Pepper Hamilton LLP
Attorneys at Law

Are You Prepared for the California Consumer Privacy Act?
Get Ready for European-Style Privacy in the U.S.
September 7, 2018
Webinar Follow-Up Questions

SPEAKERS

- Jeffrey M. Goldman, Partner
- Sharon R. Klein, Partner
- Alex C. Nisenbaum, Associate

Q1. Has the definition of personally identifiable information (PII) expanded in this context? Will companies that anonymized data for sale, such as Google, be affected as this data is technically not PII?

A. The definition of "personal information" has expanded relative to the many data privacy laws in the United States. The California Consumer Privacy Act (CCPA) defines "personal information" as "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." This is much broader than, for example, the data breach notification laws of each state in the United States, which typically use a much more narrow definition (*e.g.*, first name or first initial and last name together with specified identifiers such as Social Security number, financial account numbers and the like). The CCPA does not broaden the definition of personal information for data breach notification (see answer to question 7 below). The CCPA definition is closer to the broad definition of "personal data" under the EU General Data Protection Directive.

The CCPA incorporates the concepts of "deidentified" information and "aggregate consumer information." To qualify as deidentified information, the information cannot be "linked or reasonably linkable to any consumer" and a business must implement certain safeguards not to re-identify. Aggregate consumer information cannot be "linked or reasonably linkable to any consumer or household, including via a device." Unlike HIPAA, which provides regulatory standards for when information can be considered "deidentified," the CCPA does not provide any

such standards or guidance on the issue and does not explicitly state that personal information excludes deidentified and aggregate consumer information. Accordingly, businesses may need to look to industry standards on deidentification, such as those developed by the National Institute of Standards and Technology (NIST). Presumably, if personal information met the deidentified or aggregate consumer information standards, it would not be considered personal information under the CCPA.

Q2. Companies are prohibited from selling children's data, but can they collect and leverage data for internal use or use by their subsidiaries?

A. The CCPA requires consumer opt-in to sell the data of consumers age 16 or under (or their parents' or guardians' opt-in if under 13). The CCPA does not contain special prohibitions on the collection or internal use of a child consumer's data. However, businesses that collect children's data should be mindful of their compliance responsibilities under the Children's Online Privacy Protection Act, which does significantly restrict the collection of personal data from children online. Children's information is also more likely to be considered sensitive by state and federal regulators. Additionally, the CCPA definition of "sale" is very broad, and the definition of "business" does not clearly include subsidiaries or other affiliates of the "business." Accordingly, if a business is transferring personal information to its subsidiaries, that transfer should be examined to determine whether or not it constitutes a "sale" under the CCPA.

Q3. What is the best source to monitor developments/amendments to CCPA?

Pepper is tracking updates and developments related to the CCPA, as news arises, we will issue articles and other materials on the CCPA. You can access our publications and events at https://www.pepperlaw.com/insight-center/

Q4. Are there penalties or rights of action for a mere failure to meet the CCPA's requirements versus for actual unauthorized access/breach?

A. As it stands, the state attorney general can seek penalties for any violation of the CCPA. Section 1798.155 states that "[a] business shall be in violation of this title [*i.e.*, not just a violation of the provisions of the title concerning a data

breach] if it fails to cure any alleged violation" and that such a business is subject to a civil penalty for "each violation."

On the other hand, a private cause of action can only be brought for unauthorized access/breach. Pursuant to Section 1798.150(c), "[t]he cause of action established by this section shall apply only to violations in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law." The aforementioned subdivision (a) only relates to data breach.

Q5. People with landlines have their phone number/address listed in the telephone book, unless they pay extra. This is not a government record. But is this still considered publicly available information?

This issue is an important one and a prime example of the vague nature of the CCPA. What exactly constitutes "publicly available" information will need to be clarified.

As it stands, "publicly available" is defined in Section 1798.140(o)(2) as "information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information." As drafted, the sentence is vague and ambiguous, if not nonsensical, particularly the "if any conditions. . ." language. And, as noted, a phone book is not necessarily a government record (though query whether a book published by a utility could somehow be considered quasi-governmental).

Leaving that to the side, there is an open question as to whether the legislature will continue to exempt information from the definition of "personal information" simply because it is legally available from a governmental record. First, several pieces of information can be "lawfully" ascertained from government records. Does that, in itself, make the information exempt from the statute's reach? Second, and relatedly, the governmental record may have nothing to do with the company from which the information was pilfered.

One result here may be that information is protected even if you can locate it publicly under certain circumstances — in a government record or otherwise. For

example, the legislature may determine that it is the focused nature of the collection of "personal information" and its connection with a given service or good that impacts privacy rights and makes it worthy of protection. The fact that one or more of the names/phone numbers contained therein are found in an unrelated government record (or any other public source, such as a phone book) may not be enough to eliminate protection. By analogy, defendants in trade secret cases who have stolen a protectable client list often seek to defend themselves by arguing that the client names are all available in the phone book. But it is the compilation of information in one client list and its connection to a given company or service that gives it value. A similar argument could be made here as to the reason why protections are in place over the compiled personal information at issue.

Q6. In my professional experience in ad tech, the worst actors are small tech companies with revenues under $25 million. How does this act stop them?

A. The CCPA authorizes the state attorney general to pursue a "business, service provider, or other person that violates" the CCPA.

The CCPA defines "businesses" as companies with more than $25 million in revenues, as well as companies that buy, receive, sell or share (alone or in combination) the personal information of 50,000 or more consumers, households or devices, or make more than half of their revenues selling consumers' personal information. Accordingly, even if a small ad tech company did not meet the revenue threshold, it may still be subject to the law under one of the other two thresholds.

The CCPA further defines "service provider" as "a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise

permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business."

Finally, the CCPA defines "third party" as any person (further defined to include individuals, proprietorships, firms, partnerships, companies, limited liability companies, corporations, etc. . . .) ***who is not*** the "business" as defined above, and ***who is not*** a person to whom the business discloses personal information for a business purpose pursuant to a written contact meeting certain requirements."

Presumably a "small ad tech" company would be a "third party" subject to the attorney general's reach, even if it does not fit under the "business" and "service provider" definitions.

On the other hand, it appears that a private cause of action would only apply to "businesses," as defined above.

Q7. What are the breach/violation reporting obligations for businesses? How do they reconcile with other reporting obligations under California law?

A. The CCPA does not impose any new breach *notification* obligations. But the CCPA does permit a consumer to bring a private civil action against a business if the consumer's nonencrypted or nonredacted personal information, as defined in California's existing data breach notification law, is subject to an unauthorized access and exfiltration, theft or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. California's breach notification statute can be found at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.

Q8. Is the fine per violation defined as a single record, device or incident?

A. Section 1798.150 states that the fine in a private action is assessed "per incident," but what constitutes an incident is not defined. Presumably it is each "unauthorized access and exfiltration, theft, or disclosure as a result of the

business's violation of the duty to implement and maintain reasonable security procedures and practices." However, the term "incident" is not specifically defined as such, and thus it is unclear what constitutes an "incident." Is it each time a company's server is accessed? Each time the information concerning a person, household or device is wrongfully taken from the server? Each time the information is disclosed to a third party? As it stands, there are arguments that "incident" applies to all of the above.

The answer is even murkier when it comes to what constitutes a "violation" or "intentional violation" of the CCPA for determining when the attorney general may seek a penalty. Clearly it is broader than what constitutes an "incident" giving right to a private claim.

This is just one of many issues that the legislature needs to clarify with the CCPA.

Q9. Are residents both legal and undocumented persons residing in California?

A. Residents likely include both legal and undocumented persons residing in California.

Section 1798.140(g) defines "consumer" as "a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier." Section 17014 of Title 18 of the California Code of Regulations states, "[t]he term 'resident,' as defined in the law, includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose." Seeing as how Section 17014 does not include the requirement that a resident be a legal U.S. citizen, the definition of California resident in the CCPA is likely to include undocumented persons.

This can be further supported through AB 540 and DMV procedures. AB 540 specifically allows for non-U.S. citizens to establish residency in California for tuition purposes if the student meets certain requirements, and the DMV does not require immigration documentation to prove California residency.

Q10. Can consumers request deletion or other restrictions on PII that is received or accumulated by a HIPAA-covered entity, but that is not protected health information (PHI)?

The CCPA states that it does not apply to "medical information" governed by the California Confidentiality of Medical Information Act or PHI collected by a covered entity or business associate governed by HIPAA. If the personal information is not PHI and is not otherwise excepted from the CCPA, then a consumer would be entitled to request deletion of the information and could exercise his or her other rights under the CCPA with respect to that information. Even businesses in the health care industry regulated by HIPAA are likely to collect non-PHI as part of their business (*e.g.*, employee information). Businesses should determine as part of their data inventory whether the personal information at issue is PHI (or subject to another regulatory regime that fully or partially preempts the CCPA, such as the Gramm-Leach-Bliley Act) or not.

Q11. When you say "employees," do you mean we should protect the information for California employees regardless of whether they are consumers of the product/service?

A. Yes. Section 1798.140(g) defines "consumer" as any "natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier." This definition would include California employees, and Section 1798.140(o)(1)(I) specifically provides that "personal information" includes "professional or employment-related information."

For now, this means that employees of a "business" are covered by the definition of "consumer." We do note that the California Chamber of Commerce, in its August 6 letter requesting amendments to the CCPA, raised this issue and requested clarification. To date, no amendment has been made to modify this aspect of the law.

Q12. You have referred to individuals as "consumers," but does the CCPA regulate personal information that employers retain on their own employees in the course of employment or for their business operations?

A. As mentioned in the answer above, yes. Section 1798.140(g) defines "consumer" as any "natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier." This definition would include California employees, and Section 1798.140(o)(1)(I) specifically provides that "personal information" includes "professional or employment-related information."

For now, this means that employees of a "business" are covered by the definition of "consumer." We do note that the California Chamber of Commerce, in its August 6 letter requesting amendments to CCPA, raised this issue and requested clarification, but to date, no amendment has been made to modify this aspect of the law.

Q13. Is there any legislative interest or move underway, or soon to come, to apply the law to nonprofits, such as 501c3 colleges and universities?

A. To date, we have not heard of any such legislative interest, but we will continue to monitor developments in this area and post to Pepper's website if there is an update. Our publications and other information are available at https://www.pepperlaw.com/insight-center/

Q14. If a business provides disclosure on data capture, intended use and opt-out options, is the business in compliance?

A. Many businesses are familiar with the existing disclosure obligations for online privacy policies under California and other state law. The CCPA includes similar and enhanced disclosure obligations and also imposes a number of compliance obligations beyond disclosure — for example, businesses must build in internal processes to be able to comply with new consumer rights and update internal policies and contracts with vendors. For more information about the CCPPA requirements, please see our article available at

https://www.pepperlaw.com/publications/california-consumer-privacy-act-european-style-privacy-with-a-california-enforcement-twist-2018-07-10/

Q15. Many direct marketers already have privacy policies that provide for intended use of sharing data with other companies for relevant marketing offers. Is this sufficient?

A. Disclosure required by the CCPA also includes a strong focus on disclosing consumers' rights over their data in addition to being informed about whom it is shared with, so those details will need to be included in disclosures. As mentioned above, these disclosure obligations must also ensure businesses can respond to consumer requests within the 45-day time period. More information is available in our article, available at https://www.pepperlaw.com/publications/california-consumer-privacy-act-european-style-privacy-with-a-california-enforcement-twist-2018-07-10/.

Q16. A**re commercial vendors for nonprofit organizations exempt?**

A. If a third-party commercial vendor serves as a service provider for a nonprofit organization, that commercial vendor could still be subject to the CCPA's direct requirements if it otherwise meets the definition of a "business." In other words, a "business" does not become exempt by virtue of serving as a vendor or service provider to an exempt entity.

Q17. If a business has more than $25 million of revenue from California, but does not buy or sell any PII/consumer data, does the act still apply? (Is California revenue enough to fall within the scope, even if you do not sell any info about your employees or customers?)

A. The CCPA applies to businesses that "collect" personal information, not just businesses that "sell" personal information. "Collect" is defined very broadly as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior." So the act of collecting the information of employees, if those employees are California residents, would, providing the other thresholds

are met, subject a business to the CCPA. Also, as written, the CCPA requires only that a business "does business in the State of California," not that a business have $25 million in annual gross revenue attributable to California.

Q18. Does the CCPA apply to pharmacies? We collect medical information to take care of patients and follow HIPAA.

A. If the pharmacy is a "covered entity" governed by HIPAA (or California's Confidentiality of Medical Information Act), then any PHI collected by the entity is exempt from the CCPA requirements (although still regulated by other laws). However, any data collected by the pharmacy that is not considered PHI (for example, employee information) would not be exempt and is subject to the CCPA. (See answer to Q10 above.)

