Articles + Publications | September 15, 2022

California Privacy Fall Update: Proposed Regulations and Fading Exemptions

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox

The California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA") has had some major developments over the summer. On July 8, 2022, the California Privacy Protection Agency (California's privacy regulator, the "CPPA"), released proposed regulations for the new version of the CCPA, effective January 1, 2023, which we have discussed in prior articles on enforcement, major changes, and big picture issues. Although these regulations address many of the ambiguities in the newly amended CCPA, a few major areas of concern remain. These include the details of automated decision-making, cybersecurity audits, and data processing risk assessments, which are still to be announced. Perhaps the most alarming development is the California legislature's failure to extend the existing "employee/personnel" and "business to business contacts" exemptions before the end of the 2022 session. This means that personnel and B2B contacts of a business subject to the CCPA will be treated as consumers for all purposes of the CCPA starting January 1, 2023 as further discussed here. As most observers expected these two, important exemptions from the CCPA would be extended, for many businesses, getting to compliance by January 1, 2023 will be a sprint.

The proposed regulations released on July 8, 2022 primarily clarified the operation of the CCPA rights that were newly created by the California Privacy Rights Act to (i) limit the disclosure of sensitive personal information, (ii) correct inaccurate personal information, and (iii) opt out of the sharing of personal information for purposes of cross-context behavioral advertising. They also added more specificity in terms of the expectations for contract language between a business and its contractors, service providers, and third parties, and added an entire new section describing in detail and prohibiting the use of dark patterns when interacting with consumers. These new dark pattern requirements add a new obligation for symmetry of choice, which will effectively kill off the dreaded cookie banner that offers the option of "accept" or "more information," and takes more clicks to opt out than to simply accept. This change may have profound impacts on common web and application design, which often bias users towards options that are preferred by the designers, even if those design choices are motivated by the desire to provide a better user experience.

The proposed regulations also clarified the details of legacy CCPA rights, such as the timing and mechanics concerning requests and responses; and requirements for CCPA privacy policies, notices at collection and disclosures of financial incentive. Under the proposed regulations, businesses would no longer be required to employ disproportionate effort in order to satisfy certain consumer requests. Basically, if the time and/or resources expended by the business to respond to the individualized request significantly outweighs the benefit provided to the consumer by responding to the request, the business may have the option to deny the request. Some specific examples are provided, but a business will not be able to cite disproportionate effort as a reason for the denial of a consumer request if the business simply failed to put in place adequate processes and procedures to comply with

©2025 Troutman Pepper Locke

consumer requests.

Notably, the proposed regulations have significant omissions, as they provide no detail for the important requirements of data processing risk assessments, and cybersecurity audits. For processing risk assessments, there are existing laws that set expectations. EU/UK oriented businesses will already be familiar with performing data protection impact assessments under the GDPR, and Virginia, Colorado, and Connecticut have articulated a similar standard known as a data protection assessment, which targets assessments towards processing that presents a heightened risk of harm to consumers. There remains some hope that California will follow that lead, or at least its structure, to permit a single-assessment process that could satisfy each state's requirements. Details also remain unspecified on what will be required of the annual cybersecurity audit. As the direction for regulations in the law references scaling the factors of the assessment to the size and complexity of the business and the nature and scope of processing activities, there is some hope that the CPPA may propose a flexible system to address the needs and capabilities of large and small businesses.

The lack of further detail on automated decision-making is a major absence. Businesses already heavily rely on automated decision-making for everything from marketing, pricing, security, basic business operations and more. The regulations are expected to provide guardrails to automated decision-making in order to further protect consumers against certain types of profiling that may cause harm to specific groups of individuals, such as potential discriminatory effects that have been shown to be present in machine learning models that may reflect the systemic biases of their training data sets.

Beyond the detail of the proposed regulations, and the concerns about various open-ended issues still left unaddressed, the failure to extend the existing personnel and B2B exemptions before the end of the 2022 session presents significant challenges. Businesses will need to develop processes to identify personnel requests under the CCPA, and coordinate the handling of such requests with the requirements of applicable employment laws. While California already provides employees certain rights to access information their employer maintains about them, there are new categories of information and new requirements in the CCPA that businesses must consider. This is an increase in administrative complexity that many businesses hoped or expected would be delayed. Practical tips for achieving compliance are offered here.

With the 66 pages of proposed regulation already available for digestion, it is surprising how many issues with tangible administrative consequences remain unaddressed just a few months out from the January 1, 2023 effective date for the CCPA amendments.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber