Insurance Coverage Law Report

# READING THE FINE PRINT: WHAT INSURANCE COMPANIES NEED TO KNOW ABOUT THE CCPA

**Winter 2020**

*By Kirk J. Nahra and Ali A. Jessani*

*The purpose of this article is to provide background information on the California Consumer Privacy Act and specifically the exemptions that generally will be applicable to the insurance industry. While developing a compliance plan will require an in-depth analysis of the specific information that an insurance company collects, this article also poses questions that insurance companies should be considering as they finalize their compliance plans.*

As businesses everywhere rush to comply with the California Consumer Privacy Act ("CCPA"), which became effective January 1, 2020, insurance companies find themselves in a particularly precarious position because of the sheer amount of information they collect. All aspects of insurance—from accepting an application to underwriting to handling a claim—involve processing, transferring, and storing consumer information. While life and health insurance companies may collect different information than say property and casualty insurers, the collection and dissemination of consumer information permeates the industry, which makes the CCPA and its extensively broad definition of protected "personal information" troublesome for all insurance businesses.

CCPA compliance may be especially problematic for those insurance companies looking to take advantage of the efficiencies that Big Data and new technology have to offer, as they may collect information that is not covered by other privacy laws. This distinction is important because information collected pursuant to laws that have traditionally applied to insurance companies, such as the Gramm-Leach-Bliley Act ("GLBA"), the California Financial Information Privacy Act ("CFIPA"), the Health Insurance Portability and Accountability Act ("HIPAA"), and the Fair Credit Reporting Act ("FCRA"), is exempt from the CCPA. The CCPA does not, however, provide insurance companies with an industry-wide exemption or provide financial institutions subject to the GLBA with an entity-wide exemption,[1] which means that insurance companies that meet certain threshold requirements and collect personal information from California residents in certain situations will have to comply with the law in some form or fashion. Understanding the scope of the applicable exemptions will be critical for insurance companies to recognize their compliance responsibilities under the CCPA.

The purpose of this article is to provide background information on the CCPA and specifically the exemptions that generally will be applicable to the insurance industry. While developing a CCPA-compliance plan will require an in-depth analysis of the specific information that an insurance company collects, this article also poses questions that insurance companies should be considering as they finalize their compliance plans.

## Background

The California legislature passed the CCPA on June 28, 2018 as an alternative to statewide voting on a comprehensive data privacy law through a ballot initiative. The law has been amended twice already, once a few months after its initial passage and most recently on October 11, 2019, after Governor Gavin Newsom signed into law amendments passed during the 2019 legislative session. The California Attorney General ("California AG"), the person responsible for interpreting and enforcing the CCPA, recently proposed regulations aimed at clarifying the law, which were open to comments until December 6, 2019.[2] The law went into effect on January 1, 2020, though the California Attorney General cannot bring any enforcement actions until July 1, 2020. CCPA enforcement can be retroactive, however, which means that businesses need to focus their compliance activities on January 1st.

Essentially, the CCPA requires businesses[3] that collect personal information from California residents to provide those residents with certain data privacy rights, such as the right to access the categories of information and the specific pieces of information that a business has on file,[4] the right to have their information deleted,[5] and the right to opt-out of the sale of their personal information.[6] Personal information under the CCPA means "information that identifies, relates

to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"[7] and includes a broad range of categories such as biometric information, IP addresses, and inferences drawn about a consumer related to their preferences, predispositions, and psychological trends.[8]

The CCPA's exact requirements could be their own law review topic. For the purposes of this article, insurance companies should be aware that the CCPA, in addition to requiring businesses to provide consumers with individual data privacy rights, also creates additional requirements for businesses. Companies must, for example, include certain provisions in their privacy policies[9] and update them annually,[10] as well as provide a button on their websites that allows consumers to opt out of the sale of their personal information[11] (to the extent applicable). Businesses must also include certain language in their contracts with their service providers to ensure that the information they provide to them is not considered to be "sold" under the law.[12] These requirements (and more) will make the CCPA the most comprehensive data privacy law in the United States, as well as perhaps the most burdensome from a business perspective.

