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

California Privacy Protection Agency Public Board Meeting Sheds Light on Upcoming Risk Assessment and Cybersecurity Audit Regulations

Article By:

Frances M. Green

Alexander J. Franchilli

Scarlett L. Freeman

Tryphena Liu

The five-member Board of the California Privacy Protection Agency (the "CPPA") held a public meeting on September 8, 2023, to discuss a range of topics, most notably, draft regulations relating to risk assessments and cybersecurity audits. Once the regulations are finalized and approved after a formal rulemaking process, they will impose additional obligations on many businesses covered by the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"). The Board's discussion of these draft regulations is instructive for CCPA-covered businesses,[1] but also any business striving to maintain best practices when performing data privacy risk assessments and assessing its own cybersecurity program.

Risk Assessment Regulations

The draft regulations would require risk assessments when a CCPA-covered business processes information that presents a "significant risk to consumers' privacy," which includes selling or sharing personal information, or processing sensitive personal information, with the notable exception of processing sensitive personal information for certain HR purposes (*i.e.*, processing related to employee authorization, payroll, health plan, benefits management, or wage reporting). At the meeting, the Board discussed requiring risk assessments for other types of processing, notably, when using automated decision making tools ("ADMT"), processing personal information of consumers under the age of 16, using employee monitoring technology, processing personal information of consumers in public places to monitor behavior (*e.g.*, Bluetooth tracking), and processing personal information to train artificial intelligence. As discussed at the Board meeting, some of these categories extend beyond what would be required for a data privacy assessment under the Colorado Privacy Act—presently the only other comprehensive state privacy law in effect that has a comparable requirement to the CCPA's anticipated risk assessment regulations.

The draft regulations describe the information that must be included in a risk assessment:

- A summary of the processing that presents significant risk to consumers' privacy;
- The categories of information to be processed;
- The context of processing activity;
- The consumers' reasonable expectations with regard to the process;
- The operational elements of the processing;
- The purpose of processing;
- The benefits of processing[2];
- The negative impacts of processing;
- Safeguards to address the negative impacts; and
- An assessment of whether the negative impacts outweigh the benefits of processing.

At the meeting, the Board considered additional requirements for risk assessments, including:

- Relevant internal actors and external parties contributing to the assessment;
- Any internal or external audit conducted in relation to the assessment, including, the name of the auditor, the names and positions of individuals involved in the review process, and the details of the audit process; and
- Dates the assessment was reviewed and approved, and names, positions, and signatures of the individuals responsible for the review and approval.

While acknowledging the potential burden imposed by these added requirements, the Board stressed the goal of enabling businesses, particularly those with high turnover rates, to maintain "institutional memory" of a business' review and audit processes.

The outcome of the risk assessment would also dictate whether the business can proceed with the processing activity. That is, the draft regulations would require businesses to prohibit processing where the results of the risk assessment show that negative impacts outweigh the benefits. This is consistent with the statutory mandate for risk assessment regulations in the CCPA.[3]

The Board also discussed a requirement for businesses to certify compliance to the CPPA, and to update risk assessments both periodically and after a "material change" in the processing activity, noting that the risk assessment should be a "living document."[4] The cadence for periodic updates have not been finalized.

Risk Assessment for Automated Decision Making Technology

The draft regulations contain separate requirements applicable to risk assessments of ADMT.[5] While the Board clarified that there would be additional regulations relating to access and opt-out rights when using ADMT,[6] the draft regulations discussed at the September 8th Board meeting for risk assessments are a noteworthy first look at the Board's views on regulating ADMT.

Under the draft regulations, risk assessments for ADMT must include "plain language explanations" of the following:

- Why the business is seeking to use ADMT, including the benefits;
- The personal information processed by the ADMT;
- The outputs secured from the ADMT and how the business will use the outputs;
- The steps the business will take to maintain the quality of personal information processed by the ADMT (i.e., completeness, representativeness, timeliness, validity, accuracy, consistency, and reliability of the sources of the personal information);
- The logic of the ADMT and the assumptions of the logic;
- How the business evaluates the ADMT for validity, reliability, and fairness;
- An explanation for deciding not to use an external party for the assessment safeguards (if applicable) and the safeguards implemented to address any risks resulting from that decision;
- The degree and details of human involvement in the use of the ADMT; and
- Any safeguards the business implements to address negative impacts to consumers' privacy specific to its use of ADMT.

Use of personal information to train ADMT or artificial intelligence would be subject to further requirements. Specifically, when a CCPA-covered business offers ADMT or artificial intelligence to other persons, that business must provide an explanation of "the appropriate purposes" for which the tool can be used. Additionally, when a CCPA-covered business provides ADMT or artificial intelligence to another CCPA-covered business, the providing-business must provide all facts necessary to conduct risk assessments to the recipient-business.

