The California Consumer Privacy Act: What Every In-House Lawyer Should Know

In 2018, the world's most onerous privacy law, the European Union's General Data Protection Regulation, went into effect. California then responded, "hold my beer!" and enacted the California Consumer Privacy Act (CCPA). The CCPA imposes significant compliance costs and creates potentially enormous liability for companies that fail to comply. With in-house counsel in mind, this primer provides an overview of the CCPA's scope, its requirements, and tips on operationalization.

Once Upon a Time...

The CCPA came about because a wealthy Californian was upset at what he perceived to be a lack of transparency and control over how his personal information was being collected, sold, and used by large technology companies, social media companies, and data brokers. He took action by funding a campaign to put on the November 2018 ballot in California an initiative that would have created the most onerous privacy law ever to go into effect in the United States. The law would have created a private right of action for any violation (not just data breaches) and created a tsunami of liability for companies doing business in California. The measure gained support, eventually reaching the threshold number of signatures required to place the initiative on the November ballot.

Realizing that California residents would likely support this measure if it were to be placed on the ballot, pro-business groups reached a last-minute deal pursuant to which the ballot initiative was withdrawn in return for the California State Legislature adopting a law that encompassed most of the same requirements as the ballot initiative. This "compromise" in producing the CCPA was the lesser of two evils for companies doing business in California because it meant a slightly less draconian law and a better chance to amend the law in the future. As a result of the last-minute negotiations rush (the bill was drafted and passed within a couple of weeks), the CCPA contains inconsistencies, typographical errors, and many unresolved issues.

To Whom Does the CCPA Apply?

The CCPA applies to **for-profit entities** that:

1. collect consumer personal information (a "consumer" is currently defined as any resident of California—so think employees as well as customers—though there is an amendment to the CCPA pending that would limit the definition of consumer to the more traditional meaning)[1];

2. determine the purposes and means of processing (i.e., the business controls what happens to the personal information);

3. do business in the state of California; and

4. do any of the following:

a. earn $25 million in revenue per year (this is not limited to revenue generated solely in California);

b. receive for commercial purposes, sell, or share for commercial purposes 50,000 consumer records per year; ***or***

SHOOK HARDY & BACON

c. derive 50 percent of annual revenue from selling personal information.

The CCPA applies not just to companies located in California, but any company that collects, discloses, or sells personal information about California residents.

Are There Exceptions to the CCPA's Scope?

Yes, the law has many exceptions. For example, the CCPA doesn't apply to information governed by HIPAA/HITECH, GLBA, FCRA, clinical trial information, or information that has been de-identified or aggregated. Note, however, that these are not company-wide exceptions, meaning they apply only to the *information*. So, for example, a covered entity under HIPAA may still be governed by the CCPA to the extent it collects personal information that is not PHI. There are other exceptions, too, like where a company needs to comply with legal obligations, comply with law enforcement or a subpoena, exercise/defend a legal claim, or prevent the violation of an evidentiary privilege.

What Is "Personal Information" Under the CCPA?

The CCPA adopts the broadest definition of personal information we have ever seen. It means any 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. Examples of personal information include the following:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Any categories of personal information described in California's data breach notification law;
- Characteristics of protected classifications under California or federal law (e.g., race, gender, and ethnicity);
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;
- Education information; and
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

To put the breadth of this definition into perspective, the 50 different state data breach notifications typically limit their definition of personal information to the first two bullets above. The CCPA also includes information gleaned from a California-based IP address visiting your website. The way a person sounds, smells, and the amount of heat they emit are all types of personal information under the law. Professional and employment-related information are included in the definition (surprisingly, salary is not considered personal information under most data breach notification laws). If that definition were not broad enough alone, it also includes that any inferences drawn about individuals (or households) from any of these pieces of information would also be considered personal information

What Rights Does the CCPA Bestow on Data Subjects?

The CCPA creates **seven fundamental rights** for data subjects:

1. **The right to know** about the collection and sale of their information, and about their CCPA rights. At or before the time of collection, a business must inform data subjects of the categories of personal information collected, the sources of that information, the third parties with whom the information is shared, and the purposes for which the personal information will be used. Companies must also disclose their collection, sale, and disclosure practices, as well as descrip-

tions of data-subject rights, in their public-facing privacy notice.

2. The right to access a copy of their information that has been collected or sold. A data subject can request from a business that collects personal information: categories of personal information collected, categories of sources of personal information, the business purpose(s) for collecting the personal information; categories of third parties with whom the personal information is shared, and the specific pieces of personal information collected. These requests, commonly referred to as "data subject access requests" or DSARs, should be verifiable, which can be complicated, depending on what information the business already has about the data subject by which verification can take place. The business' response to a DSAR must cover the preceding twelve months, should be provided free of charge in a portable and usable format (typically a PDF), and delivered within 45 days of receiving the verifiable request (extendable by up to an additional 45 days[2]). The business must provide two or more methods for submitting a DSAR, including a toll-free number and a website address. Many companies choose to develop portals, accessible via their website, through which DSARs can be submitted. In certain instances, like where the DSAR is manifestly unfounded or excessive, a business can charge a fee or refuse to act on it.

3. A right to erasure. The data subject can request that a business (and its service providers) delete personal information the business or service provider collected. The exceptions to this right, however, swallow the rule. For example, a business can refuse a deletion request to complete a requested service or transaction, to detect security incidents, repair functionality errors, exercise any legal right, comply with legal obligations, and engage in certain research. But the two biggest exceptions are: (a) for solely internal uses that are aligned with the consumer's expectations; and (b) for internal purposes that are compatible with the context in which the consumer provided the information. The exceptions are important because the right to erasure extends to third parties with whom the business shares personal information, and it can be expensive and operationally difficult to ensure that personal information has truly been "deleted."

4. Right to opt out of the sale of their information. The CCPA allows a data subject to direct a business to stop selling his/her information. The definition of sale is far broader than the typical definition, as it includes the sharing of personal information not just for money but for any "valuable consideration." Businesses are required to provide notice to data subjects that their information may be sold and that they have a right to opt out of the sale of their personal information. The business' homepage, mobile application, and privacy policy must include a link titled "Do Not Sell My Personal Information" that initiates a process to opt out of the sale of personal information. This is not operationally easy to implement.

5. A right against discrimination. A business cannot deny goods or services or charge different prices to a data subject who exercises his/her rights under the CCPA. A business may, however, offer financial incentives for the collection, sale, or deletion of personal information. For example, a coffee shop can offer a free cup of coffee in exchange for a customer's personal information, but the coffee shop can't charge a customer more for coffee because the customer submitted a DSAR. Financial incentives, like loyalty programs, require opt-in consent before the collection/use of the data subject's information.

6. Consent requirements for the sale of information about children. If the data subject is younger than 13, the business must first obtain the parent or guardian's consent to sell the child's personal information. If the child is between 13 and 15 years old, however, the business need only obtain the child's consent before selling her data. Consent is not necessary to sell the information of an individual who is 16 or older.

7. A right to sue for data breaches. The CCPA will make California the first state in the nation to create a statutory private right of action for a data breach. Damages can range between $100 to $750 per person per incident depending on the degree of intentionality in the misconduct. As a threshold matter, the data subject can sue where the business' alleged failure to "implement

and maintain reasonable security procedures and practices" resulted in the unauthorized access and exfiltration, theft, or disclosure of personal information. Technically, a data breach alone (without poor procedures and practices) doesn't trigger liability under the CCPA, but plaintiff's counsel likely will not find it difficult to demonstrate at least one failure in procedures or practices in light of the fact that the company suffered a data breach. The goal of the plaintiff's counsel will be to create an issue of fact that gets the case past a motion to dismiss or motion for summary judgment and into a large settlement. The right to sue is marginally tempered by a requirement that prior to initiating an action, the data subject must notify the business and provide a 30-day term to cure. This provision makes little sense as once a breach has occurred the data subject's information is already "out there." It is possible that the right to cure means, for example, the implementation of a technical safeguard that, if implemented earlier, would have prevented the breach (e.g., encryption or multi-factor authentication). While the private right of action is currently limited to data breaches, a bill is quickly making its way through the California Legislature, which would create a private right of action for the privacy violations under the CCPA as well.

