Published on *The National Law Review* https://natlawreview.com

California's Privacy Regulator Had a Busy November, Risk Assessment Edition: What Does It Mean for Businesses?

Article By:

Liisa M. Thomas

Kathryn Smith

In the third in our series of new CCPA regulations from California, we look at obligations for conducting risk assessments under CCPA. CCPA had called on the California agency to promulgate rules to address such assessments, and when they would be needed.

This new proposal retains much of what was proposed in 2023, but does make some modifications:

- **Scope**: As previously proposed, a company would need to conduct a risk assessment if they are doing something that could "present a significant risk" to individuals. This has not changed, although some of the examples and situations outlined in the rule have been modified. As currently proposed, this would include (1) selling or sharing personal information, (2) processing sensitive personal information, or (3) using automated decisionmaking technologies in a way that would result in a significant decision (as discussed in our earlier post in this series). The updated version also simplifies requirements for conducting risk assessments for automated decision making technology.
- **Timing and Retention**: As proposed, the risk assessment will need to be conducted before beginning the process. I.e., engaging in the activity outlined above. This obligation has not changed from the prior proposal. However, there is now a timing obligation for current activities. Namely, that companies would need to conduct risk assessments within two years of the rules going into effect. Also new is that the assessment would need to be reviewed -and if needed, updated- every three years. Retained from the prior version is an obligation to update the assessment immediately if there has been a material change to the processing activity. As proposed, the assessment must be kept for five years (this has also not changed from the prior proposal).
- **Submissions**: Risk assessments will need to be submitted to the California agency under the proposed rule. Under the new proposed rules, the first must be done within two years of the effective date of the rules and then annually thereafter. Unchanged from the prior version is that as part of the submission companies will need to include a "certificate of conduct." They can then include an "abridged" or full copy of the assessment. (The possibility of providing the full risk assessment is new, the prior proposal contemplated having business submit only

an abridged version.)

- **Process**: As was included in the previous version of the rules, the proposed rules require those whose job duties relate to the activities being assessed to participate in the risk assessment. These might include external employees as well as internal ones. The purpose of the assessment is to analyze whether the risks to individuals outweighs the benefits to them. In recognition that the assessment process outlined in the rule is very similar to that contained under other laws, the proposal permits using an assessment that was conducted for compliance with another law, if it "meets all of the requirements" of the regulations.
- **Contents**: In line with both the previous version of the rules, the proposed rules call for the risk assessment to identify -with specificity- the purpose for processing information and the categories of information to be processed. It would also need to outline the steps the company has taken to "maintain the quality" of the information being processed by automated decisionmaking technology or artificial intelligence tools. Other contents include how long the company will keep the information and the approximate number of people whose information will be processed. It must also include the benefits to the business, negative impacts on individuals, and safeguard measures. Under the new proposed rules, companies would also need to include a description of how disclosures will be made to individuals.

Putting It Into Practice: These proposed rules contain a retroactive component and would apply to activity currently in place. Thus, as we await a final version of the rules regarding risk assessments, companies who are engaging in activities that might fall within scope may wish to begin the assessment process.

Listen to this post

National Law Review, Volume XIV, Number 346