Q19. Can you clarify whether a company's employee data for employees in California is covered by the CCPA? It is not really a consumer transaction, but the definition of personal data in the Act is very broad.

A. A company's employee data for employees in California is covered by the regulation. Currently, Section 1798.140(o)(1)(I) defines "personal information" to include "professional or employment-related information." Additionally, Section 1798.140(g) defines "consumer" as any California resident, which would include California employees.

Q20. GDPR contemplates the idea of a "data controller" and "data processor." The new Cayman and Bermuda privacy laws only contemplate "data controllers." Does the CCPA contemplate both data controller and processor, or just controller?

A. Unlike GDPR, the CCPA does not distinguish between the concepts of "controller" and "processor," and so, effectively, all entities are equally subject to the CCPA if they qualify as a "business" under the law. However, to qualify as a "business" subject to the CCPA, the business must "alone, or jointly with others," determine "the purposes and means of the processing of consumers' personal information." This language is from the definition of "controller" under the GDPR. Unfortunately, there is not yet any guidance as to what "purpose and means" of

processing should be interpreted under the CCPA. The CCPA also includes the concept of "service providers," to which businesses must flow down certain requirements by written contract and which may be liable for violations of the CCPA as well. Finally, each business should be aware that it needs to evaluate its posture with respect to each type of data (*e.g.*, a business will not be a service provider with respect to its own employees' data).

Q21. For the annual gross revenues threshold of $25 million, is this from California residents or worldwide?

A. Unlike the California Transparency in Supply Chains Act (Cal. Civ. Code § 1714.43(a)(1)) and California Revenue and Taxation Code Section 17942(a)(2), which have expressly defined their scope to "annual worldwide gross receipts" or "total income from all sources derived from or attributable to this state," CCPA Section 1798.140(c)(1)(A) does not specify whether the $25 million annual gross revenue threshold includes a company's California revenue or global sales.

Instead, Section 1798.140(c)(1) limits the CCPA to apply only to for-profit companies that do business in California, and Section 1798.145(a)(6) makes an exception if the company's "commercial conduct takes place wholly outside of California." Although still vague, these sections make it seem more likely that the $25 million gross revenue threshold is for the company's global sales, rather than its California revenue, because, consistent with the CCPA's purpose of protecting California consumers, the CCPA should apply to as many companies doing business in California.

Q22. Like GDPR, does the CCPA regulate only PI of California residents? What are the penalties (10 percent revenue in GDPR)?

A. The CCPA regulates any business "that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more" of the specified thresholds ($25 million in annual gross revenue, 50,000 or more records, derives 50 percent or more annual revenue from selling consumers' personal information). A "consumer" is

defined as a California resident. It does not apply to the personally identifiable information of residents of other states or countries.

Individuals may bring private rights of action and recover $100-$750 per violation or actual damages, whichever is higher. Consumers must notify the California attorney general before initiating an action. If the California attorney general chooses to prevent the consumer from bringing the action and brings the action itself, civil penalties can rise to $2,500 per violation or $7,500 per intentional violation.

Q23. GDPR fell very hard on some companies, even though they did not have consumer PII but rather had PII for, in some cases, thousands of employees. Does the CCPA apply to employee PII?

A. As mentioned in some answers above, yes. Section 1798.140(g) defines "consumer" as any "natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier." This definition would include California employees, and Section 1798.140(o)(1)(I) specifically provides that "personal information" includes "professional or employment-related information."

For now, this means that employees of a "business" are covered by the definition of "consumer." We do note that the California Chamber of Commerce, in its August 6 letter requesting amendments to the CCPA, raised this issue and requested that the law only apply to "consumers." To date, no amendment has been made to modify this aspect of the law.

Q24. Has the law defined "devices"?

A. Yes. "Device" is defined in Section 1798.140(j) as "any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device."

Q25. What is impact to a B2B company that stores customers' not personally identifiable info (*i.e.*, name and business email, phone number)?

A. The definition of personal information under the CCPA is quite broad, as is the definition of "consumer." As discussed above, the definition of "consumer" also applies to employees of a business, and, as such, the type of information you describe, although connected to a person's business contact information, is still "personal information" under the CCPA because it "relates to" a "consumer" as defined by the CCPA.