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

California Privacy Protection Agency Board Holds November Meeting, Advances New Regulations

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

On November 8, 2024, the California Privacy Protection Agency Board ("the CPPA Board") hosted its public bimonthly meeting. The CPPA Board adopted new California Consumer Privacy Act ("CCPA") regulations applicable to data brokers and initiated the formal rulemaking process for proposed regulations for insurance, cybersecurity audits, risk assessments and automated decisionmaking technologies ("ADMT").

Adopted Proposed Data Broker Regulations

The proposed data broker registration regulations adopted by the CPPA Board would amend the existing data broker regulations issued pursuant to Cal. Civ. Code Sect. 1798.99.80 by defining relevant terms, explaining procedures for registration changes, and requiring data brokers to disclose specific information about their exempt data collection practices. Among other items, the proposed data broker regulations would:

- *Raise the annual data broker registration fee to $400*, effective for the coming registration period in January 2025.
- *Define "direct relationship" within the definition of "data broker."* Cal. Civ. Code Sect. 1798.99.80(c) exempts from the definition of "data broker" businesses that have a "direct relationship" with consumers. The proposed regulations would define "direct relationship" to mean "that a consumer intentionally interacts with a business for the purpose of obtaining information about, accessing, purchasing, using, or requesting the business's products or services *within the preceding three years*." This is a notable addition, in that it requires a business to have recent interactions with a consumer to rely on this exemption.
- *Define "minor" to mean an individual under 16 years of age*. Pursuant to Cal. Civ. Code Sect. 1798.99.80(b)(2)(C), a data broker must disclose whether the data broker collects the personal information of minors.
- *Define "reproductive health care"* to mean any of the following:
    - "Information about a consumer searching for, accessing, procuring, using, or otherwise interacting with goods or services associated with the human reproductive system, which includes goods such as contraception (e.g., condoms, birth-control pills), pre-natal and fertility vitamins and supplements, menstrual-tracking apps, and

hormone-replacement therapy. It also includes, but is not limited to, services such as sperm- and egg-freezing, In Vitro Fertilization, abortion care, vasectomies, sexual health counseling; treatment or counseling for sexually transmitted infections, erectile dysfunction, and reproductive tract infections; and precise geolocation information about such treatments";
    - "Information about the consumer's sexual history and family planning, which includes information a consumer inputs into a dating app about their history of sexually transmitted infections or desire to have children is considered sexual history and family planning information"; and
    - "Inferences about the consumer with respect to (1) or (2)."

Pursuant to Cal. Civ. Code Sect. 1798.99.80(b)(2)(E), a data broker must disclose whether the data broker collects consumers' reproductive health care data. This definition is rather expansive, and notably includes information consumers input into dating apps about their history of STIs and desire to have children.

It also is notable that the proposed data broker regulations, unlike the CCPA, do not include an exemption for "publicly available" data, which the CCPA defines to include "information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience." Cal. Civ. Code Sect. 1798.140(v)(2). This means that sexual history or family planning data a consumer posts in a dating app, even if not restricted to a specific audience, would constitute "reproductive health care" data covered by the proposed regulations.

- *Require data brokers to disclose the following information about the extent to which the data broker is regulated by other laws (specified in Cal. Civ. Code. Sect.1798.99.82(b)(2)(H), e.g., FCRA, GLBA, CMIA))*:

• "The types of personal information the data broker collects and sells that are subject to the enumerated laws;"

• "The specific product(s) or services covered by the enumerated state or federal law;" and

• "The approximate proportion of data collected and sold that is subject to the enumerated laws in comparison with their total annual data collection and sales (i.e., percentage of their general data broker activities)."

These regulations now move to the Office of Administrative Law and, if approved, will become effective January 1, 2025.

Rulemaking for Insurance, Cybersecurity Audits, Risk Assessments and ADMT

The CCPA Board also voted to move proposed regulations for risk assessments, cybersecurity audits, ADMT and AI, and insurance into formal rulemaking. Among other items, the proposed regulations would:

- *Amend the definition of "sensitive personal information" to include personal information of consumers the business "has actual knowledge are less than 16 years of age."*

• If adopted, the right to limit the use and disclosure of sensitive personal information would apply to

personal information of consumers under the age of 16.

- *Regulate ADMT and AI.*

• **Definitions**. The proposed regulations define “automated decisionmaking technology” to mean “any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking,” and to include artificial intelligence and profiling. The proposed regulations define “artificial intelligence” to mean “a machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments,” including “ predictions, content, recommendations, or decisions,” and including “generative models, such as large language models, that can learn from inputs and create new outputs, such as text, images, audio, or video; and facial- or speech-recognition or -detection technology.”

• **Consumer Rights**. The proposed regulations provide consumers the right to (1) request information about the business’s use of ADMT with respect to the consumer, (2) opt out of the use of ADMT, and (3) appeal the business’s use of ADMT for a “significant decision” as defined in the proposed regs. (e.g., employment, credit, education).

• **Processing Requirements**. Businesses also would be required to (1) conduct risk assessments for the (i) use of ADMT for a significant decision concerning a consumer or for “extensive profiling” (including profiling for behavioral advertising), and (ii) processing the personal information of consumers to train ADMT or AI in enumerated circumstances; (2) issue a pre-use notice with respect to ADMT; and (3) comply with restrictions on the use of personal information to train ADMT and AI.