### Important Exceptions

Notably, the CCPA exempts "personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, and implementing regulations, or the California Financial Information Privacy Act."[13] Most insurance companies that deal directly with consumers and do business in California have long been compliant with the GLBA and CFIPA and can continue to follow the requirements of those laws for the vast majority of information they collect without adding the CCPA's obligations. Consumer-facing insurance companies should be aware, however, that information they collect that does not fall under the purview of the GLBA or CFIPA (i.e., information that is not collected from a "consumer" or "customer," as those terms are defined in those laws) will still be subject to the requirements of the CCPA. Meanwhile, commercial insurance providers—who may have been lucky enough to fall outside of the GLBA's requirements—will not be so fortunate when it comes to the CCPA: Any information they collect on California residents that is not subject to the GLBA or CFIPA (or falls under any other exception) will likely be subject to the CCPA.

To understand how information might fall outside of the GLBA exemption, consider a situation where a California resident suffers a car crash and contacts their insurance company regarding a claim. The insurance company has a relationship with the claimant and (hopefully) sends them a GLBA notice, so the information they collect from the claimant is likely subject to the CCPA's GLBA exemption. But the insurance company may also collect personal information regarding the other party to the crash, as well as information about other individuals— such as the owner of the body shop where the claimant's car is being repaired—as part of processing the claim. Information about these individuals will likely not fall under the GLBA exemption because they have no "consumer" or "customer" relationship with the insurance company. But the insurance company may still have their information on file, which means that they may have to provide these individuals with CCPA rights.

The CCPA also exempts protected health information that is collected by a covered entity or business associate that is subject to HIPAA,[14] as well as activities involving the collection, maintenance, disclosure, sale, communication, or use of any personal information relating to a consumer report by a "consumer reporting agency," "furnisher," or "user" of a consumer report, as those terms are defined in FCRA.[15] Again, these are not entity-wide exemptions, which means that insurance companies looking to avoid CCPA obligations by relying on one or more exceptions to the law should document their reliance (more on this later).

Two of the CCPA amendments that were signed into law during the 2019 legislative session create additional exemptions that will help all businesses, including insurance companies, with CCPA compliance—at least for the first year that the law is effective. Assembly Bill 25 exempts information that a business collects about employees, job applicants, officers, directors, owners, and contractors that is related to the context of those relationships.[16] This "employee exemption" seems reasonably clear. Meanwhile, Assembly Bill 1355 exempts personal information collected by businesses in instances where the consumer is an employee, owner, director, officer, or contractor of a government agency or business whose communications or transactions with the business occur solely in the context of the business conducting due diligence regarding or providing or receiving a product or service to or from that business or government agency.[17] This exemption—which applies to certain personal information collected in "B2B" situations—is both confusing and incomplete. For example, even with the exemption, B2B information is not exempt from the obligation of providing an opt-out before the sale of personal information.[18]

Both the employee and B2B exceptions are set to expire on January 1, 2021 but will likely be taken up again by the California legislature in 2020. Insurance companies should also note that, even if they collect or otherwise process personal information that falls under an exemption, the California Attorney General's proposed regulations will still require businesses to notify California residents, upon receiving verified request, when they refuse to provide CCPA rights based on an exclusion to the law.[19]

## How Can Insurance Businesses Prepare for the CCPA?

CCPA compliance will vary for every business depending on their particular needs and the same is true for the insurance industry. Consumer-facing life insurance companies will have a different compliance strategy than commercial insurers who provide workers' compensation policies, for example. Nevertheless, there are general questions that all insurance companies need to be asking themselves, which we highlight below.

