Articles + Publications | May 31, 2023

Waiting on Guidance From the CPPA. What to Do in the Meantime??

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox

RELATED OFFICES

Hartford

Last fall, we provided an update on the state of the regulations promulgated under the California Consumer Privacy Act (CCPA). At the time, we identified key gaps in the current regulations, specifically the lack of guidance on requirements for cybersecurity audits, data processing risk assessments, and automated decision-making. On March 27, 2023, the California Privacy Protection Agency (CPPA) closed its comment period for rulemaking activities on cybersecurity audits, risk assessments, and automated decision-making, which have not been addressed in the regulations to date. Absent direct guidance from the CPPA on these important issues, the CCPA statutory language and Colorado's regulatory guidance on data protection assessments (which are comparable to risk assessments under the CCPA) may provide some insights into how to prepare for the coming July 1, 2023 CCPA enforcement deadline.

Cybersecurity Audits

Cybersecurity audits must be performed by businesses subject to the CCPA on an "annual basis." These audits must define the scope of the audit and establish a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in a significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.

CCPA Sec. 1798.185(15)(A). Many organizations subject to the CCPA will already have processes and procedures in place for performing annual cybersecurity assessments. Those that do not will be able to rely on the existing and readily available resources for performing cybersecurity assessments, such as guidance from NIST and elsewhere.

Risk Assessments

The CCPA requires submissions to the CPPA "on a regular basis" of "risk assessments with respect to their processing of personal information." CCPA Sec. 1798.185(15)(B). The CCPA describes this process as identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from

processing to the consumer, the business, other stakeholders, and the public.

CCPA Sec. 1798.185(15)(B). Fortunately, Colorado has already provided guidance on data protection assessments, the Colorado analogue to CCPA data processing risk assessments. This guidance can inform the necessary preparatory work for compliance with the CCPA requirements by the July 1, 2023 enforcement deadline. Provided in part 8 of the Colorado's regulations, this guidance addresses the scope, content and timing of assessments. In summary, assessments should scale to the organization and type of processing, and one assessment may cover multiple processing activities if they are sufficiently related. Assessments must cover a wide range of content requirements, but at their core assessments involve a balancing test, comparing benefits and harms resulting from the processing activity. In terms of timing, assessments are performed prior to processing and updated as appropriate, based on changes to the expected harms or changes in the plans for the processing activity.

Automated Decision-Making

The CCPA references opt-out rights concerning automated decision-making, which is a commonly misunderstood concept. The CCPA does not include a formal definition within the statute, but includes "profiling" as a category of automated decision-making. While there are gradients of human involvement in any automated process, the concept of automated decision-making could mean anything from completely automated decisions with material effects on California residents, to automation-assisted decisions with some degree of human input. Because of the recent rise of large language models (Chat GPT, for example), this class of processing activity has recently garnered additional public attention. As such, there may be special concerns the CPPA raises in relation to automated decision-making and any organizations with significant automated decision-making activities should expect to develop opt-out mechanics for individuals that allow for more human involvement in outcomes.

* * * * *

Even while we await regulatory guidance from the CPPA on cybersecurity audits, risk assessments and automated decision-making, business subject to the CCPA can take steps now to be in position to comply by the July 1, 2023 enforcement date.

1. *Cybersecurity Audits.* Many businesses have already conducted cybersecurity audits to satisfy other requirements, or as a best practice. For others, NIST has published resources (linked above) to guide businesses in conducting cybersecurity audits. Any business subject to the CCPA should take this opportunity to review and enhance, or implement, cybersecurity audit procedures in order to prepare for the enforcement date.
2. *Risk Assessments.* Businesses should look to the Colorado regulatory guidance linked above, and prepare for the enforcement date of the CCPA risk assessment requirement.
3. *Automated Decision-Making*. Absent any state guidance, businesses should start cataloguing and reviewing processing that could be considered automated decision-making, including profiling. Once the CPPA issues regulatory guidance, steps can then be taken in order to determine the scope and substance of the forthcoming requirements. Note that we expect the CPPA to set a delayed enforcement date, or a transition date, for business to comply with the automated decision-making requirements, given the dearth of guidance in the CCPA itself, or in other states.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber