Scott A. Sinder
202 429 6289
ssinder@steptoe.com

1330 Connecticut Avenue, NW
Washington, DC 20036-1795
202 429 3000 main
www.steptoe.com

Steptoe
STEPTOE & JOHNSON LLP

November 16, 2018

TO: The Council of Insurance Agents & Brokers

FROM: Scott A. Sinder
Eva V. Rigamonti

RE: **California Consumer Privacy Act of 2018**

On June 28, 2018 California Governor Jerry Brown signed CA AB-375, the California Consumer Privacy Act of 2018 (CCPA or the Act) into law. The CCPA is widely regarded as the nation's most aggressive data privacy law to date, and as its name suggests it is a privacy law; it does not focus on data security or data breach notification requirements. More akin to the European Union's General Data Protection Regulation than cybersecurity legislation, such as the NAIC data security model law or the New York State Department of Financial Services' cybersecurity regulation, the CCPA focuses on business information collection practices and a consumer's right to find out about that data collection. The legislation will impose significant disclosure obligations on companies when it goes into effect on January 1, 2020. **Insurance agents and brokers generally should be exempt from the Act's requirements unless they are collecting data related to internet searching and browsing activities.**

The Act, which is described in more detail below, requires businesses to inform consumers about what types of personal information they hold and the entities with whom they share (or to whom they sell) that information—and it gives consumers the ability to control how those businesses use that information. A consumer has the right to ask companies to delete that information and to opt out of the data collection and data sharing. Companies will be prohibited from charging individuals or otherwise discriminating against them because they chose to opt out of having their data shared.[1]

On September 23, 2018, the CCPA was formally amended by CA SB 1121, which expanded and clarified the exemption for institutions regulated by the Gramm-Leach-Bliley Act (GLBA). Under the amended CCPA, insurance carriers and producers will be exempt from the legislation with respect to the 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."[2]

---

[1] CCPA §1798.125. The CCPA does permit a company to offer financial incentives to consumers if they share data.

[2] CCPA § 1798.145(e) as amended by California Senate Bill 1121 (Sept. 23, 2018)(noting in its preamble: "The bill would also prohibit application of the act to personal information collected, processed, sold, or disclosed pursuant to a specified federal law relating to banks, brokerages, *insurance companies*, and credit reporting agencies, among others, and would also except application of the act to that information pursuant to the California Financial Information Privacy Act."(emphasis added)).

It will be important, however, for Council members to confirm that they are not engaging in data tracking relating to website search/browsing, advertisements, etc. that would not be covered by the GLBA exemption. *If they are engaged in such non-GLBA data collection practices, then the CCPA's requirements will apply for <u>that data</u>*. In other words, companies will have to notify consumers about the non-GLBA data they are collecting and provide consumers with the ability to opt out of that data collection etc.

In addition, even if a company is generally exempt from the CCPA via the GLBA or another exemption, the Act creates a private right of action for consumers to seek statutory damages of "not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater" if the business is subject to a data breach and the consumer's nonencrypted or nonredacted personal information is compromised.[3] This private right of action would apply even to businesses that can otherwise claim a GLBA exemption. In short, the CCPA creates a strict liability model for the breach of unencrypted or unredacted personal information. Thus, Council members should consider whether to encrypt any (or all) consumer data they hold to avoid the potential penalties under the Act in the event the company suffers a data breach.

Below is a more detailed summary of the CCPA as it stands today. Since the Act was rushed through the California legislature in a week, however, it is expected that the Act will continue to be amended in the coming months and the effective date may be delayed.[4]

<u>Summary of the California Consumer Privacy Act of 2018</u>

1. What does the CCPA do?

The CCPA gives consumers – defined as a "natural person who is a California resident" – the ability to control how companies use and share their personal information.[5] Specifically, the Act grants a consumer the right to:

> (1) Know what type of data a business holds about the consumer and the right to request that a business that collects the consumer's personal information disclose to that consumer what categories and *specific pieces* of personal information the business has collected,[6] (i.e., "the right to know")

[3] CCPA §1798.150.

[4] The Act was rushed through the legislature to head off a voter-driven privacy initiative that would have been much more onerous for businesses. Since passage in June 2018, many groups have worked to tweak and fix the legislation.

[5] Under the legislation, a "consumer" is defined as "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." CCPA §1798.140(g).

[6] CCPA §1798.100(a), 110(a).

(2) Request that a business that sells the consumer's personal information, or discloses it for business purposes, disclose that fact to the consumer,[7] (i.e., "the right to know to/with whom the data is shared")

(3) Request that the business delete any personal information about the consumer,[8] (i.e., "the right to delete");

(4) Direct a business that sells personal information about the consumer to third parties not to sell that information (the "right to opt out");[9] and

(5) Receive equal treatment (i.e., services and cost), whether or not the consumer exercises the rights described above (the "right to equal treatment").[10]

Thus, businesses will have to disclose to consumers both the type of data they collect and the entities with whom they share information. Companies will also have to:

(1) Have a privacy policy and disclose to the consumer (at or before the point of collection) what categories of personal information are being collected and for what purpose the data will be used;[11]

(2) Make available two or more designated methods for consumers to submit information requests;[12]

(3) Disclose the required information to the consumer free of charge and within 45 days of receiving the information disclosure request;[13]

(4) Provide a "clear and conspicuous" link on the business' homepage saying "Do Not Sell My Personal Information" that allows a person to opt out of having their personal information sold along with a description of the consumers' rights.[14]

2. What "personal information" is protected under the CCPA?

[7] CCPA §1798.115(a).

[8] CCPA §1798.105(a).

[9] CCPA §1798.120(a). Under the CCPA, a business may not sell the personal information of minor consumers (under 16 years old) without their affirmative consent. For minor consumers under 13 years, the minor's parent or guardian must provide affirmative consent.

[10] CCPA §1798.125.

[11] CCPA §1798.100(b).

[12] CCPA §1798.130(a)(1)(at minimum: a toll free telephone number and a website address).

[13] CCPA §1798.130(a)(2).

[14] CCPA §1798.135(a)(1).

The CCPA defines "personal information" as 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."[15] In short, the legislation covers a broad swath of information including, but not limited to:

- "Commercial information" (including "records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies");
- 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 Web site, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act; and
- Inferences drawn from any of the information specified in the Act to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

In layman's terms: many types of data, including "clicks" on online advertisements, browsing history or search data on a company's website, "cookies," profile data posted on Facebook/twitter, etc. would be covered under the CCPA.

3. What businesses are covered by the CCPA?

The law will apply to any for profit business that "collects consumers' personal information, or on the behalf of which such information is collected," does business in California, and that (1) has more than $25 million in annual gross revenue, (2) alone or jointly sells or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or (3) derives 50 percent or more of its annual revenues from selling consumers' personal information.[16] In addition, the CCPA covers corporate affiliates that share common branding with those businesses.[17]

---

[15] CCPA §1798.140(o).

[16] CCPA §1798.140(c)(1). ("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 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 following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000). (B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.")

[17] CCPA §1798.140(c)(2)(" Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.")

4. What businesses are exempt under the CCPA?

The legislation contains exemptions for protected or health information collected under the California Confidentiality of Medical Information Act or the Health Insurance Portability and Availability Act of 1996 (HIPAA)[18] as well as personal information collected under the GLBA.[19] These carve outs should, in almost all instances, exempt insurance producers from the CCPA.

The GLBA regulates covered entities' collection and use of nonpublic personal information, provided it is "personally identifiable financial information" that is (i) provided by a consumer to a financial institution, (ii) results from any transaction with a consumer or any service performed for the consumer, or (iii) is otherwise obtained by the financial institution.[20] Yet, the CCPA captures many other types of data. Thus, any data collection – such as tracking cookies or search data on a company's website – that goes beyond the GLBA and strays into the CCPA purview may trigger requirements under the Act. Insurance producers should review their data collection practices to determine whether they engage in any data collection that is not covered by the GLBA.

5. What penalties does the Act impose?

If a business is subject to a data breach and the consumer's nonencrypted or nonredacted personal information is compromised, the CCPA creates a private right of action for consumers to seek statutory damages of "not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater."[21] In addition, if a business violates the Act, and fails to cure any alleged violation within 30 days of being notified of the alleged violations, it shall be "liable for a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation."[22]

---

[18] CCPA §1798.145(c).

[19] CCPA § 1798.145(e). The CCPA also contains an exemption for "the sale of personal information to or from a consumer reporting agency [if used to generate a consumer report]… and use of that information is limited by the federal Fair Credit Reporting Act." *See* § 1798.145(d).

[20] 15 U.S.C. § 6809.

[21] CCPA §1798.150.

[22] CCPA §1798.155(b)("A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.")