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

California's Potential Approach to Regulations on Risk Assessments and Cybersecurity Audits Could Be a Game Changer

Article By:

Alan L. Friel

Niloufar Massachi

Until late August 2023, California's data protection law, the California Consumer Privacy Act, or "CCPA," only provided for future rulemaking on automated decision-making, including profiling, on risk assessments, and on cybersecurity audits. However, during a board meeting it held this past Friday, September 8th, the California Privacy Protection Agency ("CPPA" or "Agency"), which shares enforcement authority of the CCPA with the California Attorney General, discussed a new set of draft regulations ("Regs") it released for Agency discussion purposes in late August 2023. While not yet part of the official rulemaking, the draft and the discussions around it provides direction on its upcoming rulemaking on these topics. We will refer to the draft and related commentary as the "Roadmap." Most notably, the Roadmap proposes that condensed versions of assessments and audits completed by businesses pursuant to their CCPA obligations be filed with the CPPA and sets forth detailed obligations surrounding such assessments and audits. The implication of this is that it may become obvious to the Agency which companies are or are not conducting assessments or audits and thus complying with their CCPA obligations. It may also provide the Agency an easily accessible way to review the evaluate businesses' practices, especially with regard to higher risk processing activities. Furthermore, the Agency's Roadmap suggests assessment requirements that not only incorporate, but exceed, what is required in the Colorado regulations, including risk / harm assessments of any monitoring of personnel or students, or monitoring of consumers in public places.

CPPA Board Meeting

During its September 8th board meeting, the Agency discussed its Roadmap on cybersecurity and risk assessment without commencing formal rulemaking. The Agency plans to further revise the Roadmap based on the discussions had and comments received during the meeting, and stated that it aims to release proposed Regulations out of the subcommittee process to the CPPA board for further discussion by the next board meeting, scheduled for December 8, 2023. Accordingly, the Roadmap will not become enforceable regulations until Q1 of 2024, at the earliest.

Members of the Agency Board evaluated the pros and cons of the various provisions during the meeting, evaluating the benefits to consumers from the privacy protections offered by the Roadmap against the burden on businesses who must comply.

Regarding cybersecurity audits, the CPPA Board discussed several topics, including:

- The threshold which will determine when a business will have to conduct a cybersecurity audit. The Agency Board discussed whether the threshold should follow the threshold for businesses in the CCPA, including a not-yet-determined number of consumers whose personal information is processed by that business. Other options discussed would set the threshold at a certain annual gross revenue of the business, or a certain number of employees. To this end, the CCPA threshold along with number of consumers whose personal information was processed and the annual gross revenue were the most popular options. The Agency stressed that the risk to security is the most important consideration in determining whether a business should conduct a cybersecurity audit, but acknowledged that costly cybersecurity audits may be burdensome, especially on smaller businesses with fewer resources.
- The scope of cybersecurity audits. The Agency Board considered two options for the scope of cybersecurity audits. One option considered sets forth that a cybersecurity audit should assess and document risks that materially affect, or are reasonably likely to materially affect, consumers. The other option provides that cybersecurity audits should protect against certain enumerated negative impacts to consumer's security such as economic harm and reputational harm. One member of the Agency Board suggested merging the two options by including the risks of harms in tandem with the "materially affected" threshold. In its discussions the Agency Board also highlighted that it's important for a business to consider not only risks to itself when conducting cybersecurity audits, but also risks to consumers.
- Safeguards that businesses should consider in conducting cybersecurity audits. The Roadmap provides that businesses should document the safeguards that will be implemented to minimize risks. The Agency Board noted that not all safeguards may be applicable to every business, and the listed safeguards are considerations rather than explicit mandates.

As for privacy assessments, the CPPA Board discussed:

- Details required to be in an assessment. The Agency Board evaluated the pros and cons of requiring certain details to be included in an assessment, such as listing the names and titles of all individuals within a business that prepared, contributed to or reviewed the assessment, describing the qualifications of those who participated and identifying the number of hours contributed to conducting the assessment. The Agency Board noted that this may be too burdensome and could involve privacy concerns related to mandating individuals within a business to share such information. Certain members of the CPPA Board proposed recrafting the obligations such that this detail is recorded internally without a business having to include it in the form of the assessment documentation to be submitted to the CPPA.
- Benefits within an assessment. Members of the Agency Board expressed an interest in assessments including information on whether a business is directly financially benefitting from selling or sharing personal information, rather than a broader inquiry into the benefits of processing.
- Timing of updates to assessments. The Board considered whether assessments should be conducted every three years, or whether to require businesses to review and update assessments as necessary, and whether they should be made available to the Agency in an abridged or full form. Some Board members noted that requiring updates every three years

may be unnecessary, but that more frequent updates may be important for automated decisionmaking ("**ADM**") technology, given the potential for discriminatory outcomes. The Board members noted that having full risk assessments, rather than abridged risk assessments, submitted to the Agency in every circumstance could lead to a database of risk assessments that would be very large and difficult to manage.

