



California Regulators Take Aim at Resume Screening and Other Automated Tech: 4 Steps for Businesses After Latest Privacy Agency Meeting

Insights

11.13.24

In its public meeting last week, California privacy officials pushed forward key initiatives that could impact businesses and employers, including initiating formal rulemaking that would significantly impact those using resume screening and other automated decision-making technology (ADMT). But that's not all – the agency also is looking at finalizing data broker registration requirements and updating the future direction of California Consumer Privacy Act. These rulemaking initiatives have added to businesses' to-do list in order to stay compliant – and to stay ahead of a last-minute scramble to comply. Here's what businesses need to know about these latest actions and the four steps you should take to prepare.

CPPA Pushes ADMT Regulations Forward for Public Comment

For employers already subject to the California Consumer Privacy Act, the California Privacy Protection Agency (CPPA) on Friday advanced its proposed regulations on ADMTs to the formal rulemaking process, now open for public comment. These regulations will ultimately only apply to businesses who are subject to the CPPA.

According to the [regulation's proposed text](#), ADMTs are defined as “any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking.” [Examples of ADMTs](#) identified by the CPPA which employers already use include resume-screening tools, facial recognition technology, and emotion-assessment technology. Those businesses interested in or already incorporating AI systems into their processes will need to pay particular attention.

The draft regulations would impose significant additional requirements on businesses using ADMTs. These requirements would include:

- a pre-use notice about the ADMT;
- the right to opt out (with certain exceptions to the opt-out requirement); and
- for consumers who did not opt out, the right to access information about how the ADMT the business used the ADMT with respect to them.

The proposed regulations create some potentially significant carve-outs to the right to opt-out in the employment context, but each use of an ADMT would need to be evaluated to determine whether a carve-out applies. In certain circumstances, businesses would be able to omit an opt-out if they create an appeal mechanism to have the results of the ADMT reviewed by a human.

New Data Broker Registration Requirements and Fee Increase Approved

The CPPA has moved a step closer to finalizing regulations which clarify which companies must register as data brokers, and these regulations will take effect 30 days after approval by the California Office of Administrative Law (OAL).

Under existing law, a business is a data broker if it “knowingly collects or sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.” The term direct relationship was never defined – a gap these new regulations seek to fill in.

Under the new regulations, a direct relationship exists when a consumer intentionally interacts with a business to obtain, use, or inquire about its products or services within the last three years. Interactions aimed at exercising legal rights or identity verification under the California Consumer Privacy Act do not count as creating a direct relationship.

This means a business is still considered a data broker if it sells information collected from consumers indirectly. The CPPA clarified that this definition underscores that the consumer’s intent, not the act of data collection, establishes a direct relationship. It also clarified that businesses can qualify as data brokers through both direct and third-party interactions. Critically, the CPPA has acknowledged through the rule-making process that collection and sale of data through website tracking technology may bring a business within the ambit of the “data broker” definition.

The CPPA also approved an increase of the data broker registration fee, currently estimated at \$6,600, to fully fund the Data Request Opt-Out Platform (DROP), pursuant to the Delete Act (SB 362). Data brokers must register annually, access DROP at least every 45 days, pay an access fee adjusted to the current number of registrants, update mandatory disclosures by July 1 each year, report on the previous year’s activities, and undergo an independent audit every three years. The fee increase is to accommodate DROP’s project cost of \$3.5 million, with its expected launch in January 2026.

A Look To The Future

The CPPA has identified several key topics as priorities for potential regulation, including employment data, financial incentives and loyalty programs, insurance, and a whistleblower or self-reporting mechanism to encourage compliance and aid enforcement. While these topics have not yet been ranked in priority, the agency plans to revisit and formally prioritize them at its May 2025 meeting to accommodate for the CPPA’s current emphasis on advancing DROP.

CPPA Executive Director Ashkan Soltani, the agency's inaugural leader, announced he will be stepping down after three years in his role in January 2025. The CPPA Board governs the agency and administers the policies set by the CPPA Board, so Soltani's exit does not mean that businesses should expect a wholesale policy shift with a new Executive Director.

That being said, at the last meeting the CPPA Board members took turns elaborating how much help they received from Soltani, especially within the context of navigating the technical aspects of CPPA work, and how his input and experience helped influence their decisions in drafting regulations. The CPPA Board also emphasized how Soltani was integral to the design and implementation of DROP. As such, the next Executive Director will have likely have the ability to inform and guide the CPPA Board based on their own experiences in the privacy sphere, as well as influencing how the agency's policies are administered on a day-to-day basis.

Your Next Steps

To best position your organization for these CPPA updates, we suggest you consider the following three steps:

1. Identify ADMTs in Your Business

Identify any ADMTs in use and assess areas potentially impacted by the proposed regulations. This preparation will ready your business for compliance and enable you to provide meaningful feedback to the CPPA (as discussed below), potentially shaping the final regulations.

2. Consider Submitting a Public Comment on CPPA Regulations

Consider submitting detailed feedback to the CPPA during the public comment period. These regulations are projected to impose \$3.5 billion in direct compliance costs if enacted as proposed. While instructions for submitting comments are not yet public, businesses can currently follow the path of regulations on the [CPPA's website](#). The CPPA Board emphasized its desire for specific input from stakeholders, noting that public comments will directly shape and potentially revise the regulations. The formal 45-day public comment period will begin once the OAL posts the notice of proposed rulemaking. While this period may be extended for the holidays, it's best to plan for the original deadline to ensure your public comment will be considered.

3. Evaluate Whether You Qualify as a Data Broker

In light of the anticipated regulations, businesses should take a second look at whether they could qualify as a data broker. If you qualify as a data broker under these regulations, follow the [CPPA's instructions](#) on how to register and submit your registration and fee no later than January 31, 2025, to remain compliant.

4. Review Your Website's Tracking Technology

The data broker law requires that the direct relationship exist within the preceding three years. Any website tracking technology that lasts longer than that could make your business a data broker under this law. As such, it is important that business's take a close look at the tracking technology on their website and ensure that such technology has a built-in expiration date for users.

Conclusion

In support of businesses navigating these complex regulations, we've launched our [U.S. Privacy Hub](#), which offers FAQs and comprehensive charts on all 19 state consumer privacy laws currently in effect. For more information on these laws, please explore [our latest insight](#) and discover our expanded consumer privacy resources in the U.S. Privacy Hub.

Fisher Phillips will continue to monitor CCPA obligations and enforcement efforts and provide updates as warranted, so make sure that you are subscribed to [Fisher Phillips' Insights](#) to get the most up-to-date information directly to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's [Consumer Privacy Team](#).

This Insight was co-authored by Law Clerk [Chelsea Viola](#) (Los Angeles).

Related People

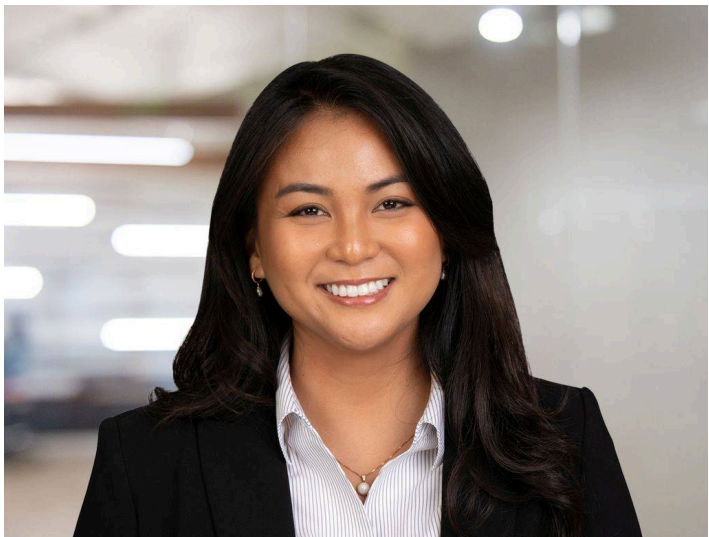


Darcey M. Groden, CIPP/US

Associate

858.597.9627

Email



Chelsea Viola
Associate
213.403.9626
Email

Service Focus

Privacy and Cyber
AI, Data, and Analytics
Consumer Privacy Team
Government Relations

Trending

AI Governance Hub

Related Offices

Irvine
Los Angeles
Sacramento
San Diego
San Francisco
Woodland Hills