What Happens if My Company Violates the Law?

Currently, the CCPA will be enforced by the California Attorney General beginning the earlier of July 1, 2020, or six months after the Attorney General's office releases much anticipated guidance on the CCPA. The Attorney General can impose fines of up to $2,500 for each negligent violation of the CCPA or up to $7,500 for each intentional violation of the CCPA. Violation will mean each person and possibly also each provision of the CCPA that has been violated. The Attorney General may also pursue injunctive relief.

The CCPA's private right of action is, for the time being, limited to data breaches where there is a lack of reasonable security procedures and practices. That could change soon. If the California Legislature passes SB 561 and it is signed into law, you could see class action lawsuits based on companies' failure to disclose collection practices, failure to comply with the opt-out requirements, failure to obtain consent for financial incentive programs, or any of the CCPA's other privacy requirements. A class action lawsuit will be less likely in the context of DSARs, where each individual's request may involve a different set of facts.

What Steps Must An In-House Lawyer Take to Protect the Company?

First, **don't procrastinate**. There will be a temptation to believe you have plenty of time because the law doesn't go into effect until January 2020 (and may not be enforced until as late as July 2020). Resist this temptation! Remember that in response to a DSAR, you have to provide information for the preceding 12 months. So if you receive a DSAR in January 2020, will you be prepared to provide a response based on information in your company's possession in January 2019?

Begin by **creating a task force and developing a compliance strategy**. The task force should be comprised of at least one person from each of the following functions: legal, IT, HR, marketing, sales, and corporate communications. Try to do this in conjunction with and at the direction of highly qualified outside counsel like Shook's Privacy and Data Security Practice, which can leverage its experience performing CCPA and other privacy compliance work to draw from templates, their knowledge of the law, benchmarking experience, and relationships with the right vendors. As an additional benefit, performing this work at the direction of outside counsel for the purpose of allowing counsel to advise the company on its obligations under the CCPA, may have the supplemental benefit of triggering attorney-client privilege. As part of this phase, counsel should help you prepare a task list for the compliance work.

Next, **perform a data inventory and data map**. What's the difference between them? A data inventory provides a description of what personal information the company collects, in which systems, why, where it comes from, and where it goes. A data map tracks the lifecycle of the data from the point it enters until the point it leaves your environment. How an inventory and map is created often depends on your available resources. Companies with limited resources may need to perform the inventory themselves through the help

of counsel's templates or use a small consulting company. Larger companies (particularly those that collect considerable amounts of personal information) should consider procuring technology solutions that perform ongoing data discovery, identification, and mapping in real time. They may also choose to retain a larger consulting firm to assist with this step at the direction of counsel. Just remember that both a data inventory and a data map are snapshots in time. To overcome this problem, you may need to review them periodically or purchase a solution that will help you track the data in real time.

Once you know what personal information you're collecting and what you're doing with it, you can **determine your legal obligations**. Again, this is where experienced outside counsel should have a chart at the ready, and should be able to explain (without significant research) which laws apply to you, why, and what those laws require. Use this opportunity to think in the long term. Don't just focus on the CCPA. There are already, as of the time of this article, at least 13 other states considering privacy laws, some of which are comprehensive. Identify the privacy principles that you will abide by as a company and build those into your operation.

You will next need to **create a process for responding to DSARs**. DSARs can be handled manually or via technology solutions that allow you to respond much more efficiently to these requests. Again, Shook's privacy team can point you in the right direction. They can also ensure that your process adequately captures the information you will be legally obligated to provide in response to a DSAR. Counsel should also draft formal guidance and policies to help the company determine whether there is a legal obligation to respond to a request, how to process the request, the content of the response, how to document the request and response process, and when to deny requests.

In conjunction with creating a process for responding to DSARs, you will want to **create a process for responding to requests for deletion**. You'll need a policy that describes when information should or should not be deleted. You'll need to identify responsible personnel for handling those requests. You will also need a method for actually deleting the data (this is where involvement by IT is crucial). Similarly, you will want to ensure that, to the extent you sell consumer information, you have the ability to implement any opt-out requests.

