Armstrong Teasdale

October 26, 2023 • Advisory • www.atllp.com

CALIFORNIA'S NEWEST CYBERSECURITY RULE – WHAT YOU NEED TO KNOW

PEOPLE

Jeffrey Schultz, CIPP/US

F. Scott Galt, CIPP/E

Casey E. Waughn, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

With cybersecurity incidents continuing to make headlines, it is no surprise that lawmakers are attempting to address the proliferation with proposed regulations in a variety of sectors and jurisdictions. However, the California Privacy Protection Agency (CPPA) – an agency formally tasked with enforcing the California Consumer Privacy Act (CCPA), a data privacy statute – has officially entered the mix and has taken steps to begin the rulemaking process for a new data security regulation promulgated based on its rulemaking authority under the CCPA. The initial draft regulation was released on Aug. 28 and discussed at the Sept. 8 CPPA meeting. While a formal notice process and second public comment period must still occur before the rule is finalized, the wheels are in motion.

As currently drafted, the CPPA's proposed regulation would require businesses that meet the requisite thresholds set forth in the CCPA and whose processing of consumers' personal information "presents a significant risk to consumers' privacy or security" to conduct annual cybersecurity audits and submit regular risk assessments to the CPPA. While the proposed regulation is in the early stages of the rulemaking process and could undergo substantial revision in the coming months, there are several compliance considerations and practices that businesses may need to adopt if the core framework of the proposed rule is kept.

ANNUAL CYBERSECURITY AUDITS

The draft language of the proposed cybersecurity regulation requires that every business subject to the CCPA that processes consumer information in a way that "presents a significant risk to consumers' privacy or security," conduct an annual cybersecurity audit. While it is not yet clear the scope of processing activities that "present a significant risk to consumers' privacy or security," the CPPA has made clear that businesses which derive more than half their revenue from "selling" and "sharing" personal information are engaged in processing activities that present significant risk to consumers' privacy and security. The CPPA has also hinted that businesses which process sensitive personal information of a threshold number of consumers are also engaged in higher-risk processing activity that requires a cybersecurity audit. Processing a large number of consumers' personal information – sensitive or not – may also

trigger the audit requirement under the current draft regulations. The threshold numbers that trigger the audit requirement have not yet been determined.

As proposed, businesses that fall under this requirement would have 24 months from the regulation's effective date to complete their first cybersecurity audit. After that, businesses must conduct an annual audit for as long as the business continues to meet the thresholds that trigger the audit requirement. While auditors can be internal or external to the business, the auditors cannot be individuals who contribute to the development or maintenance of the business's cybersecurity program or prepare documents that the auditor would later have to review during the annual cybersecurity audit. Businesses would also be required to present these annual cybersecurity audits to their respective board of directors (or equivalent) as well as submit either a certification of compliance or acknowledgement of noncompliance to the CPPA. Under the proposed rule, service providers and vendors of covered businesses are also required to assist the business in its cybersecurity audit and risk assessment.

RISK ASSESSMENTS

In addition to conducting annual cybersecurity audits, businesses must also conduct regular risk assessments under the CPPA's proposed regulation. Similar to the cybersecurity audit requirement, those businesses that meet the requisite thresholds and whose processing activities present a "significant risk to consumers' privacy" are required to conduct risk assessments prior to engaging in that processing activity. Under the proposed regulation, businesses that use artificial intelligence (AI) or other automated decision-making technology in certain circumstances (i.e., in connection with financial or lending services, education, health care services, employment, etc.) are required to conduct a risk assessment prior to commencing the high-risk processing activity.

Other legislation, such as the European Union's General Data Protection Regulation (GDPR) and other state laws, also require risk assessments for certain processing activities, including when the business is engaged in "profiling," which many interpret to extend to the use of AI and similar technologies. It is not yet clear the extent to which California's risk assessment requirement will overlap with or compliment the risk assessment requirement under other statutory or regulatory regimes.

Unlike the proposed language regarding the annual cybersecurity audit requirement, which has less definite parameters, the CPPA has outlined seven specific processing activities which constitute a significant risk to consumers' privacy and that would require a business to conduct a risk assessment prior to engaging in the processing activity:

1. selling or sharing consumers' personal information;
2. processing consumers' sensitive personal information (except for the purposes of employee authorization, payroll, health plan and benefits management, or wage reporting);
3. using automated decision-making technology to make certain decisions regarding financial or lending services, housing, education, employment and more;
4. processing the personal information of consumers that the business has actual knowledge are under the age of 16;
5. processing the personal information of job applicants, independent contractors, employees or students using surveillance technology (e.g., keystroke loggers, productivity monitors);
6. processing the personal information of consumers in public places using surveillance technology (e.g., WiFi or Bluetooth trackers, video or audio recordings, facial or speech recognition technology); and
7. processing the personal information of consumers to train AI or automated decision-making technology tools.

Under the proposed regulation, companies must consider a minimum of 10 specific components outlined in the proposed rule as they assess the risk, including the categories of personal information to be processed, the context in which the processing activity takes place, the purpose for processing, and any safeguards in place to address negative impacts to consumer privacy associated with that processing, among others. Businesses which use automated decision-making technology are also required, among other requirements, to include plain language explanations for the reason for using the technology, the outputs secured by the technology and how they will be used, and any degree of human involvement in the decision-making process.

If a risk assessment reveals that the processing activity's benefits are outweighed by the risks to consumers' privacy, the business is not allowed to engage in that processing activity. Businesses are required to submit their full risk assessments to the CPPA upon request, but they must also submit an abridged form of all risk assessments and a certification of compliance annually.

CPRA RULEMAKING PAUSED

As a reminder, enforcement of the new regulations under the CPPA is paused until March 29, 2024, following a ruling this summer by a California state court noting concerns with requiring businesses to immediately comply with the new regulations without giving them time to adjust their practices and procedures accordingly. This delay only applies to the new regulations that were issued

under the CPRA on March 29, 2023, not to those regulations under the CCPA that remain unchanged by the CPRA and that were promulgated before March 29, 2023. Any other regulations – including the new annual cybersecurity audit and risk assessment rule – will go into effect one year after they are finalized.

Because the CPPA has just begun the lengthy rulemaking process, these regulations likely will not come into effect before 2025 at the earliest. However, it is important for businesses to be aware of and prepared for these upcoming changes to the California cybersecurity landscape so they can allocate resources appropriately. Our Data Innovation, Security and Privacy lawyers can assist you with determining how this new rule may impact your business's operations and with crafting tailored compliance solutions. For more information specific to your business needs, please contact one of the listed authors or your regular AT lawyer.