Simpson Thacher

Memorandum

California Privacy, Cybersecurity, and AI Update

October 21, 2025

California has historically been a bellwether state in the areas of privacy, cybersecurity, and artificial intelligence regulation and enforcement. This memorandum provides an overview of several recent noteworthy developments out of the state that suggest it will continue to earn that status, as they impact businesses operating in the state and may signal changes beyond California as well.[1]

New Regulations Regarding ADMT, Cybersecurity Audits, and Risk Assessments Are Set to Go Into Effect

The California Privacy Protection Agency ("CPPA") announced on September 23, 2025 the approval of regulations issued under the California Consumer Privacy Act ("CCPA") concerning automated decision-making technology ("ADMT"), cybersecurity audits and risk assessments (the "Rules").

Businesses using ADMT—technology that processes personal information and replaces human decision-making—to make "significant decisions" (*i.e.*, those involving financial, housing, education, employment, or healthcare) about consumers must provide "pre-use" notices to consumers disclosing their purpose for using ADMT. They must also notify consumers of their right to access information about such ADMT and to opt out of such use. Certain exceptions apply, and an opt-out is not required if the business offers a compliant "human reviewer" process to appeal the ADMT-made decisions or, in the education and employment context, if the ADMT is not unlawfully discriminatory.

The deadline for compliance with the ADMT Rules is January 1, 2027.

Businesses whose data processing activities are deemed to "present significant risks to consumers' security"[2] will be required to undergo an annual cybersecurity audit from an independent auditor and submit an annual written certification to the CPPA. The Rules require the audit to include an assessment of the business's processes for authentication, encryption, access controls, inventory management, secure configurations, vulnerability testing, audit logs, network defenses, and malware protections, among other things. Notably, a business may use an audit or evaluation that it has prepared for another purpose, if it meets the Rules' requirements. The deadlines for

[1] This memorandum provides only a high-level summary of these laws and developments. For a more detailed discussion, please consult one of the authors of this memorandum.

[2] This applies if, in the prior calendar year, (i) the business met the revenue threshold (currently $26,625,000), and processed the personal information of 250,000+ consumers or households, or processed the sensitive personal information of 50,000+ consumers; or (ii) derives 50+% of annual revenues from "selling" or "sharing" consumers' personal information (as defined in the CCPA).

compliance with these obligations start on a rolling basis—larger businesses must comply first—beginning on April 1, 2028.[3]

Businesses must perform risk assessments before processing personal information in a way that "presents significant risk to consumers' privacy", namely:

- "sales" or "sharing" of personal information (as defined in the CCPA),
- processing of sensitive personal information (as defined in the CCPA),
- use of ADMT to make a significant decision about a consumer,
- use of automated processing to infer or extrapolate certain traits based upon observing consumers in the education and employment context,
- use of automated processing to infer or extrapolate certain traits based upon consumers' presence in a sensitive location, and
- the processing of personal information to train (x) ADMT for a significant decision or (y) technology that verifies identities or conducts physical or biological identification or profiling.

Risk assessments must include, among other things, discussions of the benefits to the business, consumer, other stakeholders and the public from the processing activity, and the resulting negative impact to consumers' privacy.

The Rules relating to risk assessments take effect on January 1, 2026, and businesses must submit an attestation and summary of their risk assessment by April 1, 2028.

CPPA Fines Tractor Supply Company $1.35M for Privacy Violations

On September 26, 2025, the CPPA fined Tractor Supply Company ("Tractor Supply") $1,350,000 for multiple privacy violations under the CCPA. These violations fell into three categories: failure to honor consumer opt-out requests, failure to provide sufficient notice to consumers and job applicants, and failure to comply with the CCPA's contractual requirements for service providers and third parties that receive data.

CONSUMER OPT-OUT REQUESTS

The CPPA found that Tractor Supply failed to honor consumer requests to opt out of the "share" or "sale" of personal information under the CCPA, specifically with regard to advertising cookies and similar technology on its website. The opt-out requests were submitted either through an online webform or via browser-based opt out preference signals, such as the Global Privacy Control. The agency found nearly identical violations earlier this

[3] Beginning on April 1, 2028, if the business's annual gross revenue was more than $100,000,000 in 2026, April 1, 2029, if the business's annual gross revenue was between $50 million and $100 million in 2027, and April 1, 2030, if the business's annual gross revenue was less than $50 million in 2028.

year in the American Honda Motor Co., and Todd Snyder enforcement actions, highlighting its focus on California consumers' right to opt-out under the CCPA.

DEFICIENT NOTICE TO CONSUMERS AND JOB APPLICANTS

The CPPA also found violations associated with Tractor Supply's privacy policies. Its website privacy policy had not been updated for over two years (rather than annually as required under the CCPA), nor did it include a description of California consumers' privacy rights under the CCPA. Further, the Tractor Supply employee privacy policy—which was posted on its job posting page—similarly did not include a description of California consumers' privacy rights. Among the many states that have passed privacy laws, California's privacy law is the only one to broadly apply in the employment context. The fine against Tractor Supply is the first against a business for violating an employee's privacy rights under the CCPA.

CCPA CONTRACT REQUIREMENTS

Finally, the CPPA found that Tractor Supply did not enter into CCPA compliant contracts with its service providers or third parties, such as advertising technology companies, by failing to include CCPA-required terms in those contracts.