*1. Do you have CCPA obligations?*

Unless you do not meet the threshold requirements of a "business," the answer is almost certainly yes. Even those insurance companies who only collect information pursuant to the GLBA will likely have some obligations under the CCPA because, as noted earlier, the California AG's proposed regulations require businesses to tell consumers when they are relying on an exemption to deny a consumer their CCPA rights.[20] The proposed regulations also require businesses to implement training and record-keeping requirements.[21] Because the CCPA does not exempt GLBA institutions and only exempts GLBA information, insurance companies will also likely have to comply with these requirements, even if the only training they have to provide employees is in regards to properly denying consumer requests.

*2. Are you able to track your data?*

Data tracking will be critical for any business that is looking to comply with the CCPA, but it will be especially important for insurance companies looking to rely on the various exemptions available to them. Tracking your data in CCPA context for insurance companies means identifying the categories of consumers for whom you collect information and determining whether they fall under an exemption to the law. Most of this will be easy. Almost all of your individual policyholders, for example, will be subject to the GLBA exemption. In other contexts, it will be trickier. In the example given earlier involving an insurance company processing a claim after an accident, that company will have to account for the other parties involved with the claim that are not the claimant (e.g., the other party to the accident, body shop owner, any potential doctors) and ensure that they are prepared to respond to CCPA requests with respect to those parties (unless a different exemption applies).

*3. Have you updated your GLBA notice?*

Insurance companies that are GLBA-compliant may have previously taken their annual GLBA notices for granted. Those looking to rely on the GLBA as a way to minimize CCPA obligations now need to ensure that their GLBA notices are up-to-date and holistically reflect their data collection practices so that consumers and regulators are aware as to what information is covered under the GLBA.

*4. Do you have a compliance plan in place?*

Regardless of whether yours is a business that collects all of your information pursuant to the GLBA or if the GLBA does not apply to you at all, you will need to implement some sort of a CCPA-compliance plan. The particular elements of the plan will vary. Some businesses will collect more information outside of the GLBA than others, which means they will spend more time developing a mechanism for California residents to exercise their rights under the law. Others will mostly avoid having to provide CCPA rights but will still need to comply with other parts of the law. Again, unless you do not qualify as a business or do not operate in California, the CCPA will likely apply to you.

One element of a CCPA compliance plan that all companies need to be thinking about is whether to employ a local or a national strategy. In other words, should you limit CCPA compliance to whom the law applies to (California residents) or should you preemptively offer CCPA protections to all customers? There are pros and cons to both options. On one hand, limiting CCPA compliance to California residents may reduce the costs associated with compliance, especially since the number of people who are likely to exercise their rights under the CCPA will be minimal. On the other hand, providing all customers with CCPA rights can help companies use CCPA-compliance as a marketing strategy, as well as prepare companies for other state laws that may mirror the CCPA. We should note, however, that there is no guarantee that other state comprehensive privacy laws will copy the CCPA. For example, Washington—the state that came the closest to adopting such a law in 2019—passed a bill through its state senate that differed from the CCPA in many respects, including in its definitions of "personal information" and "sale" and through the fact that it explicitly required businesses to obtain consent prior to using facial recognition services.[22] Thus, if other states join California in 2020 and pass comprehensive data privacy laws, there is no guarantee that CCPA-compliance will mean automatic compliance with the requirements of those other laws.

*5. Have you updated your service provider contracts?*

Another critical element of CCPA compliance will be properly categorizing your relationships under the law in terms of your service providers. The CCPA has a very specific definition of a "service provider": It is defined as 1) a for-profit entity that 2) processes information on behalf of a business 3) to which the business discloses a consumer's personal information for a business purpose 4) 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 [the CCPA], including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business."[23] Insurance companies will need to include this CCPA "magic language" in all of their written contracts with their service providers to ensure that those relationships are treated as business/service-provider arrangements.

