**LAW OFFICE OF ALAN J. THIEMANN**

**ATTORNEYS AT LAW**

**700 12th Street, NW, Suite 700 Washington, DC 20005**

**(202) 904-2467**

**M E M O R A N D U M**

**TO:** William G. Harris, CEO ATP Board of Directors

**FROM:** Alan J. Thiemann, General Counsel

DATE: September 18, 2018

**RE:** **California Consumer Privacy Act**

The California Legislature passed the California Consumer Privacy Act (“CCPA”) on June 28, 2018, and it was signed into law by Governor Brown the same day. The law was hastily enacted in order to preempt a proposed voter referendum on a stricter privacy law and take it off the November ballot (generally, the language in a voter referendum cannot be changed). Subsequently, on August 31, 2018, the California Legislature passed a separate bill (SB 1121) to make technical changes to the CCPA, but which largely preserved the substance of the CCPA.

The CCPA, which goes into effect Jan 1, 2020, grants consumers unprecedented control over their personal information. Indeed, it places into California law a significant number of data subject rights that are similar to the requirements of the EU General Data Protection Regulation (“GDPR”), although significantly, the CCPA is principally an “opt-out” law, while the GDPR is an “opt-in” law.

The CCPA also imitates GDPR’s emphasis with fines for violations, but the original provision creating a private right of action was changed in the August amendments – consumers may only sue for data breaches and not violations of CCPA (clarifying that a private right of action set forth in **§**1798.150(a) only applies to “violations” that are security incidents as described in CA CIVIL CODE **§**1798.150(a)).  Additionally, the recent amendments also delayed enforcement by the California Attorney General until July 1, 2020 (or one year after the AG promulgates implementation regulations), thereby giving businesses more time to get ready to comply.

At the most basic level, the law allows California residents to: (1) see what data companies collect on them; (2) request that it be deleted; (3) know what third-party companies their data has been sold to; and (4) direct businesses to stop selling that information. Among concerns that have surfaced about the new law is that there are a few “loopholes.” Apparently, technology companies can "share" a person’s data even if the consumer bars them from selling it and the law allows companies to charge higher prices to consumers who opt out of having their data sold.

Essentially, at a high level, the scope of the CCPA’s definitions for “collection” and “selling” information in the CCPA are similar to the GDPR definition of “processing.” However, while there are many overlapping elements, the GDPR definition of processing is much broader. As noted above, companies may be able to “share” personal information even if the individual has directed that such information cannot be sold.

Californian residents are not merely protected in their roles as consumers, but also as employees, patients, tenants, students, parents, children, etc. Cal. Civ. Code §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 situation portends a major concern, including for testing organizations, about how to treat customer representatives who provide contact information not in a personal capacity, but purely on behalf of their employer who is a customer. On the other hand, the regulations define a “resident” to include: “(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," subject to a number of clarifications and specifications set forth in Section 17014 of Title 18 of the California Code of Regulations. This definition resolves the questions that have arisen about the GDPR concerning transient individuals.

Under the CCPA, Cal. Civ. Code §1798.140(o)(1) defines the term "personal information" broadly as "any information that ... relates to ... a particular consumer or household." Thus, data can be protected even if it does not relate to a single individual and if it does not contain a name. For example, annual water or energy consumption of a household, a particular employee's job description, an Internet Protocol address, web browsing history and "purchasing tendencies" will be regulated as personal information, even if no names are associated with it. And, the issue about the relationship of a customer contact represents a real threat.

A number of limited and complex exceptions apply to this definition of personal information. For example "publicly available information" (Cal. Civ. Code §1798.140(o)(2)) and "commercial conduct [that] takes place wholly outside of California" (Cal. Civ. Code §1798.145(a)(6)) are excluded. However, a number of open questions remain unaddressed at this point.

The CCPA specifies that PI includes, but is not limited to: (i) identifiers, such as names, aliases, addresses, and IP addresses; (ii) characteristics of protected classifications under California or federal law; (iii) commercial information, including records of personal property, products or services purchased, or consuming histories or tendencies; (iv) biometric information; (v) Internet or other electronic network activity information, such as browsing history; (vi) geolocation data; (vii) audio, electronic, visual, thermal, olfactory, or similar information; (viii) professional or employment-related information; (ix) education information; and finally, (x) any inferences drawn from any of the information identified to create a profile about a consumer. The Act does, however, include a few limitations. First, the Act excludes “aggregate consumer information,” which is defined as data that is “not linked or reasonably linkable to any consumer or household, including via a device.” Data kept in such a fashion does not fall within the definition of PI. Second, information that is publicly available from federal, state, or local government records is similarly excluded.

Who Must Comply?

Companies around the world have to comply with the California Consumer Privacy Act if they receive personal data from California residents and if they — or their parent company or a subsidiary — exceed one of three thresholds: (a) annual gross revenues of $25 million (but it is unclear whether this is “worldwide” or just in California); (b) obtains personal information of 50,000 or more California residents, households or devices annually; or (c) 50 percent or more annual revenue from selling California residents’ personal information. Parent companies and subsidiaries using the same branding are covered in the definition of "business," even if they themselves do not exceed the applicable thresholds.

Moreover, there is a limit on liability for businesses that have disclosed PI to third parties that subsequently violate the Act. To qualify for this limit, a business must only disclose PI pursuant to a contract including specific provisions. The contract must include a certification that the third party understands the requirements of the Act and provisions prohibiting the third party from reselling the data, retaining or using the data for any purpose other than what was enumerated in the contract, and retaining or using the data outside of the direct business relationship between the third party and the disclosing business. A business that abides by these requirements, and thus “did not have actual knowledge or reason to believe that the service provider intends to commit such a violation,” is immune from liability for violations of the Act by such third-party recipients.

**CONCLUSION**

 Passage of, and the recent amendments to, the CCPA likely opens the door for GDPR-like privacy regulation in the United States. Indeed, the Internet Association (whose members include Microsoft, Google) has come out in favor of national legislation in order to avoid piecemeal regulation of privacy at the state level. Accordingly, the ATP should closely monitor future developments in order to provide testing organizations with up-to-date information on this important topic.