1. Transparency in Frontier Artificial Intelligence Act (SB 53)

SB 53, the Transparency in Frontier Artificial Intelligence Act ("TFAIA"), signed into law on September 29, 2025, imposes requirements on "frontier model developers" of artificial intelligence systems. Under that act, that term means the developers who train, or initiate the training of, an artificial intelligence model using "frontier models," (*i.e.*, an model trained using computing power above a certain threshold[4]). Frontier model developers must publish on their website a mechanism to communicate with the developer, the release date of the frontier model, languages supported, modalities of output, intended uses, and generally applicable restrictions. "Large frontier developers" (those exceeding $500 million gross annual revenue in the preceding year), have additional obligations. For example, they must publish and comply with an AI framework that includes, among other things, technical and organizational protocols to manage, assess and mitigate certain statutorily defined "catastrophic risks," and they must periodically provide the California Office of Emergency Services with a report on their assessment of these catastrophic risks resulting from internal use of their frontier models.

The law prohibits all frontier developers from making materially false or misleading statements about catastrophic risks and prohibits large frontier developers from making materially false or misleading statements about their implementation or compliance with their AI framework. The TFAIA also includes certain

[4] The relevant computing power threshold is 10^26 integer floating-point operations (or "FLOPs"). FLOPs represent, generically, the number of calculations performed, in this case, to train the AI model.

whistleblower protections for employees of frontier developers who are responsible for addressing critical safety incidents.

TFAIA goes into effect on January 1, 2026.

2. California's Opt Me Out Act (AB 566)

AB 566, signed into law on October 8, 2025, requires that web browser developers include functionality—configurable by consumers—to send a "universal opt-out preference signal" to opt-out of the "sale" or "sharing" of the consumer's personal information on websites they visit. While the CCPA already requires website operators to honor universal opt-out preference signals, such as Global Privacy Control, this law imposes obligations on a different part of the internet ecosystem: the web browsers.

The law becomes effective on January 1, 2027, and the CPPA may adopt further regulations to implement it before that date.

3. Updated Requirements for Data Brokers (SB 361)

SB 361, also signed into law on October 8, 2025, requires data brokers[5] subject to the CCPA to (i) provide to the CCPA details regarding new enumerated categories of personal information the data broker collects (*e.g.*, account login in combination with a security code/password, citizenship data, biometric information, and precise geolocation data, among other categories), and (ii) indicate to the CPPA whether the data broker has shared or sold consumers' data to certain specified third parties (*e.g.*, foreign actors, the federal or state government, law enforcement, and developers of generative AI systems/models), as such terms are defined in the CCPA.

The law becomes effective January 1, 2026.

4. Companion Chatbots (SB 243)

SB 243, signed into law on October 13, 2025, imposes requirements on operators of "companion chatbots," which are defined as an AI system with a "natural language interface that provides adaptive, human-like responses to user inputs and is capable of meeting a user's social needs, including by exhibiting anthropomorphic features and being able to sustain a relationship across multiple interactions." The law requires operators to: (i) provide a conspicuous notice indicating that the companion chatbot is artificially generated, if a reasonable person would otherwise be misled to believe they are interacting with a human; (ii) maintain a protocol for preventing the production of suicidal ideation, suicide, or self-harm content, including by referring users to contact a crisis service provider or suicide hotline; and (iii) where the operator knows that the user is a minor, disclose that the user is interacting with AI, remind the user to "take a break" every three hours of continuous use, and institute reasonable measures to prevent the chatbot from producing visual material of sexually explicit conduct or from

[5] Defined under existing law as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship, subject to specified exceptions.

stating that the minor should engage in sexually explicit conduct. The law also requires operators to report information to the Office of Suicide Prevention, including the number of crisis service provider referrals, and the protocols required under the law.

The law begins to take effect on January 1, 2026, with reporting requirements beginning July 1, 2027.

Key Takeaways

These recent developments demonstrate that California continues to be an active leader in this space and is committed to ensuring robust consumer protections and business accountability. In particular, the Tractor Supply case serves as a cautionary example that businesses must not overlook compliance with seemingly minor or routine obligations, as even low-level violations can attract scrutiny and result in monetary penalties. Companies operating in California should be evaluating their policies and practices to ensure compliance with the state's current and future regulatory requirements.

For further information regarding this memorandum, please contact one of the following authors:

NEW YORK

Lori E. Lesser
+1-212-455-3393
llesser@stblaw.com

Caroline Geiger
+1-212-455-3572
caroline.geiger@stblaw.com

James Talbot
+1-212-455-3544
james.talbot@stblaw.com

Alexander J. Franchilli
+1-212-455-6654
alexander.franchilli@stblaw.com

Alysha J. Sekhon
+1-212-455-3762
alysha.sekhon@stblaw.com

Margerite Blase
+1-212-455-2369
margerite.blase@stblaw.com

Kate E. Mirino
+1-212-455-2055
kate.mirino@stblaw.com

PALO ALTO

Corina Holland
+1-650-251-5073
corina.holland@stblaw.com

Alexander Kokka
+1-650-251-5374
alexander.kokka@stblaw.com

LOS ANGELES

Ron Ben-Yehuda
+1-310-407-7537
ron.ben-yehuda@stblaw.com