*6. Have you evaluated whether you "sell" personal information?*

The reason it is important for your service providers to meet the definitional requirements of the CCPA is because otherwise they will be considered to be "third parties"[24] in relation to the information you provide to them. To the extent there is any "monetary or other valuable consideration" being given in relation to an exchange of personal information between a business and a business or a business and a third party (and there is not a proper service provider contract in place), the information will be considered to be "sold" under the CCPA,[25] which means that consumers will have the right to opt-out of this exchange. Insurance companies subject to the CCPA need to evaluate where possible "sales" are occurring in relation to the information they share with the various entities they work with and determine: 1) whether a CCPA-compliant service provider contract can implemented between the two parties; 2) whether the relationship between the two parties is governed by the GLBA or another law that puts it outside of the purview of the CCPA; or 3) how to operationalize providing consumers with the right to opt-out in relation to this information.

Insurance companies also need to be aware that the term "sell" is defined broadly under the CCPA, such that information they would not otherwise considered be sold may still be considered as such under the law. For example, information disclosed to industry associations that accumulate data in order to prevent fraud or provide other services across the industry (and who, as a result, may not be able to abide by the CCPA's contractual restrictions for service providers because they share information across their membership) may be considered "sold," unless it falls under an exemption to the law.

*7. Are you properly protecting the personal information you have on file?*

Even if all of the personal information you process is subject to the GLBA exemption, you could still be susceptible to the CCPA's private right of action,[26] which applies to data breaches. To the extent that you have nonencrypted and nonredacted personal information and it is subject to "unauthorized access and exfiltration, theft, or disclosure as a result of the [your] violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information…,"[27] a consumer may bring a private right of action against you for damages that can be as high as $750 per consumer per incident (or actual damages).[28]

A few points about the CCPA's private right of action. First, the definition of personal information as it applies to the private right of action is far narrower than the definition used in the rest of the law.[29] Second, unlike actions brought by the California AG for privacy violations, the CCPA's private right of action is enforceable beginning on January 1, 2020. Third, prior to a consumer bringing an individual or class action lawsuit under the CCPA, the consumer must first provide a business with 30 days' written notice identifying the specific provisions of the CCPA that the consumer deems to have been violated and providing the business an opportunity to "cure" the alleged violations.[30]

Lastly, neither the CCPA nor the draft regulations define "reasonable" security procedures and practices. Insurance companies may be able to rely on other insurance laws governing information security, such as the National Association of Insurance Commissioner's ("NAIC") Data Security Model Law,[31] for standards as to what courts may deem to be reasonable when it comes to protecting personal information collected in the insurance context.

## Conclusion

We are still awaiting final regulations from the California Attorney General's office, but unless the law drastically changes, CCPA-compliance will be a major undertaking for insurance companies. And while the various exemptions offer some recourse, no insurance company can completely rely on them to absolve themselves of all of their responsibilities under the law. All businesses (as defined in the CCPA) that operate in California would be best advised to be in compliance, or else risk enforcement fines that could be as high as $7,500 per violation.[32]

## About the Authors

**Kirk J. Nahra** is a partner with **WilmerHale** in Washington, D.C., where he co-chairs the firm's global Cybersecurity and Privacy Practice. He assists companies in a wide range of industries in analyzing and implementing the requirements of privacy and security laws across the country and internationally. He provides advice on data breaches, enforcement actions, contract negotiations, business strategy, research and de-identification issues and privacy, data security and cybersecurity compliance, for companies ranging from Fortune 500 companies to start-ups. A graduate of Georgetown University and Harvard Law School, he teaches Information Privacy Law and Health Care Privacy Law at the Washington College of Law at American University. He also is a fellow with the Cordell Institute for Policy in Medicine & Law at Washington University. He can be reached at kirk.nahra@wilmerhale.com.

**Ali A. Jessani** is an associate in the Cybersecurity and Privacy Practice at **WilmerHale**, in the Washington, D.C., office. He counsels clients on the privacy, cybersecurity and regulatory risks presented by new and proposed uses of technology and consumer information. Specifically, he advises clients with compliance issues related to the California Consumer Privacy Act, the General Data Protection Regulation, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, state biometric laws and other federal and state laws governing data sharing, ownership, and protection. Mr. Jessani also guides companies through regulatory investigations, as well as legal obligations after data breaches. He can be reached at ali.jessani@wilmerhale.com.

### Notes

[1]. This is different from other privacy laws, such as Nevada's online privacy law and Illinois's Biometric Information Privacy Act, which provide entity-level exemptions to financial institutions subject to the GLBA.

[2]. The draft regulations are available at: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-proposed-regs.pdf.

[3]. A "business" under the CCPA is defined as a for-profit entity that collects personal information (or has personal information collected on its behalf) and that alone, or jointly with others, determines the purposes and means of processing consumers' personal information while also meeting one of the following threshold requirements: 1) has annually gross revenues in excess of $25 million; 2) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, in alone or in combination, the personal information of 50,000 or more consumers; or 3) derives 50 percent or more of its annual revenue from selling consumers' personal information. Cal. Civ. Code § 1798.140(c)(1).

[4]. Cal. Civ. Code § 1798.100; Cal. Civ. Code § 1798.110; Cal. Civ. Code § 1798.115.

[5]. Cal. Civ. Code § 1798.105.

[6]. Cal. Civ. Code § 1798.120.

[7]. Cal. Civ. Code § 1798.140(o)(1).

[8]. *Id.*

[9]. *See* Cal. Civ. Code § 1798.130(a)(5); *see also* 11 CCR § 999.308(b).

[10]. Cal. Civ. Code § 1798.130(a)(5).

[11]. Cal. Civ. Code § 1798.135(a)(1).

[12]. *See* Cal. Civ. Code § 1798.140(v) (definition of "service provider").

[13]. Cal. Civ. Code § 1798.145(e); Gramm-Leach-Bliley Act (Public Law 106-102).

[14]. Cal. Civ. Code § 1798.145(c)(1).

[15]. Cal. Civ. Code § 1798.145(d)(1).

[16]. Cal. Civ. Code § 1798.145(g)(1).

[17]. Cal. Civ. Code § 1798.145(m)(1).

[18]. *See id.*

[19]. 11 CCR § 999.313(c)(5); 11 CCR § 999.313(d)(6).

[20]. *Id.*

[21]. 11 CCR § 999.317.

[22]. *See* Washington Senate Bill 5376 (2019-2020), available at: http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376.pdf. This bill did not pass the Washington state house of representatives.

[23]. Cal. Civ. Code § 1798.140(v).

[24]. The CCPA defines a "third party" essentially as an entity that does not fall under the definition of a "business" or a "service provider" under the law. *See* Cal. Civ. Code § 1798.140(w).

[25]. *See* Cal. Civ. Code § 1798.140(t)(1) (definition of "sell").

[26]. The CCPA's GLBA exemption specifically notes that it does not apply to the private right of action. *See* Cal. Civ. Code § 1798.145(e) (… "This subdivision shall not apply to Section 1798.150").

[27]. Cal. Civ. Code § 1798.150(a)(1).

[28]. Cal. Civ. Code § 1798.150(a)(1)(A).

[29]. The only information that is subject to the private right of action is information that is protected under California's data breach statute, which is: (A) an individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements (i) social security number; (ii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iii) medical information; (iv) health insurance information; and (v) unique biometric data. Cal. Civ. Code § 1798.150(a)(1); *see also* Cal. Civ. Code § 1798.81.5(a)(1)(A) (definition of "personal information" under California's data breach statute).

[30]. Cal. Civ. Code § 1798.150(b). Since the private right of action only seems to apply to data breaches and the rest of the CCPA addresses potential privacy violations, it is unclear as to what specific provisions of the CCPA a plaintiff would allege have been violated when asking a business to cure (except for the provision that provides the private right of action itself).

[31]. *See* NAIC Model Law 668, available at: https://www.naic.org/store/free/MDL-668.pdf.

[32]. Cal. Civ. Code § 1798.155(b).