Which Processing Activities Would Require a Risk Assessment?

The Roadmap's potential regulations would obligate businesses subject to the CCPA to conduct assessments when the processing of consumers' personal information presents a significant risk to their privacy. Such processing includes:

i. **selling or sharing** personal information;
ii. **processing sensitive personal information**;
iii. **using automated decisionmaking technology** in furtherance of a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or contracting opportunities or compensation, healthcare services or access to essential goods, services or opportunities;
iv. processing the personal information of consumers that the business has **actual knowledge are less than 16 years of age**;
v. processing the personal information of consumers who are employees, independent contractors, job applicants or students **using technology to monitor employees, independent contractors, job applicants or students**;
vi. processing the personal information of consumers in **publicly accessible places using technology to monitor consumers'** behavior, location, movements or actions; and
vii. processing the personal information of consumers to **train artificial intelligence ("AI") or ADM technology**.

What Information Must Assessments Contain?

An assessment under the Roadmap should involve all individuals from across the business' organizational structure who are responsible for preparing, contributing to or reviewing the assessment, and may include external parties to identify, assess and mitigate the risks (e.g., those that are part of the fraud-prevention team, product team or compliance team). Assessments must include a short summary of the processing, information about the context and purposes of processing and the personal information to be processed, and the risks, benefits and safeguards implemented.

In comparison, Colorado requires assessments to include a risk-benefit analysis, including a discussion of safeguards taken to offset the risks. The Colorado regulations also provide a list of 12 explicit inquiries that must be discussed, along with an additional 12 that are required if a business is engaging in profiling. Colorado's requirements for assessments are currently the most stringent, though we have yet to see what the CPPA will ultimately propose. The draft regulations on assessments can be found here.

What does the Roadmap say about AI and ADM?

Regarding AI and ADM technology, the Roadmap does not yet articulate the trigger for when AI or ADM require an assessment. However, the Roadmap defines AI as "*an engineered or machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or*

implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments."

The Roadmap also defines ADM broadly, as "*any system, software, or process—including one derived from machine-learning, statistics, other data-processing techniques, or artificial intelligence— that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decisionmaking. Automated Decisionmaking Technology includes profiling*." This definition would capture a wide range of automated decision-making activities, requiring businesses to conduct risk assessments prior to using such systems.

In addition to conducting assessments if the yet to be determined triggers are met, the Roadmap suggests that there will be several other obligations related to AI and automated decisionmaking. For example, the Roadmap proposes that when making AI technology available to other businesses, the business must provide all facts necessary for the recipient-businesses to conduct the recipient-businesses' risk assessments. This provision of the Roadmap, if passed, will be helpful for the vendor diligence process and in drafting data protection agreements ("DPAs").

Are there any Filing Obligations under the Draft Regulations?

Assessments conducted pursuant to the Roadmap's draft potential regulations will have to be made available to the CPPA or California Attorney General upon request. Businesses will also have to submit abridged versions of risk assessments annually, including a certification by a designated executive that the business has complied with the requirements of these draft regulations. As noted above, some Board members are advocating for the filing of full reports, at least in some instances.

Do the Other State Privacy Laws Require Risk Assessments?

Under the other U.S. state privacy laws in effect, including the Virginia Consumer Data Protection Act ("VCDPA"), Connecticut's Public Act No. 22-15 ("CTPA") and the Colorado Privacy Act ("CPA"), data privacy practice assessments are required for certain high-risk processing activities. Such activities include selling personal information, processing sensitive personal information, engaging in targeted advertising and profiling, defined generally as "*any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements*." Profiling does not necessarily implicate AI. However, it can use AI to power to analyze data and group consumers to produce relevant advertising, for example. In such cases, and with the use of AI generally, it is important to conduct such risk assessments prior to using the AI system. For more information on risk assessment requirements, please see our blog post.

Cybersecurity Audits

In addition to potential draft regulations in the Roadmap related to risk assessments, the CPPA also outlined a rulemaking roadmap for regulations on cybersecurity audits. The initial discussion draft, if ultimately passed, will require businesses to conduct cybersecurity audits if processing of consumers' personal information presents significant risk to consumers' security. Cybersecurity audits will have to be performed using a qualified, objective and independent auditor. The audit must:

- Assess, document and summarize each applicable component of the business' cybersecurity program;

- Specifically identify any gaps or weaknesses in the business' cybersecurity program;
- Specifically address the status of any gaps or weaknesses identified in any prior cybersecurity audit; and
- Specifically identify any corrections or amendments to any prior cybersecurity audits.

Service providers and contractors of a business will be required to cooperate with that business in its completion of a cybersecurity audit. Businesses will have 24 months from the effective date of the regulations to complete a first cybersecurity audit, and audits must be completed annually thereafter. The draft regulations related to cybersecurity audits can be found here.

Sasha Kiosse, an author at Privacy World, co-authored this article.

National Law Review, Volume XIII, Number 255