtain a financial product or service. Notably, consumers still have a private right of action against financial institutions if GLBA-covered information is the subject of a data breach.[31] Additionally, it is not clear whether information gathered about a consumer who interacts with a financial institution, but does not go on to obtain a financial product or service, would be covered by the CCPA exemption.
- **Driving record information** collected or disclosed pursuant to the Driver's Privacy Protection Act by state Departments of Motor Vehicles.[32]

WHAT ARE THE CONSEQUENCES FOR NON-COMPLIANCE?

The California AG is empowered to monitor compliance with the CCPA and impose civil penalties for violations—up to $2,500 for each non-intentional violation, and up to $7,500 per intentional violation.[33] Such penalties can be imposed for violations like failing to properly respond to consumer access or deletion requests. The AG must allow a 30-day period to cure violations before imposing penalties.[34] During the San Diego public forum on January 14, 2019, a representative of the Consumer Attorneys of California (a plaintiff's attorney organization) who helped draft the CCPA commented that businesses should not be taking a "sky is falling" mentality and will not really have to worry about compliance for a long time because the AG's office does not have the resources to fully enforce the CCPA. This comment does not provide much comfort to companies against whom enforcement is possible, particularly given the expansive reach of the CCPA as drafted, and the fact that violations (and corresponding penalties) for covered businesses could add up very quickly.

The CCPA also includes a private right of action—a boon to plaintiff's lawyers—because plaintiffs in data breach lawsuits have previously struggled to establish standing in the absence of concrete financial harm attributable to a breach. Under the CCPA, where (1) a consumer has suffered a data breach of a narrower category of personal information (i.e., a consumer's first name or first initial, plus last name, plus at least one of the following: Social Security number, driver's license of state identification number, credit/debit card number or financial account number plus security code, medical information, or health insurance information) and (2) the data breach is the result of a business's failure to implement and maintain reasonable and appropriate security procedures and practices, the consumer may collect either statutory damages between $100 and $750 "per consumer per incident", or actual damages, whichever is greater.[35] (Businesses are already required by statute to notify consumers if there is a breach concerning those categories.[36])

A lawsuit for statutory damages cannot be brought if the business "actually cures" its violations of the CCPA within 30 days of receiving written notice.[37] But it is unclear whether a failure to maintain reasonable security resulting in a breach can "actually" be cured. If a customer's Social Security number is breached, for example, a business may not be able to cure such exposure, even if it patches the security issue after-the-fact. Additionally, businesses are not liable for the CCPA violations of their service providers, provided that the business did not have actual knowledge, or reason to believe, that its service provider intended to violate the CCPA when disclosing the relevant personal information to the service provider.[38]

CCPA COMPLIANCE IS A MOVING TARGET

The CCPA in its current form takes effect on January 1, 2020. But that current form is likely to change. February 22, 2019 is the last day for bills to be introduced for the 2019 legislative session.[39] And the California Attorney General is required to promulgate regulations to implement the CCPA by July 1, 2020. These regulations may provide some more clarity for businesses seeking to comply with the CCPA, or they may further increase the burden of compliance.

The AG is currently holding forums and inviting written comments in the initial rule-making process. At those forums, speakers have repeatedly requested that the AG provide more clarity—such as by publishing template privacy notice formats and offering a safe harbor to companies who adopt the formats (as is already the case for breach notifications to individuals).[40]

Two particular areas of discussion in the public forums thus far have been the threshold for covered businesses, and the CCPA's potential application to employee data. In particular, as written, the CCPA does not exclude data that companies have about their employees, and the CCPA's definition of personal information explicitly includes "professional or employment-related information."[41] Attendees at both of the AG's first two CCPA public forums in San Francisco and San Diego this month requested that the AG clarify whether the definition of "consumer" includes employee and human resources data. Absent clarification, employees might be able to exercise the same rights as consumers under the CCPA to learn the specific content of personnel files collected about them or request that information about them be deleted. Employers may attempt to rely on the CCPA's exemptions to avoid disclosing or deleting the contents of personnel files. First, the CCPA "shall not restrict a business's ability" to comply with laws or exercise or defend legal claims.[42] Furthermore, a business does not have to comply with a deletion request if the business needs to maintain the personal information to detect security incidents, protect against illegal activity, or "enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business."[43] Businesses will probably be able to avoid deleting the data they gather on employees if such data is reasonably related to the employee's expectations based on the employment relationship. But businesses may still have to disclose any data they gather about their employees to those employees upon request—unless the business can claim that such disclosure would interfere with the business's ability to defend legal claims (e.g., against a lawsuit by a disgruntled employee).[44]

Rulemaking and legislative amendments may change or clarify some of the CCPA's requirements. They will not, however, change the fact that covered businesses will face new, sweeping, and sometimes ambiguous obligations with respect to California consumers. And California's obligations may soon be accompanied by other federal and state legislation: the CCPA may galvanize the passage of a comprehensive federal privacy statute—especially if other states may decide to follow California's lead and update or enact their own, distinct privacy statutes. Indeed, a CCPA-like comprehensive privacy bill was proposed in the Washington Senate last month and is currently in committee.[45]

CURRENT COMPLIANCE STEPS

Covered businesses should consider taking the following minimum steps to comply with the CCPA as currently drafted.

1. **Determine applicability:** analyze whether they are or may become covered businesses, as well as which categories of information and whether the business possesses personal information of California residents who are covered by the law.

2. **Consider data requirements**: evaluate whether collecting identifiable personal information about California residents is required and whether it justifies the costs of compliance.

3. **Track data streams**: to respond to consumer requests and provide required privacy disclosures, businesses must know what personal information they collect about California residents, how they store that information, and what third parties or service providers the information may be shared with. Businesses must also be able to access and modify those records in order to comply with the deletion, access, portability, and opt-out requirements. While the CCPA goes into effect on January 1, 2020, consumers can make requests about the information gathered about them over the preceding 12 months – thus, data collection, storage, and deletion policies *currently in place* may determine the ability of a covered business to comply with the CCPA.[46]

4. **Make necessary operational changes for compliance**: businesses must develop the processes necessary to comply with the obligations imposed by the CCPA by:

   — Setting up a toll-free number and web address for consumers to submit verifiable consumer requests;[47]

   — Designating individuals to verify the identity of consumers making requests and respond to verifiable consumer requests, generally within 45 days;[48]

   — If selling consumer information, enabling consumers to opt in and opt out of the sale of their information and posting a clear and conspicuous link titled "Do Not Sell My Personal Information" on their home page;[49]

   — Establishing reasonable security practices and procedures to protect data and avoid civil liability for a data breach;[50]

   — Including required contractual clauses in agreements with service providers;[51]

5. **Update privacy policies and contracts with vendors to comply with the CCPA.**[52]

6. **Train employees for compliance.**[53]

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,000 lawyers in 20 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice.
In some jurisdictions, this may be considered "Attorney Advertising."

ABU DHABI
ATLANTA
AUSTIN
CHARLOTTE
CHICAGO
DUBAI
FRANKFURT
GENEVA
HOUSTON
LONDON
LOS ANGELES
MOSCOW
NEW YORK
PARIS
RIYADH
SAN FRANCISCO
SILICON VALLEY
SINGAPORE
TOKYO
WASHINGTON, D.C.

[1] The CCPA applies to businesses that collect (buy, rent, access, or obtain by any means) personal information and that determine the purposes and means of the processing of the personal information, either by themselves or jointly. Cal. Civ. Code §§ 1798.40(c)(1), (e).
[2] Id. § 1798.40(c).
[3] Comments from public forum in San Francisco on January 8, 2019. For more information about the AG's planned forums, see California Attorney General, Press Release, Attorney General Becerra to Hold Public Forums on California Consumer Privacy Act as Part of Rulemaking Process, available at https://oag.ca.gov/news/press-releases/attorney-general-becerra-hold-public-forums-california-consumer-privacy-act-part (Dec. 19, 2019).
[4] General Data Protection Regulation ("G.D.P.R."), Article 3 (2).
[5] Cal. Civ. Code § 1798.40(g), citing 18 C.C.R. § 17014.
[6] Cal. Civ. Code § 1798.125.
[7] G.D.P.R. Art. 4(1).
[8] Cal. Civ. Code § 1798.40(o)(1).
[9] Id. §§ 1798.100, 105, 110, 115.
[10] Id. § 1798.40(y).
[11] Id. §§ 1798.110, 115.
[12] Id. §§ 1798.130(a)(3), (4).
[13] Id. § 1798.100.
[14] Id.
[15] Id. § 1798.105.
[16] Id. § 1798.135(a)(1).
[17] Id. §§ 1798.120(a), (c).
[18] Id. § 1798.130(a)(5).
[19] Id. § 1798.130(a)(2).
[20] Id. § 1798.125(a)(1).
[21] Id. § 1798.135(a)(3).
[22] Id. § 1798.115(d).
[23] The CCPA also states that no obligations contained in the Act can restrict a business's ability to

- comply with federal, state, or local laws;
- comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;
- cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law; or
- collect, use, retain, sell, or disclose consumer information that is deidentified or aggregated.

Id. § 1798.145(a).
[24] Id. § 1798.145(a)(4).
[25] Id. § 1798.145(a)(6).
[26] Id. § 1798.145(c)(1)(A), exempting medical information as defined by the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56.05(j).

[27] Cal. Civ. Code § 1798.40(c)(1)(A).
[28] Id. § 1798.40(c)(1)(B).
[29] Id. § 1798.40(c)(1)(C).
[30] Id. § 1798.40(d), citing the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.).
[31] Cal. Civ. Code § 1798.40(e); see also 16 CFR § 313.3(o)(1).
[32] Cal. Civ. Code § 1798.40(f), citing 18 U.S.C. Sec. 2721 et seq.).
[33] Id. § 1798.155.
[34] Id.
[35] Id. § 1798.50(a).
[36] Cal. Civ. Code. § 1798.82.
[37] Id. § 1798.50(b).
[38] Id. § 1798.145(h).
[39] California State Assembly, 2019 Legislative Deadlines (Oct. 31, 2018) available at https://www.assembly.ca.gov/legislativedeadlines.
[40] Cal. Civ. Code § 1798.82(d)(1)(D).
[41] Id. § 1798.40(o)(1)(I). While the CCPA's provisions establishing rights to access and delete data refer to the rights of, and personal information about, "consumer[s]," a "consumer" is simply defined as a California resident—under the law as written, it appears that an employee can also be a "consumer." Id. § 1798.40(g).
[42] Id. §§ 1798.145(a)(1), (4).
[43] Id. § 1798.105(d).
[44] Id. § 1798.145(a)(5).
[45] Senate Bill 5376, Washington Privacy Act, proposed on January 18, 2019, available at https://app.leg.wa.gov/billsummary?BillNumber=5376&Year=2019.
[46] Cal. Civ. Code. §§ 1798.130(a)(3), (4).
[47] Id. § 1798.130(a)(1).
[48] Id. § 1798.130(a)(2).
[49] Id. § 1798.135(a)(1).
[50] Id. § 1798.150(a)(1).
[51] Id. § 1798.140(v).
[52] Id. § 1798.135(a).
[53] Id. § 1798.130(a)(5).