

March 13, 2019

### **California Changes the Privacy Landscape Again: The California Consumer Privacy Act of 2018**

As businesses struggle to keep pace with new cybersecurity threats and data privacy laws, California has raised the stakes again. Last year, California passed a consumer privacy law that could impose significant new requirements on U.S. businesses. The new law, known as the California Consumer Privacy Act of 2018 (CCPA), was signed into law on June 28, 2018, and is currently set to take effect on January 1, 2020.

The CCPA was passed quickly in a single day to avoid a ballot initiative that would have included even greater restrictions. As a result, the law contains many ambiguous and inconsistent provisions, a few of which have been addressed through amendments that passed last summer and fall. The law, however, continues to be the subject of debate in the California legislature and may be further amended before it goes into effect next year.

While in many respects, the CCPA does not go quite as far as the European Union's new General Data Protection Regulation (GDPR), it still raises new risks and imposes new obligations on businesses' handling of personal information of California residents, i.e., "consumers," as defined under the Act. Moreover, businesses need to be aware that the CCPA differs from the GDPR in many respects and compliance with the GDPR does not equal compliance with the CCPA. Below are the key takeaways for business owners.

#### **When Does the CCPA Take Effect?**

The law becomes effective on January 1, 2020.

#### **Which Businesses Are Subject to the CCPA?**

The businesses covered by the law include those that collect the personal data of California residents and satisfy any one of the following criteria:

- The business has annual gross revenues in excess of \$25 million, as may be adjusted for inflation; **or**
- The business "annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices"; **or**
- The business derives 50 percent or more of its annual revenues from selling California residents' personal information.

The CCPA can also apply to certain affiliates of businesses covered by the law that share common trademarks and other branding. Businesses should keep in mind that the CCPA is not limited solely to online or digital data collection and can apply to any collection or other handling of any personal information, whether offline or online (such as through a website ).

### **What Does “Personal Information” Include?**

The CCPA’s definition of “personal information” is very broad and includes not only names, physical addresses, email addresses, social security numbers, driver’s license numbers and passport numbers, but 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.” Thus, the definition appears broad enough to include inferences drawn from different forms of information to create profiles of customers. The statute provides several examples of such information, illustrating the breadth of the definition, including IP addresses, online identifiers, commercial purchasing information (including buying histories or tendencies), biometric information, browsing, search and online interactivity histories, geolocation data, employment information, etc.

### **What Are the Key Requirements for Businesses?**

Businesses covered by the law will be subject to new obligations regarding disclosure, management and use of consumer personal information. Such obligations include:

- Disclosing the categories of information collected and the purposes for which such information will be used prior to collecting any personal information of a consumer. Businesses cannot collect any additional categories of information or use collected information for additional purposes that have not been disclosed to the consumer prior to such collection or use.
- Providing at least two methods for consumers to request information from the business, which methods should include at least a toll-free hotline and, if the business has a website, the website address. The information consumers may request includes: (a) the categories of personal information that the business has collected about the consumer; (b) the categories of sources from which the information is collected; (c) the purpose for collecting such information; (d) the categories of third parties (such as marketers, other businesses, etc.) with whom the information is shared; (e) the specific pieces of personal information that the business has collected from the consumer; (f) the categories of the consumer’s personal information that the business sold to third parties and the categories of such third parties (subject to certain requirements for the information’s organization); and (g) the categories of personal information that the business disclosed about the consumer for a business purpose. All responses to consumer requests must be provided within 45 days of the request, although businesses are not required to provide such information more than twice during any 12 month period.
- Disclosing to consumers their right to ask the business to delete their personal information. Subject to certain exceptions (completing transactions, performing contracts, detecting

security incidents, etc.), businesses must also comply with any deletion requests, including instructing service providers to also delete the information.

- Businesses that sell personal information must notify consumers in advance “in a form that is reasonably accessible to consumers” that their information may be sold and of their right to “opt-out” of such sales. This includes providing on the business’ website homepage a clear and conspicuous link titled “Do Not Sell My Personal Information” to a website to make the opt-out request. For consumers who are 16 years old or younger, an affirmative “opt-in” agreement is required either by the consumer or their parent (for ages 13 and younger).
- Businesses cannot discriminate against consumers who wish to or have exercised their rights under the CCPA, such as by denying services, goods, changing pricing, degrading service quality, etc. However, businesses may provide different pricing, service or product quality, provided that any such difference is “reasonably related to the value provided to the consumer by the consumer’s data.”
- Businesses must update their privacy policies to disclose the foregoing rights to consumers, including (as applicable) the right to request information, copies or access to personal information, deletion of personal information, and “opt-out” rights with respect to information that may be sold. In addition, privacy policies must disclose a list of the categories of personal information that the business has collected, shared or disclosed about consumers in the preceding 12 months.

### **What Are the Penalties for Violating the CCPA?**

Private causes of action under the CCPA are limited to data breaches where a consumer can show a business failed to “implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.” For such private claims, the CCPA provides for damages ranging from \$100 to \$750 per consumer per incident, as well as equitable or other relief the court deems appropriate.

California’s Attorney General may also prosecute any violations of the CCPA and such actions can result in potentially significant damages. However, a business will not be viewed as being in violation unless it fails to cure any alleged violation within 30 days of notice from the state. The penalties for such uncured violations are limited to \$2,500 per violation, although the penalty may be increased to \$7,500 per violation if the violation was intentional.

Although the law becomes effective as of January 1, 2020, the Attorney General cannot begin enforcement until the later of July 1, 2020 or issuance of the final regulations.

### **Are There any Exemptions under the CCPA?**

The CCPA provides for certain limited exemptions for personal information collected and processed pursuant to certain federal privacy laws, such as HIPAA and Gramm-Leach-Bliley, as well as certain California state laws. However, these exemptions are subject to certain qualifications and

may not apply to the CCPA's data breach obligations and liabilities. Thus, businesses should carefully assess whether, and to what extent, any exemptions under the CCPA may apply to them.

### **What Are the Next Steps for Businesses?**

While it is very possible that the CCPA will be further amended before January 1, 2020, businesses should not assume that the amendments will reduce businesses' obligations. In fact, the California Attorney General recently recommended that the private right of action be expanded to include any violation of the Act (not just data breaches) and a new state senate bill was just introduced that would make this change. Such an expansion of the private right of action could significantly increase risks for businesses handling California resident information.

In addition, as stated above, compliance with the GDPR does not mean a business is also compliant with the CCPA. Indeed, the CCPA may impose greater obligations in certain respects. For example, the CCPA's definition of "personal information" may be broader than the GDPR's; California residents may have greater rights to request deletion of information; and such residents may have stronger rights to access personal information held by businesses.

Businesses should therefore assess whether the CCPA may apply to them and begin developing a plan to bring their operations into compliance by January 1 of next year. Such steps may include updating privacy policies, websites and internal information technology systems and procedures.

We will continue to monitor developments on the CCPA and other privacy laws that may impact your business and are available to answer any questions that you may have.

### **Contacts**

#### **Robert P. Henley, III**

Partner

804.771.9550

[rhenley@hirschlerlaw.com](mailto:rhenley@hirschlerlaw.com)