- *Set forth requirements for conducting risk assessments*.

• **Criteria**. The proposed regulations would require businesses to conduct risk assessments for the: (1) “sale” or “sharing” of personal information; (2) processing of sensitive personal information; (3) use of ADMT for a “significant decision” concerning a consumer or for “extensive profiling”; and (4) processing of personal information to train ADMT or AI in enumerated circumstances.

• **Personnel Involvement**. The proposed regulations would require relevant individuals to prepare, contribute to, or review the risk assessment, based upon their level of involvement in the processing activity that is subject to the risk assessment (e.g., product, fraud-prevention and compliance teams), and would permit external parties to assist with conducting risk assessments (e.g., service providers, contractors, consumer advocacy organizations).

• **Content Requirements**. The proposed regulations would require risk assessments to:

• *specifically* identify the business’s purpose for processing consumers’ personal information (and not use general terms, such as “to improve our services” or for “security purposes”);

• *identify the categories of personal information* to be processed and whether they include sensitive personal information;

• *identify enumerated operational elements* of the business’s processing of personal information (e.g., method of information processing, data retention periods, technology used in processing, approximate number of consumers whose personal information is processed);

• *specifically* identify the *benefits* to the business, the consumer, other stakeholders, and the public from the processing of the personal information (*e.g.,* not use the general term "improving our services," and identify the business's expected profit from the processing);

• *specifically* identify the *negative* impacts to consumers' privacy associated with the processing (e.g., unauthorized access to personal information, discrimination, physical harms, reputational harms);

• *identify the safeguards* the business plans to implement to address the negative impacts (e.g., encryption, privacy-enhancing technologies);

• *specify whether the business will initiate the processing* subject to the risk assessment;

• *identify the contributors* to the risk assessment, the date the assessment was reviewed and approved, and the names and positions of the individuals responsible.

• **Prohibition on High-Risk Processing**. Notably, the proposed regulations would prohibit the business from conducting processing activities where the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public.

• **Timing**. The proposed regulations would require risk assessments to be conducted prior to the processing and updated at least once every three years, or immediately whenever there is a material change relating to the processing activity. Businesses would be required to retain risk assessments (including updated versions) for as long as the processing continues or for five years after the completion of the risk assessment, whichever is longer.

• **Submission to the CPPA**. Businesses would be required to submit to the CPPA the risk assessment materials identified in the proposed regulations within 24 months of the effective date of the regulations, and submit to the CPPA subsequent risk assessments every calendar year. The CPPA and the CA AG also would have the right to request a risk assessment at any time, at which point a business would be required to submit such risk assessment within 10 business days of such request.

- *Set forth requirements for cybersecurity audits.*
    - **Criteria**. The proposed regulations would require businesses to conduct cybersecurity audits where the processing of consumers' personal information presents "significant risk to consumers' security," defined as when the business *either*: (1) derives at least 50 percent of its annual revenues from "selling" or "sharing" consumers' personal information in the preceding calendar year *or* (2) in the preceding calendar year had annual gross revenues in excess of $25 million *and* (a) processed the personal information of at least 250,000 consumers or households *or* (b) processed the sensitive personal information of at least 50,000 consumers.
    - **Scope of Cybersecurity Audit**. The proposed regulations would require cybersecurity audits to identify, assess, and document:

• the business's establishment, implementation, and maintenance of its cybersecurity program, including the related written documentation thereof;

• the following components of the business's cybersecurity program:

• authentication (including MFA, password requirements);

• encryption of personal information in-transit and at rest;

• zero trust architecture;

• account management and access controls;

• inventory and management of personal information and the business's information system;

• secure configuration of hardware and software;

• internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs);

• audit-log management;

• network monitoring and defenses;

• antivirus and antimalware protections;

• segmentation of an information system;

• limitation and control of ports, services, and protocols;

• cybersecurity awareness, education and training;

• secure development and coding best practices;

• oversight of service providers, contractors and third parties;

• retention schedules and proper disposal of personal information;

• incident response procedures; and

• business-continuity and disaster-recovery plans, including data-recovery capabilities and backups.

• **Content Requirements**. The cybersecurity audit would need to, among other items, (1) assess any gaps or weaknesses identified and the business's plans to address them; and (2) identify and describe any data breaches experienced by the business and include sample individual and regulator notification letters.

• **Submission to the CPPA**. The business would be required to submit to the CPPA every calendar year a written certification that the business completed the cybersecurity audit. The written certification would need to be signed and dated by a member of the business's board or governing body, or if no such board or equivalent body exists, the business's highest-ranking executive.

During the CPPA Board's discussion of whether to advance the draft regulations to formal rulemaking, CCPA Board Chair Jennifer M. Urban emphasized that engaging in formal rulemaking is the beginning of the regulatory process and would allow the CCPA Board to make substantial

changes to the regulations to account for the comments and feedback it receives from the broader community. She further encouraged all those who have submitted comments into the record to date to resubmit comments into the formal rulemaking record.

The CPPA's Executive Director, Ashkan Soltani, announced that he will be stepping down in January 2025. Mr. Soltani, who was appointed by the CPPA Board, was the first to hold the position of CPPA Executive Director.

The date of the CPPA Board's next meeting has not yet been announced.

National Law Review, Volume XIV, Number 316