Cybersecurity Audit Regulations

The Board discussed draft regulations related to cybersecurity audits. As discussed at the Board meeting, these draft regulations would supplement the CCPA's existing statutory requirement that businesses implement reasonable security procedures and practices to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure.[7]

The draft regulations require cybersecurity audits to be undertaken by any business that derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information in the preceding calendar year. At the meeting, the Board discussed at length certain other thresholds that would expand the scope of businesses required to comply with the cybersecurity audit regulations. One option that received some support was to include businesses with: $25 million revenue in the prior calendar year and that process (a) personal information of one million consumers, (b) sensitive personal information of 100,000 consumers, or (c) personal information of 100,000 consumers under the age of 16 years in the prior calendar year. Other options included requiring business with a minimum employee head-count or gross revenue—although the Board has not yet determined what these minimums will be. Based on the Board's discussion on this topic, final scoping criteria will address concerns that small and medium-sized organizations might incur significant costs. The Board also discussed concerns that high-risk businesses should be sufficiently covered, and that businesses should have clarity concerning when they are covered. Based on the complexity and impact of these policy considerations, the Board anticipates conducting an economic analysis of the impact of these scoping questions before finalizing the thresholds.

In terms of the methodology and content of a cybersecurity audit, the draft regulations require covered businesses to (1) assess, document, and summarize the "components" of their cybersecurity program, (2) identify gaps and weaknesses in the program, (3) address the status of gaps and weaknesses identified from prior cybersecurity audits, and (4) identify corrections or amendments to prior cybersecurity audits. The "components" of a business' cybersecurity program are further broken down into three categories:

- the establishment, implementation, and maintenance of the program, including written documentation, and the names of qualified employees responsible for the program;
- the safeguards used to protect personal information; and
- how the business implements and enforces compliance with those safeguards.

The draft regulations then identify 18 more specific categories of "safeguards," including, for example, multi-factor authentication, encryption, access controls, zero trust architecture, and network segmentation. At the meeting, the Board discussed that the draft regulations allowed flexibility in use of these safeguards, as an auditor can determine the appropriateness of these safeguards given the circumstances of the business.

At the meeting, the Board discussed one of the unique requirements included in the draft regulations: the requirement for cybersecurity audits to address the risks to *individuals*, such as the economic, physical, psychological, and reputational harm resulting from a breach. As written, this mandate would go further than most other cybersecurity laws and regulations; however, concerns raised by Board members at the meeting will likely necessitate revisions to the current formulation of this

requirement in the draft regulations.

Cybersecurity audits would be required on an annual basis, and through an independent auditor, who may be external or internal. Perhaps due to concerns with the independence of an internal auditor, internal audits must be reported to the board of directors or governing body, or the highest-ranking executive that does not have direct responsibility for the cybersecurity program. Businesses required to conduct cybersecurity audits must also certify compliance with the CPPA. The draft regulations would also require that contracts between a business and a "service provider" or "contractor," as those terms are defined by the CCPA, include language allowing the service provider or contractor assist the business in conducting cybersecurity audits.

Next Steps

The CPPA subcommittees responsible for the draft regulations will implement changes to the draft regulations discussed at the meeting, share drafts with the Board, and potentially present final drafts at the next Board meeting which is anticipated to take place in November 2023. When the formal rulemaking process begins, the public will have an opportunity to submit written comments on the proposed regulations.

As Board member Vincent Le stated at the meeting, in many cases, the draft regulations are designed to codify what businesses "should be doing or are already doing." In that regard, CCPA-covered businesses should assess their own risk assessment practices and protocols, and cybersecurity programs, with an eye towards these future regulations.

---

[1] Covered businesses are those doing business in California and meeting one or more of the following thresholds: (a) annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year; (b) annually buys, sells, or shares the personal information of 100,000 or more consumers or households; (c) derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

[2] At the meeting, the Board discussed adding language to the draft regulations to require businesses to describe any financial and other benefits with specificity.

[3] Cal. Civ. Code 1798.185(a)(15)(B).

[4] The Board left for further consideration the logistics of the submission (e.g., whether the CPPA will have an electronic portal for submissions and create a secure database for businesses' risk assessments).

[5] "Automated Decisionmaking Technology" is defined in the draft regulations to mean 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. "Profiling" means any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

[6] *See* Cal. Civ. Code 1798.185(a)(16) (requiring the CPPA to issue regulations governing access

and opt-out rights with respect to businesses' use of ADMT).

[7] Cal. Civ. Code 1798.100(e).

National Law Review, Volumess XIII, Number 256