HINSHAW

Alerts

More Proposed Regulations from California: What Do These Mean for Your Business?

July 29, 2024
Privacy, Cyber & AI Decoded

What Issues Did the California Privacy Protection Agency Raise?

On July 16, 2024, the California Privacy Protection Agency (Agency) discussed proposed updates to the California Consumer Privacy Act (CCPA) regulations. These proposed updates involve:

- Enforcement priorities
- Insurance company privacy-related regulations
- Cybersecurity audits
- Privacy risk assessments
- Automated decision-making technology (ADMT)

Enforcement Priorities

As part of the July 16 meeting, the Agency discussed continued staff expansion and Agency enforcement priorities:

- The Agency indicated that enforcement investigations will continue to grow, including the ongoing connected car privacy investigation.
- The Agency reemphasized its priorities for compliant privacy notices and policies, businesses implementing a consumer's right to delete, and implementation of consumer requests.
- The Agency indicated that noncompliance with ongoing enforcement advisories, like the April 2024 data minimization advisory, can show a lack of compliance and potentially lead to higher fines.
- The Agency stressed four additional categories of enforcement priorities:

1. failure to honor opt-out requests unless a consumer submits verification;
2. businesses that share and sell personal information without an opt-out mechanism;
3. businesses that use dark patterns to prevent consumers from exercising their rights; and
4. violations of the CCPA and implementing regulations impacting vulnerable groups.

Attorneys

Sabrina Janeiro

Cathy Mulrow-Peattie

Service Areas

Privacy, Security & Artificial Intelligence

We recommend that businesses review their privacy practices immediately for compliance with these enforcement priorities.

Insurance Regulations

Insurance companies that fall under the CCPA's definition of a business are now required to comply with the act regarding any personal information collected for purposes other than in connection with an insurance transaction.

For example, an insurance company that collects personal information from consumers visiting its website solely for advertising purposes (and not for an insurance product or service) must now comply with the CCPA's requirements, such as providing an opt-out right for consumers for the sale or sharing of its data and an updated privacy policy/notice at collection.

This change will likely impact most insurance companies, many of which are not familiar with the CCPA's requirements and obligations.

Cybersecurity Audits

- Similar to the New York State Department of Financial Services (NYSDFS) Part 500, the revised Agency regulations require that subject businesses annually undertake an independent cybersecurity audit and submit a written certification that the businesses have complied with the CCPA security requirements, including an audit requirement.
- The scope of the audit must include determining whether the business's cybersecurity program is appropriate for its size and the complexity of its data processing activities.
- Service providers are required to assist with such cybersecurity audits.
- While businesses have 24 months from the effective date of the regulations to complete their first audit, businesses that are trying to streamline their cybersecurity regulatory compliance should review these regulations as the Agency will most likely promulgate them in a substantially similar form.

Risk Assessments

Businesses that engage in processing activities deemed by the revised regulations as presenting **"significant risks"** to consumer privacy will now be required to conduct risk assessments.

These significant risks include selling or sharing personal information, processing sensitive data (with certain exceptions), and using artificial intelligence (AI) for higher-risk activities.

The risk assessment will assess:

- Whether the risks to consumer privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public, and what safeguards or mitigation tactics are in place.
- Service providers are required to assist with such risk assessments.
- Businesses required to conduct a risk assessment will have 24 months from the effective date of the revised regulations to submit the risk assessment materials to the Agency. Subsequent risk assessment materials are required to be submitted annually.

Companies updating their risk assessment processes for AI may want to consider these Agency requirements for their 2025 planning.

Automated Decision-making Technology (ADMT) Regulations

The Agency's ADMT regulations have a broad definition of artificial intelligence and ADMT technology, which includes scoring and profiling technologies. New consumer rights, such as pre-use notices and the option to opt out and access data in ADMT technology, would be required.

These regulations could be challenging for companies leveraging large language models (LLM) and untagged data. The Agency is still discussing these regulations.

What's Next?

- The Agency did not send the regulations to final rulemaking because they are still discussing certain topics we itemized above, particularly the ADMT regulations and risk assessments. These regulations will be reviewed for final approval and will begin a 45-day public comment period in September 2024.
- Once finalized, these regulations may have significant operational changes for subject organizations. The earliest the draft regulations could take effect is January 1, 2025, with a more likely effective date sometime in April–June 2025.
- We will watch the development of these regulations closely. Given the lack of progress with a federal privacy law, we expect other states to follow California's path. As companies begin their planning process for 2025, they should keep these requirements in mind.