Updating your privacy notices and online presence will be required. For example, your consumer-facing privacy statements will need to be reviewed to be consistent with the CCPA's requirements. Privacy statements shared with job applicants and contractors, to the extent you have them, will need to be updated. You will likely have to address what to do if you always believed (and stated) that you do not "sell" personal information but, under California's much broader law, you now do. Again, this is where an experienced team like Shook's will be key. Additionally, you will need to add a link to your company's homepage and mobile application that allows a California resident to opt out of the sale of their information.

Do you collect **information from children**? If so, you'll need to review your consent mechanisms and ensure they comply with the requirements under the CCPA (and perhaps other privacy laws like the GDPR or the Children's Online Privacy Protection Act).

Review your contracts with service providers. If a service provider fails to comply with the CCPA, your company could be liable if it does not build into the contract some specific language set forth in the CCPA. You will want to identify and update applicable contracts, just as you may have done for GDPR.

Lastly, make sure your **incident response plan and information security policies and procedures are in order**, to minimize the risk of a data breach that triggers the potential right of action.

"

It's the future of U.S. privacy law.

We are seeing other states considering similar comprehensive privacy laws, and the trend is moving towards that, not away from it.

"

Al Saikali, CCPA Webinar

What's Next?

For now, we await any additional changes from the California Legislature, which is considering approximately 20 amendments to the CCPA. The ones that appear to have the greatest traction thus far involve expanding the private right of action. And removing the right to cure for Attorney General enforcement. Other changes being considered include:

- "Consumers" does not apply to mean employees, job applicants, contractors, or agents. (AB 25)
- Loyalty programs are not prohibited by the CCPA. (AB 846)
- It is not a "sale" to share information with a third party for the purpose of measuring online advertisements. (SB 753)
- Removing the requirement of a "Do Not Sell My Personal Information" link. (SB 753)
- Exempting insurance companies and the sharing of personal information between car dealers and manufacturers from the CCPA. (SB 981, AB 1146)
- Fixing obvious errors in the statute. (AB 874)
- Requiring data brokers to register with the Attorney General. (AB 1202)

We also await further guidance from the California Attorney General's office. Under the CCPA, the Attorney General is required to provide guidance on the following topics:

- Updating the **categories of personal information** to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.
- Updating the definition of **unique identifiers** to address changes in technology.
- Establishing **exceptions** necessary to comply with state or federal law, including, those **relating to trade secrets and intellectual property rights**.
- Establishing rules and procedures for:
  - Facilitating and **governing the submission of a DSR to opt-out of the sale** of personal information
  - Governing business **compliance with a consumer's opt-out request**.
- The development of a **uniform opt-out logo or button**.
- **How to give notice** under this provision to consumers.
- **How to verify a consumer's** request for information.

At the time of this article, other states like Massachusetts and Washington are considering equally or more onerous data privacy laws. There is also a push in Congress for a federal data privacy law. Both sides seem to agree in principle that a law is necessary, but the devil will be in the details, specifically preemption. Only time will tell whether we see a patchwork of privacy laws (like breach notification laws) or a federal privacy law with strong preemption.

QUESTIONS

Should you have any questions regarding the California Consumer Privacy Act, please contact:

Al Saikali
Chair, Privacy and Data Security Practice | Miami
305.358.5171
asaikali@shb.com

Steve Vieux
Of Counsel | San Francisco
415.544.1960
svieux@shb.com

Colman McCarthy
Associate | Kansas City
816.559.2081
cdmccarthy@shb.com

[1] The individuals to whom a privacy law applies are commonly referred to as "data subjects." We will use that term throughout this article so as not to create confusion that "consumer" means only customers.

[2] Due to the hasty drafting of the CCPA, there is a conflict in the law regarding how much additional time a business can extend the time to respond to a DSAR. One section specifies 45 days, while another allows an additional 90 days. We recommend using the 45-day period to be conservative.